CHAPTER 7

Monitoring Content Security

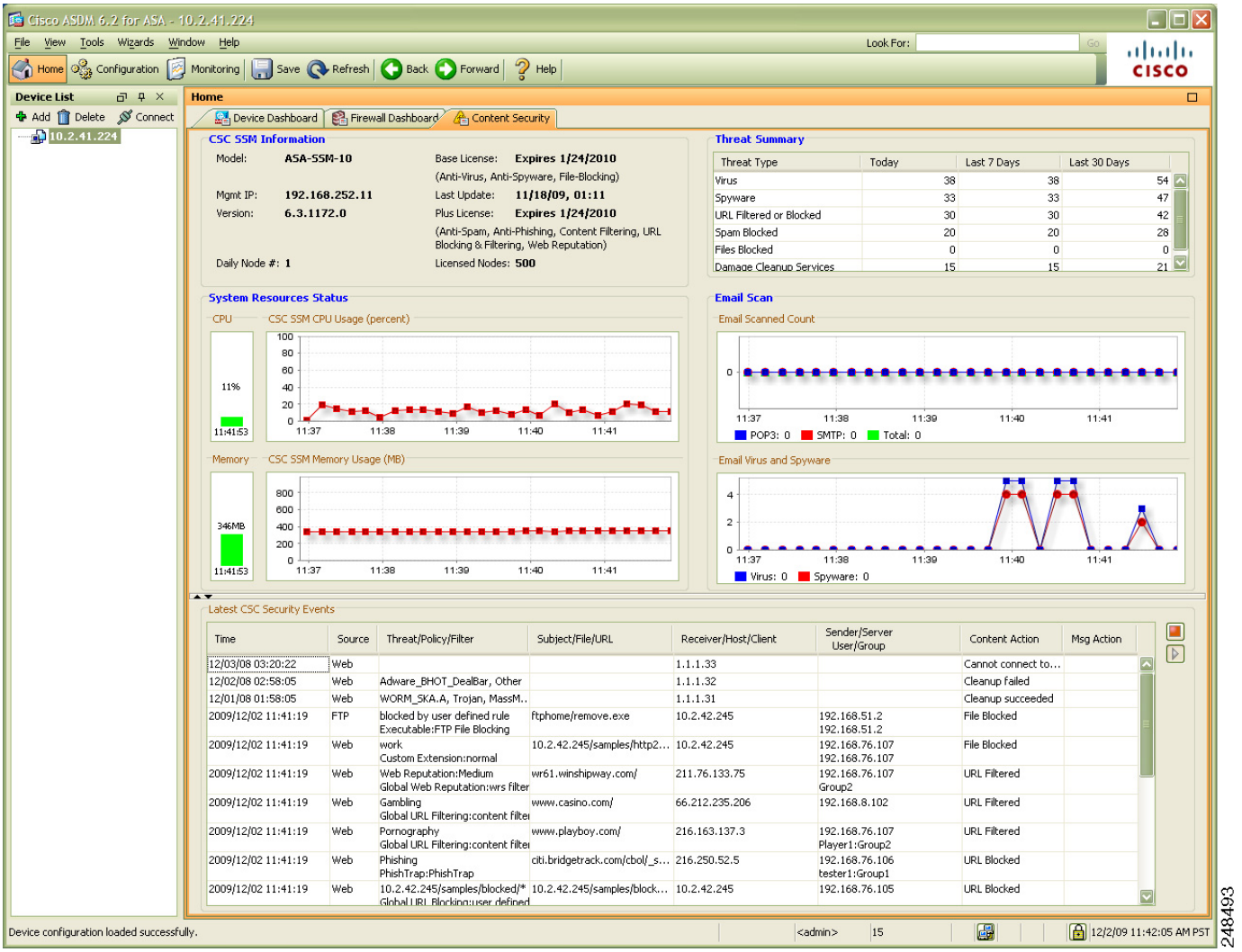
This chapter describes monitoring content security from ASDM, and includes the following sections:

Features of the Content Security Tab

After you have connected to the CSC SSM, the Content Security tab displays, as shown in Figure 7-1 on page 7-2. The Content Security tab shows you content security status at a glance, including the following:

- CSC SSM Information—Displays the product model number, IP address of the device, version, and build number of the CSC SSM software.
- Threat Summary—Displays a table summarizing threats detected today, within the last seven days, and within the last 30 days.
- System Resources Status—Allows you to view CPU and memory usage on the SSM.
- Email Scan—Provides a graphical display of the number of e-mail messages scanned and the number of threats detected in the scanned e-mail.
- Latest CSC Security Events—Lists the last 25 security events that were logged.

