CHAPTER 5

Managing Updates and Log Queries

This chapter describes how to manage component updates, proxy and syslog message settings, and log queries, and includes the following sections:

Updating Components

New viruses and other security risks are released on the global computing community via the Internet or other distribution means at various times. TrendLabs[SM] immediately analyzes a new threat, and takes appropriate steps to update the components required to detect the new threat, such as the virus pattern file. This quick response enables Trend Micro InterScan for Cisco CSC SSM to detect, for example, a new worm that was launched from the computer of a malicious hacker in Amsterdam at 3:00 A.M. in the morning.

It is critical that you keep your components up-to-date to ensure that new threats do not penetrate your network. To accomplish this, you can do the following:

- Perform a manual update of the components at any time, on demand.
- Set up an update schedule that automatically updates the components on a periodic basis.

The managed components, either manually or via a schedule, are the following:

- The virus pattern file
- The virus scan engine
- The spyware pattern file (also includes patterns for other types of grayware)
- The PhishTrap pattern file
- Anti-spam rules
- The anti-spam engine
- IntelliTrap pattern
- IntelliTrap exception pattern

The PhishTrap pattern file, anti-spam rules, and anti-spam engine are active and updated only if you have purchased the Plus License.

To find out whether you have the most current components installed, go to the Manual Update window and check the component status.

Note The CSC SSM software does not support rollback of these updates for either the scan engine or the pattern file.

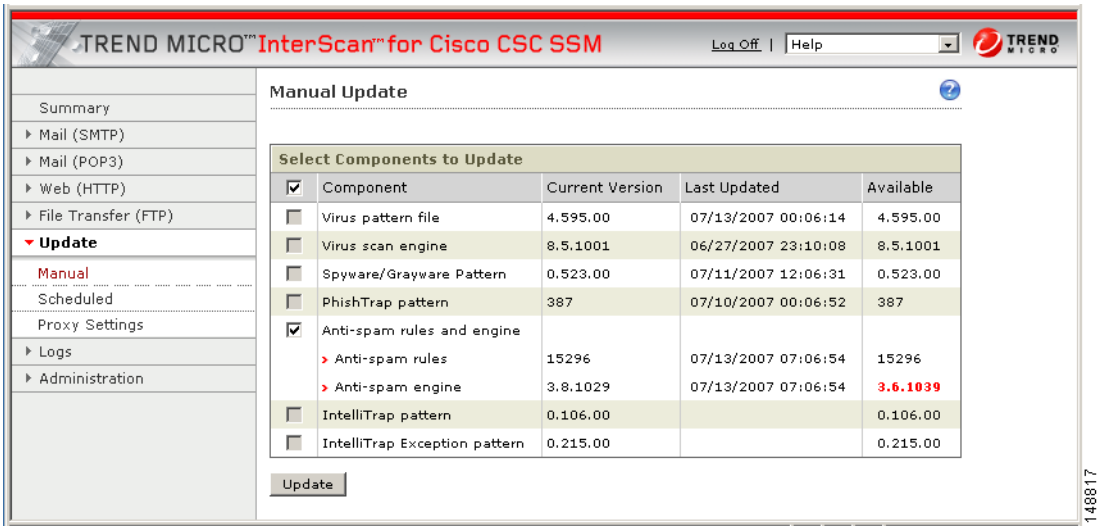
Manual Update

To view component status or update components manually, perform the following steps:

Step 1 Choose **Update > Manual**.

The Manual Update window displays (shown in Figure 5-1).

Figure 5-1 Manual Update Window



To view the component status, check the Available column on the right side of the window. If a more current component is available, the component version displays in red.

Step 2 Click **Update** to download the latest pattern file version.

A progress message displays while the new pattern is downloading. When the update is complete, the Manual Update window refreshes, showing that the latest update has been applied.

See the online help for more information about this feature.

Scheduled Update

You can configure component updates to occur as frequently as every 15 minutes.

To schedule component updates, perform the following steps:

Step 1 Choose **Update > Scheduled** to view the Scheduled Update window.

Step 2 Choose the components to be updated according to the update schedule.

Step 3 Make the desired schedule changes.

Step 4 Click **Save** to update the configuration.

See the online help for more information about this feature.

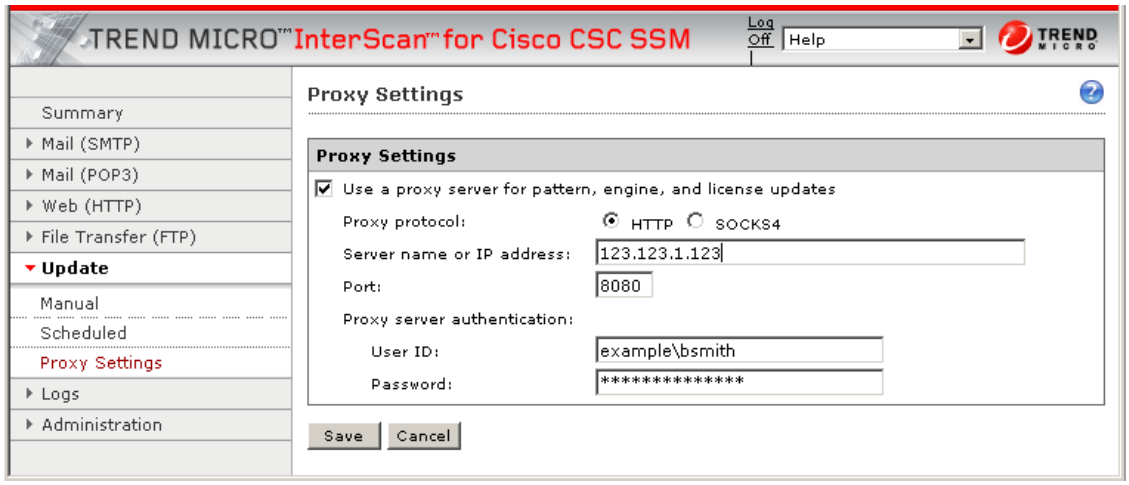
Configuring Proxy Settings

If you are using a proxy server to communicate with the Trend Micro ActiveUpdate server, you must specify a proxy server IP and port during installation.

