



CHAPTER 48

Monitoring Trend Micro Content Security

**Note**

The ASA 5580 does not support the CSC SSM feature.

ASDM lets you monitor the CSC SSM statistics as well as CSC SSM-related features.

For an introduction to the CSC SSM, see the [“Information About the CSC SSM”](#) section on page 31-1.

**Note**

If you have not completed the CSC Setup Wizard in Configuration > Trend Micro Content Security > CSC Setup, you cannot access the panes under Monitoring > Trend Micro Content Security. Instead, a dialog box appears and lets you access the CSC Setup Wizard directly from Monitoring > Trend Micro Content Security.

Threats

To view information about various types of threats detected by the CSC SSM in a graph, perform the following steps:

Step 1 Choose **Monitoring > Trend Micro Content Security > Threats**.

The Available Graphs area lists the components whose statistics you can view in a graph. You can include a maximum of four graphs in one frame. The graphs display real-time data in 12-second intervals for the following:

- Viruses detected
- URLs filtered, URLs blocked
- Spam detected
- Files blocked
- Spyware blocked
- Damage Cleanup Services

Step 2 The Graph Window Title lists the types of statistics available for monitoring. You can choose up to four types of statistics to show in one graph window. You can open multiple graph windows at the same time. The statistics already included in the graph window appear in the Selected Graphs list.

Step 3 To move the selected statistics type in the Available Graphs For list to the Selected Graphs list, click **Add**.

- Step 4** To remove the selected statistics type from the Selected Graphs list, click **Remove**. The button name changes to **Delete** if the item you are removing was added from another pane, and is not being returned to the Available Graphs pane.
- Step 5** To display a new window that shows a Graph tab and an updated graph with the selected statistics, click **Show Graphs**. Click the **Table** tab to display the same information in tabular form.
- Step 6** From the Graph or Table tab, click **Export** in the menu bar or choose **File > Export** to save the graph or tabular information as a file on your local PC.
- Step 7** From the Graph or Table tab, click **Print** in the menu bar or choose **File > Print** to print the information displayed in the window.

For more information, see the [“Prerequisites for the CSC SSM”](#) section on page 31-2.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Live Security Events

To view live, real-time security events in a separate window, perform the following steps:

- Step 1** Choose **Monitoring > Trend Micro Content Security > Live Security Events**.
- The Buffer Limit field shows the maximum number of log messages that you may view. The default is 1000.
- Step 2** Click **View** to display the Live Security Events Log dialog box. You can pause incoming messages, clear the message window, and save event messages. You can also search messages for specific text.

For more information, see the [“Information About the CSC SSM”](#) section on page 31-1.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Live Security Events Log

To view live security events messages that are received from the CSC SSM, perform the following steps:

-
- Step 1** To filter security event messages from the Filter By drop-down list, choose one of the following:
- Filter by Text, type the text, then click **Filter**.
 - Show All, to display all messages or remove the filter.
- Step 2** To use the Latest CSC Security Events pane, in which all columns are *display-only*, choose one of the following options:
- The time an event occurred.
 - The IP address or hostname from which the threat came.
 - The type of threat, or the security policy that determines event handling, or in the case of a URL filtering event, the filter that triggered the event.
 - The subject of e-mails that include a threat, or the names of FTP files that include a threat, or blocked or filtered URLs.
 - The recipient of e-mails that include a threat, or the IP address or hostname of a threatened node, or the IP address of a threatened client.
 - The type of event (such as Web, Mail, or FTP), or the name of a user or group for HTTP or FTP events, which include a threat.
 - The action taken upon the content of a message, such as cleaning attachments or deleting attachments.
 - The action taken on a message, such as delivering it unchanged, delivering it after deleting the attachments, or delivering it after cleaning the attachments.
- Step 3** To search security event messages based on the text that you enter, choose one of the following:
- In the Text field, enter the text to search for in the security event messages log, then click **Find Messages**.
 - To find the next entry that matches the text you typed in this field, click **Find**.
- Step 4** To pause the scrolling of the Live Security Events log, click **Pause**.
- Step 5** To save the log to a file on your PC, click **Save**.
- Step 6** To remove the list of messages, click **Clear Display**.
- Step 7** To close the pane and return to the previous screen, click **Close**.

For more information, see the [“Information About the CSC SSM”](#) section on page 31-1.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Software Updates

To view information about CSC SSM software updates, perform the following steps:

Choose **Monitoring > Trend Micro Content Security > Software Updates**.

The Software Updates pane displays the following information, which is refreshed automatically about every 12 seconds:

- The names of parts of the CSC SSM software that can be updated.
- The current version of the corresponding component.
- The date and time that the corresponding component was last updated. If the component has not been updated since the CSC SSM software was installed, “None” appears in this column.
- The date and time that ASDM last received information about CSC SSM software updates.

For more information, see the [“Information About the CSC SSM” section on page 31-1](#).

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Resource Graphs

The adaptive security appliance lets you monitor CSC SSM status, including CPU resources and memory usage.

- [CSC CPU, page 48-4](#)
- [CSC Memory, page 48-5](#)

CSC CPU

To view CPU usage by the CSC SSM in a graph, perform the following steps:

Step 1 Choose **Monitoring > Trend Micro Content Security > Resource Graphs > CSC CPU**.

The CSC CPU pane displays the components whose statistics you can view in a graph, including statistics for CPU usage on the CSC SSM.

Step 2 To continue, go to Step 2 of the [“Threats” section on page 48-1](#).

For more information, see the [“Information About the CSC SSM” section on page 31-1](#).

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

CSC Memory

To view information about memory usage on the CSC SSM in a graph, perform the following steps:

Step 1 Choose **Monitoring > Trend Micro Content Security > Resource Graphs > CSC Memory**.

The Available Graphs area lists the components whose statistics you can view in a graph, including the following.

- The amount of memory not in use.
- The amount of memory in use.

Step 2 To continue, go to Step 2 of the [“Threats” section on page 48-1](#).

For more information, see the [“Information About the CSC SSM” section on page 31-1](#).

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