Figure 7-1 Content Security Tab



Click the **Help** icon to view more details about the information that appears in this window.

Monitoring Content Security

This section describes how to monitor content security, and includes the following topics:

- Monitoring Threats, page 7-3
- Monitoring Live Security Events, page 7-4
- Monitoring Software Updates, page 7-5
- Monitoring Resources, page 7-7

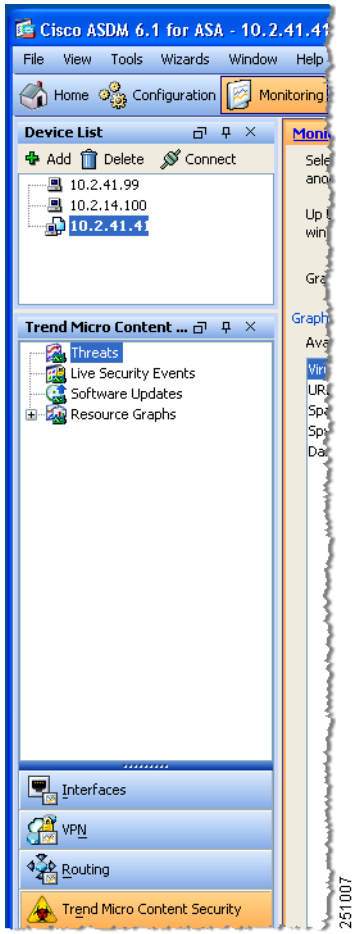
To display the content security monitoring settings for recent threat activity, perform the following steps:

Step 1 Choose **Monitoring > Trend Micro Content Security**, as shown in Figure 7-2.

Step 2 Choose from the following options:

- Threats—Displays recent threat activity.
- Live Security Events—Displays a report of recent security events (content-filtering violations, spam, virus detection, and spyware detection) for monitored protocols.
- Software Updates—Displays the version and last date and time for updates to content security scanning components (virus pattern file, scan engine, and spyware or grayware pattern).
- Resource Graphs—Displays graphs of CPU usage and memory usage for the SSM.

Figure 7-2 Content Security Monitoring Options in ASDM



Monitoring Threats

To monitor threats, perform the following steps:

Step 1 Click **Threats** in the Monitoring pane, as shown in Figure 7-2, to choose up to four categories of threats for graphing.