To configure proxy settings, perform the following steps:

Step 1 To view current proxy server settings on the Proxy Settings window (shown in Figure 5-2), choose **Update > Proxy Settings**.

Figure 5-2 Proxy Settings Window



Step 2 If you set up a proxy server during installation, the HTTP proxy protocol is configured by default. To change the proxy protocol to SOCKS4, click the **SOCKS4** radio button.

Step 3 If needed, add an optional proxy authentication username and password in the User ID and Password fields.

Step 4 Click **Save** to update the configuration when you are finished.

See the online help for more information about this feature.

Configuring System Log Message Settings

After installation, log data such as virus and spyware or grayware detection are saved temporarily. To store log data, you must configure at least one syslog server. You may configure up to three syslog servers.

To configure system log messages, perform the following steps:

Step 1 Choose **Logs > Settings** to display the Log Settings window.

Step 2 Configure at least one syslog server. Check **Enable**, and then enter the syslog server IP address, port, and preferred protocol (either UDP or TCP).

Step 3 Click **Save**.

See the online help for more information about this feature.

By default, detected security risks are logged. You can turn off logging for features you are not using. For example, if you purchased a Plus License, but do not want to log data for URL blocking/ anti-phishing and URL filtering, uncheck those options.

For information about choosing and viewing log data, see the "Viewing Log Data" section on page 5-4. System log messages are also viewable from the ASDM. For more information, see the ASDM online help.

Viewing Log Data

After you have installed and configured Trend Micro InterScan for Cisco CSC SSM, security risks are being detected and acted upon according to the settings you chose for each type of risk. These events are recorded in the logs. To conserve system resources, you need to purge these logs periodically.

To view log data, perform the following steps:

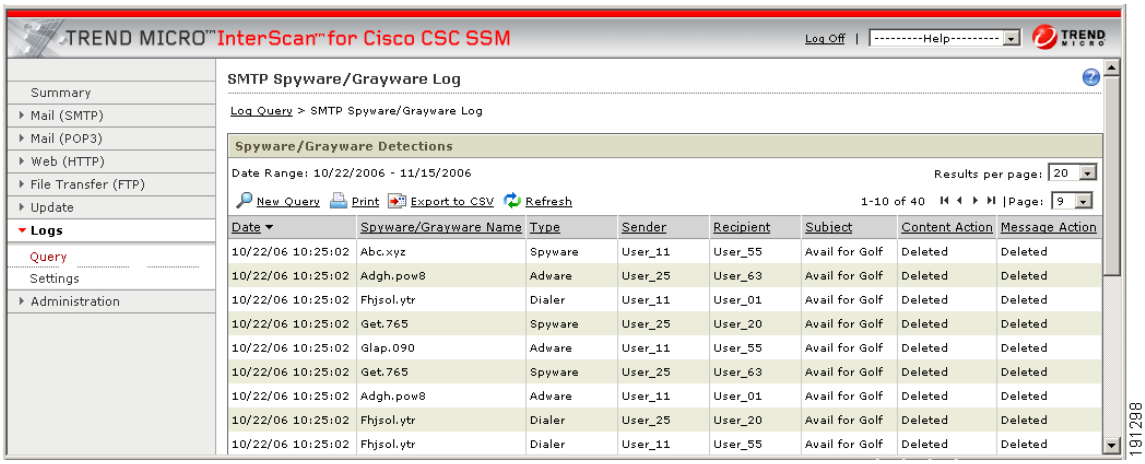
Step 1 Choose **Logs > Query** to display the Log Query window.

Step 2 Specify the inquiry parameters and click **Display Log** to view the log.

See the online help for more information about this feature and exporting logs.

Figure 5-3 shows an example of the SMTP spyware and grayware log.

Figure 5-3 SMTP Spyware/Grayware Log



Logging of Scanning Parameter Exceptions

Exceptions to the scanning parameters are specified in the following locations:

- Mail (SMTP)> Scanning > Incoming/Target tab
- Mail (SMTP)> Scanning > Outgoing/Target tab
- Mail (POP3) > Scanning/Target tab
- Web (HTTP) > Scanning/Target tab
- File Transfer (FTP) > Scanning/Target tab

Exceptions to the following scanning parameters display in the Virus/Malware log. For SMTP, POP3, HTTP, and FTP, the exceptions are as follows:

- Compressed files that when decompressed, exceed the specified file count limit.
- Compressed files that when decompressed, exceed the specified file size limit.
- Compressed files that exceed the number of layers of compression limit.
- Compressed files that exceed the compression ratio limit (the size of the decompressed files is “x” times the size of the compressed file).
- Password-protected files (if configured for deletion).

For HTTP and FTP only, an additional exception is files or downloads that are too large for scanning.

In place of the virus or malware name, these files are identified with messages similar to the following:

```
Decompressed_File_Size_Exceeded
Large_File_Scanning_Limit_Exceeded
```