



## CHAPTER 37

# Monitoring Trend Micro Content Security

---

ASDM lets you monitor the Content Security and Control (CSC) SSM statistics as well as CSC SSM-related features.

For an introduction to CSC SSM, see [About the CSC SSM](#).



### Note

If you have not completed the 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 Setup Wizard directly from Monitoring > Trend Micro Content Security.

---

## Threats

Threats lets you view in a graph format information about various types of threats detected by the CSC SSM. You can graph a maximum of four graphs in one frame.

### Fields

- Available Graphs for—Lists the components you can graph. The graphs display data in ten-second intervals.
  - Viruses detected—Displays statistics about viruses detected.
  - URL Filtered, URL Blocked—Displays statistics about URLs filtered and blocked.
  - Spam detected—Displays statistics about spam e-mail detected.
  - Spyware blocked—Displays the statistics about spyware blocked.
- Graph Window—Shows the graph window name to which you want to add a statistic type. If you have a graph window already open, a new graph window is listed by default. If you want to add a statistic type to an already open graph, choose the open graph window name. The statistics already included in the graph window are shown in the Selected Graphs list, to which you can add additional types (up to a maximum of four types per window).
- Add—Click to move the selected entries in the Available Graphs For list to the Selected Graphs list.
- Remove—Removes the selected statistic type from the Selected Graphs list.
- Show Graphs—Click to display a new or updated graph window with the selected statistics.

### Modes

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

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

**For More Information**

[Managing the CSC SSM](#)

## Live Security Events

Use the Live Security Events pane to view live, real time security events in a separate window.

**Fields**

- Buffer Limit—The maximum number of log messages to view. The default is 1000.
- View—Opens a separate window that displays the event messages. From here you can pause incoming messages, clear the message window, and save event messages. You can also search messages for specific text.

**Modes**

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

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

**For More Information**

[Managing the CSC SSM](#)

## Live Security Events Viewer

The Live Security Events Viewer lets you view security event messages in real time that are received from the CSC SSM. You can filter security event messages based on text you specify.

**Fields**

- Filter Incoming Messages
  - Show All—Displays all messages.
  - Filter by Text—Lets you filter the messages based on text you enter.
- Filter—Use to filter the messages.
- Find Messages—Searches the messages based on the text you enter.
  - Text—Enter the text to search for in the messages log.

- Find Next—Use to find the next entry that matches the text you typed in Text.
- Columns—Displays the following, read-only columns:
  - Time—Displays the time an event occurred.
  - Source—Displays the IP address or hostname from which the threat came.
  - Threat/Filter—Displays the type of threat or, in the case of a URL filter event, the filter that triggered the event.
  - Subject/File/URL—Displays the subject of e-mails containing a threat, the names of FTP file containing a threat, or URLs blocked or filtered.
  - Receiver/Host—Displays the recipient of e-mails containing a threat or the IP address or hostname of a node threatened.
  - Sender—Displays the sender of e-mails containing a threat.
  - Content Action—Displays the action taken upon the content of a message, such as cleaning attachments or deleting attachments.
  - Msg Action—Displays the action taken upon a message, such as delivering the message unchanged, delivering the message after deleting the attachments, or delivering the message after cleaning the attachments.
- Pause—Use to pause the scrolling of the Live Security Events log.
- Save Events As—Click to save the log to your PC.
- Clear Display—Clears the list of messages.
- Close—Closes the pane and returns to the previous screen.

### Modes

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

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

### For More Information

[Managing the CSC SSM](#)

## Software Updates

The Software Updates pane displays information about updates to software on the CSC SSM.

### Fields

- Component—Displays names of parts of the CSC SSM software that can be updated.
- Version—Displays the current version of the corresponding component.
- Last Update—Displays the date and time that the corresponding component was updated. If the component has never been updated since the CSC SSM software was installed, “None” appears in this column.

- Last Refresh—Displays the date and time when ASDM last received information from CSC SSM regarding software updates.

### Modes

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

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

### For More Information

[Managing the CSC SSM](#)

## Resource Graphs

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

- [CSC CPU](#)
- [CSC Memory](#)

## CSC CPU

The CSC CPU pane lets you view information in a graph format about CPU utilization by the CSC SSM.

### Fields

- Available Graphs for—Lists the components you can graph.
  - CPU Utilization—Displays statistics for CPU use on the CSC SSM.
- Graph Window—Shows the graph window name to which you want to add a statistic type. If you have a graph window already open, a new graph window is listed by default. If you want to add a statistic type to an already open graph, choose the open graph window name. The statistics already included in the graph window are shown in the Selected Graphs list, to which you can add additional types (up to a maximum of four types per window).
- Add—Click to move the selected entries in the Available Graphs For list to the Selected Graphs list.
- Remove—Removes the selected statistic type from the Selected Graphs list.
- Show Graphs—Click to display a new or updated graph window with the selected statistics.

### Modes

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

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

**For More Information**

[Managing the CSC SSM](#)

## CSC Memory

The CSC Memory pane lets you view in a graph format information about memory usage on the CSC SSM.

**Fields**

- Available Graphs For—Lists the components you can graph.
  - Free Memory—Displays statistics about the amount of memory not in use.
  - Used Memory—Displays statistics about the amount of memory in use.
- Graph Window—Shows the graph window name to which you want to add a statistic type. If you have a graph window already open, a new graph window is listed by default. If you want to add a statistic type to an already open graph, choose the open graph window name. The statistics already included in the graph window are shown in the Selected Graphs list, to which you can add additional types (up to a maximum of four types per window).
- Add—Click to move the selected entries in the Available Graphs For list to the Selected Graphs list.
- Remove—Removes the selected statistic type from the Selected Graphs list.
- Show Graphs—Click to display a new or updated graph window with the selected statistics.

**Modes**

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

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

**For More Information**

[Managing the CSC SSM](#)