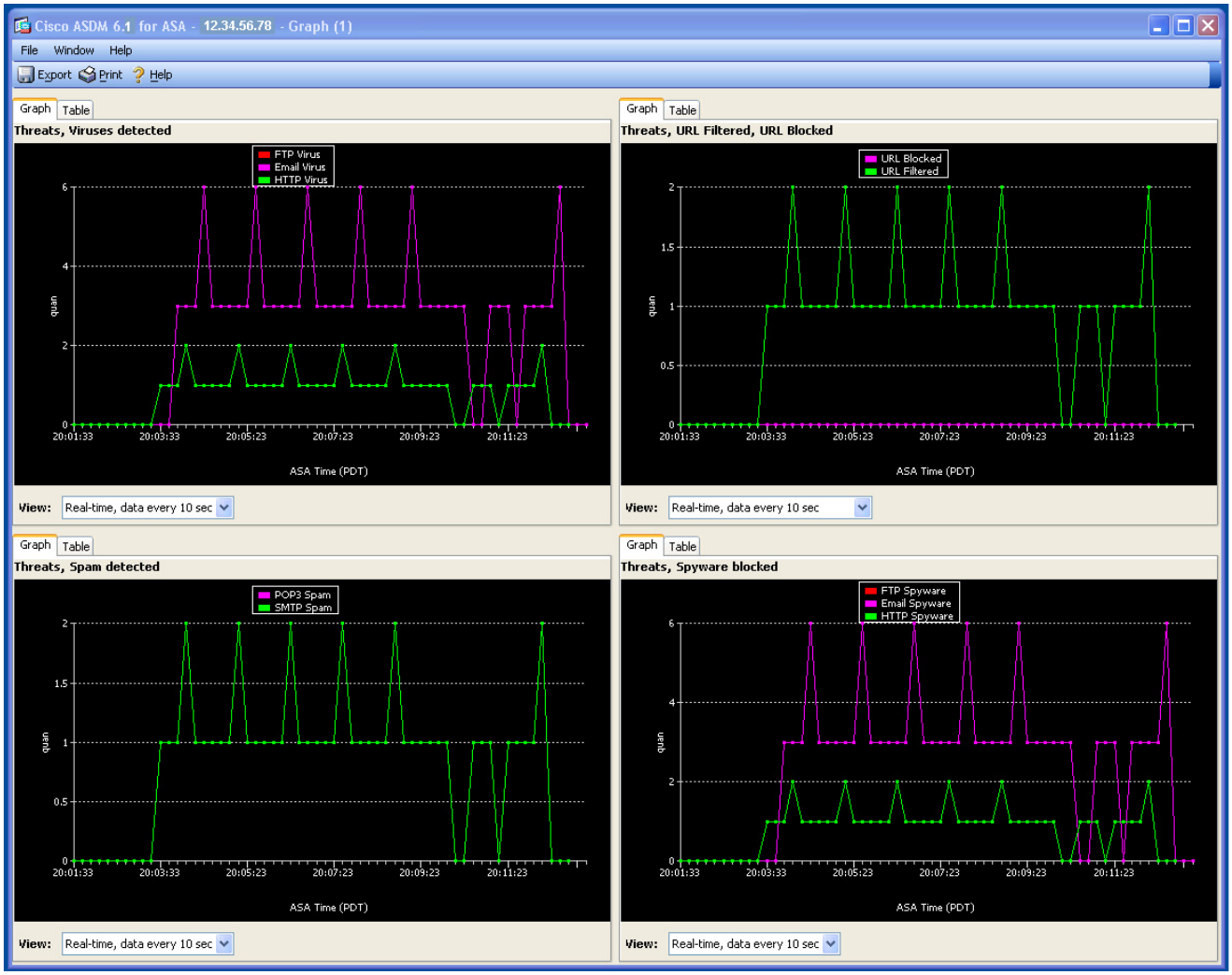
Step 2 To display recent activity, choose one or more of the following categories:

- Viruses and other threats detected

- Spyware blocked
- Spam detected (requires the Plus license)
- URL filtering activity and URL blocking activity (requires the Plus license)

For example, if you have the Basic license and Plus license, and you choose all four threat types for monitoring, the graphs appear similar to the example shown in Figure 7-3.

Figure 7-3 Threat Monitoring Graphs



The graphs refresh at frequent intervals (every ten seconds), which allows you to view recent activity at a glance. For more information, see the online help.

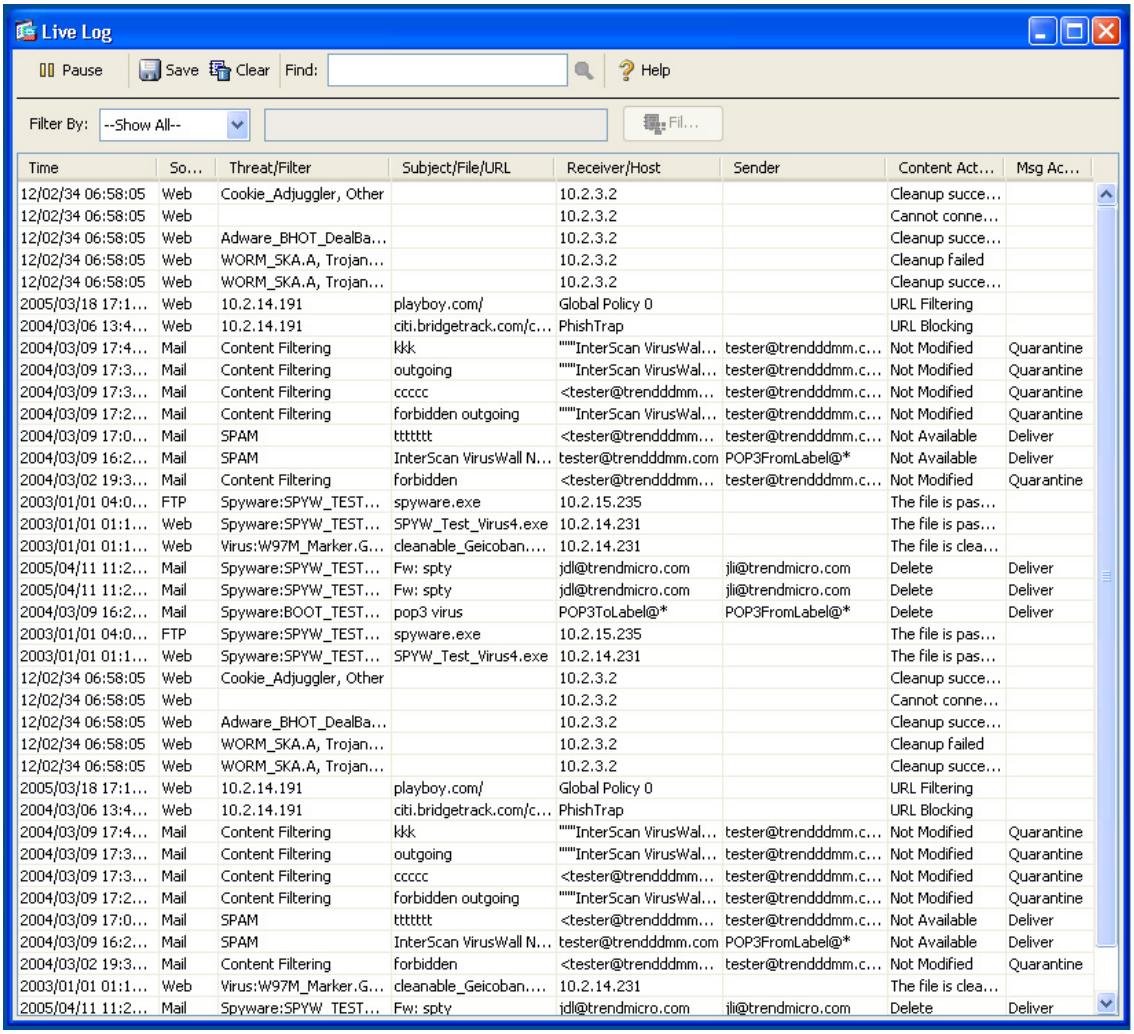
Monitoring Live Security Events

To monitor live security events, perform the following steps:

Step 1 Click **Live Security Events** in the Monitoring pane.

Step 2 Click **View** to create a report similar to the example shown in Figure 7-4.

Figure 7-4 Live Security Events Report



This report lists events that the CSC SSM detected. The Source column displays “Mail” for both SMTP and POP3 protocols. The horizontal and vertical scroll bars allow you to view additional report content. Filters at the top of the screen allow you to refine your search for specific events. For more information, see the online help.

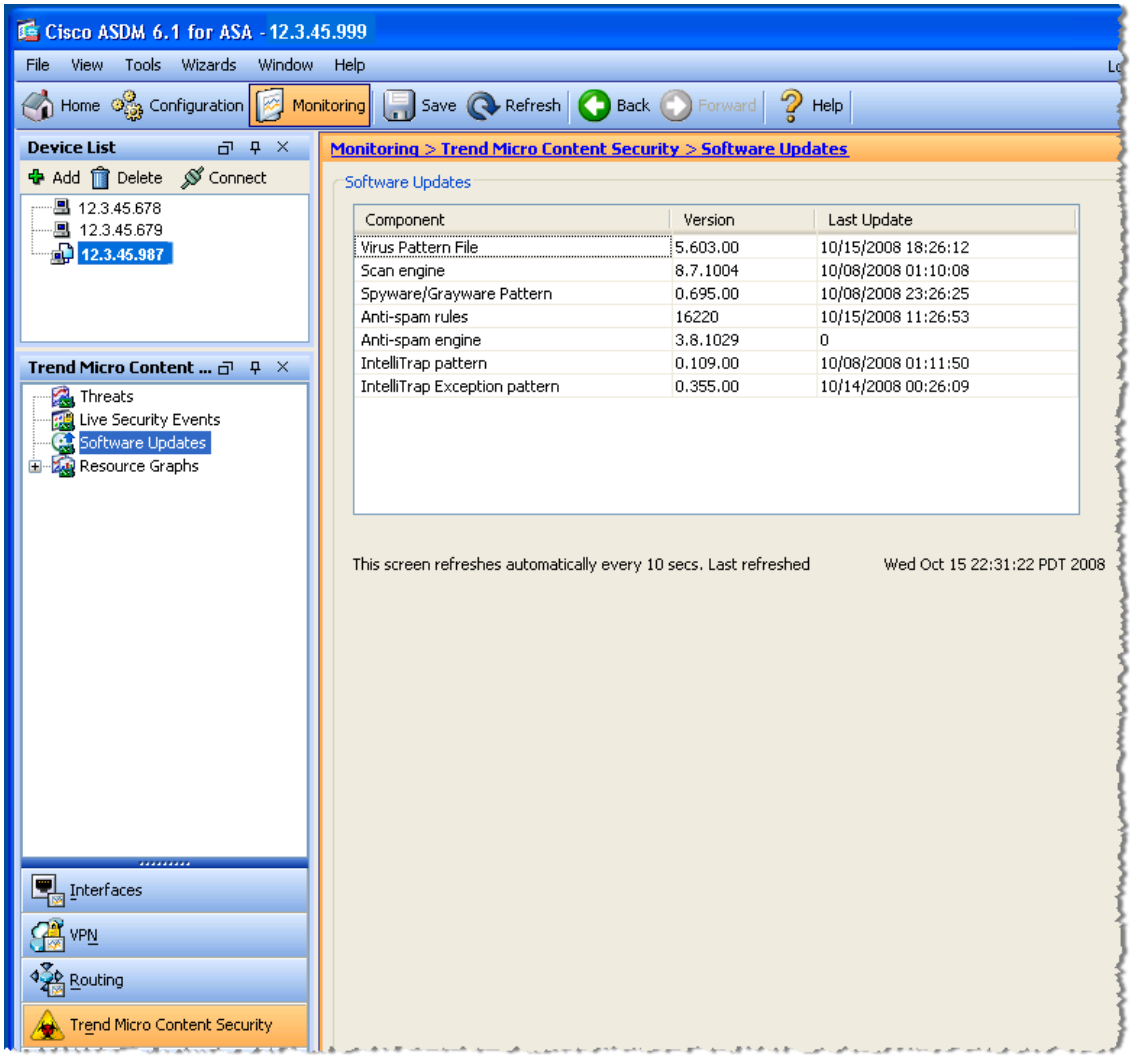
Monitoring Software Updates

To monitor software updates, perform the following steps:

Step 1 Click **Software Updates** in the Monitoring pane, as shown in Figure 7-5.

The component name, version number, and the date and time that the CSC SSM software was last updated appears.

Figure 7-5 Software Updates Window



Step 2 To display the Scheduled Update window shown in Figure 7-6, choose **Configuration > Trend Micro Content Security > Updates**.

Figure 7-6 Scheduled Updates in ASDM

Step 3 Click the **Configure Updates** link to access the Scheduled Update window in CSC SSM. For an example, see Figure 2-4 on page 2-5.

The Scheduled Update window allows you to specify the interval at which CSC SSM receives component updates from the Trend Micro ActiveUpdate server, which can be daily, hourly, or every 15 minutes.

You can also update components on demand via the Manual Update window in the CSC SSM console. For an example, see Figure 5-1 on page 5-2. For more information about both types of updates, see the online help.

Monitoring Resources

To monitor resources, perform the following steps:

Step 1 Click **Resource Graphs** in the Monitoring pane. You can monitor two types of resources: CPU usage and memory. If these resources are being used at almost 100%, you can do one of the following:

- Upgrade to ASA-SSM-20 (if you are currently using ASA-SSM-10).
- Purchase another adaptive security appliance.

Step 2 To view CPU or memory usage, select the information and click **Show Graphs**, as shown in Figure 7-7.

Figure 7-7 Memory Monitoring Graphs