CHAPTER 4

Configuring Web (HTTP) and File Transfer (FTP) Traffic

This chapter describes how to make HTTP and FTP traffic configuration updates, and includes the following sections:

Default Web and FTP Scanning Settings

After installation, by default your HTTP and FTP traffic is scanned for viruses, worms, and Trojans. Malware such as spyware and other grayware require a configuration change before they are detected. Table 4-1 summarizes the web and file transfer configuration settings, and the default values that are in effect after installation.

Table 4-1 Default Web and FTP Scanning Settings

Feature	Default Setting
Web (HTTP) scanning of file downloads	Enabled using All Scannable Files as the scanning method.
Webmail scanning	Configured to scan Webmail sites for Yahoo, AOL, MSN, and Google.
File transfer (FTP) scanning of file transfers	Enabled using All Scannable Files as the scanning method.

Table 4-1 Default Web and FTP Scanning Settings (continued)

Feature	Default Setting
Web (HTTP) compressed file handling for downloading from the Web File transfer (FTP) compressed file handling for file transfers from an FTP server	Configured to skip scanning of compressed files when one of the following is true: • Decompressed file count is greater than 200. • Decompressed file size exceeds 30 MB. • Number of compression layers exceeds three. • Decompressed or compressed file size ratio is greater than 100 to 1.
Web (HTTP) and file transfer (FTP) large file handling (do not scan files larger than a specified size) Enabled deferred scanning of files larger than a specified size	Configured to skip scanning of files larger than 50 MB. Configured to enable deferred scanning of files larger than 2 MB.
Web (HTTP) downloads and file transfers (FTP) for files in which malware is detected	Clean the downloaded file or file in which the malware was detected. If uncleanable, delete the file.
Web (HTTP) downloads and file transfers (FTP) for files in which spyware or grayware is detected	Files are deleted.
Web (HTTP) downloads when malware is detected	An inline notification is inserted in the browser, stating that Trend Micro InterScan for CSC SSM has scanned the file you are attempting to transfer, and has detected a security risk.
File transfers (FTP) notification	The FTP reply has been received.

These default settings give you some protection for your Web and FTP traffic after you install Trend Micro InterScan for Cisco CSC SSM. You may change these settings. For example, you may prefer to use the Scan by specified file extensions option rather than All Scannable Files for malware detection. Before making changes, review the online help for more information about these selections.

After installation, you may want to update additional configuration settings to obtain the maximum protection for your Web and FTP traffic. If you purchased the Plus License, which entitles you to receive URL blocking, anti-phishing, and URL filtering functionality, you must configure these additional features.

Downloading Large Files

The Target tabs on the HTTP Scanning and FTP Scanning windows allow you to define the size of the largest download you want scanned. For example, you might specify that a download under 20 MB is scanned, but a download larger than 20 MB is not scanned.

In addition, you can:

- Specify large downloads to be delivered without scanning, which may introduce a security risk.
- Specify that downloads greater than the specified limit are deleted.

By default, the CSC SSM software specifies that files smaller than 50 MB are scanned, and files 50 MB and larger are delivered without scanning to the requesting client.

Deferred Scanning

The deferred scanning feature is not enabled by default. When enabled, this feature allows you to begin downloading data without scanning the entire download. Deferred scanning allows you to begin viewing the data without a prolonged wait while the entire body of information is scanned.

Caution When deferred scanning is enabled, the unscanned portion of information can introduce a security risk.

If deferred scanning is not enabled, the entire content of the download must be scanned before it is presented to you. However, some client software may time out because of the time required to collect sufficient network packets to compose complete files for scanning. The following table summarizes the advantages and disadvantages of each method.

Method	Advantage	Disadvantage
Deferred scanning enabled	Prevents client timeouts	May introduce a security risk
Deferred scanning disabled	Safer. The entire file is scanned for security risks before being presented to you.	May result in the client timing out before the download is complete

Note Traffic moving via HTTPS cannot be scanned for viruses and other threats by the CSC SSM software.

Detecting Spyware and Grayware

Grayware is a category of software that may be legitimate, unwanted, or malicious. Unlike threats such as viruses, worms, and Trojans, grayware does not infect, replicate, or destroy data, but it may violate your privacy. Examples of grayware include spyware, adware, and remote access tools.

Spyware or grayware detection is not enabled by default. To detect spyware and other forms of spyware and other grayware in your Web and file transfer traffic, you must configure this feature in the following windows:

- Web (HTTP) > Scanning > HTTP Scanning/Target
- File Transfer (FTP) > Scanning > FTP Scanning/Target

To configure web scanning, do the following:

On the Configuration > Trend Micro Content Security > Web window in ASDM, click the **Configure Web Scanning** link.

To configure FTP scanning, do the following:

On the Configuration > Trend Micro Content Security > File Transfer window in ASDM, click the **Configure File Scanning** link.

For more information, see the "Enabling SMTP and POP3 Spyware and Grayware Detection" section on page 3-3 and the online help for these windows.

Scanning Webmail

As specified in Table 4-1, Webmail scanning for Yahoo, AOL, MSN, and Google is already configured by default.

Caution If you elect to scan only Webmail, HTTP scanning is restricted to the sites specified on the Webmail Scanning tab of the Web (HTTP) > Scanning > HTTP Scanning window. Other HTTP traffic is not scanned. Configured sites are scanned until you remove them by clicking the **Trashcan** icon.

To add additional sites, perform the following steps:

Step 1 On the Configuration > Trend Micro Content Security > Web window in ASDM, click the **Configure Web Scanning** link.

The Target tab of the HTTP Scanning window appears.

Step 2 Click the **Webmail Scanning** tab.

Step 3 In the Name field, define the Webmail site by entering the exact website name, a URL keyword, and a string.

Note Attachments to messages that are managed via Webmail are scanned.

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

For more information about how to configure additional Webmail sites for scanning, see the online help.

File Blocking

This feature is enabled by default; however, you must specify the types of files you want blocked. File blocking helps you enforce your organization policies for Internet use and other computing resources during work time. For example, your company does not allow downloading of music, both because of legal issues as well as employee productivity issues.

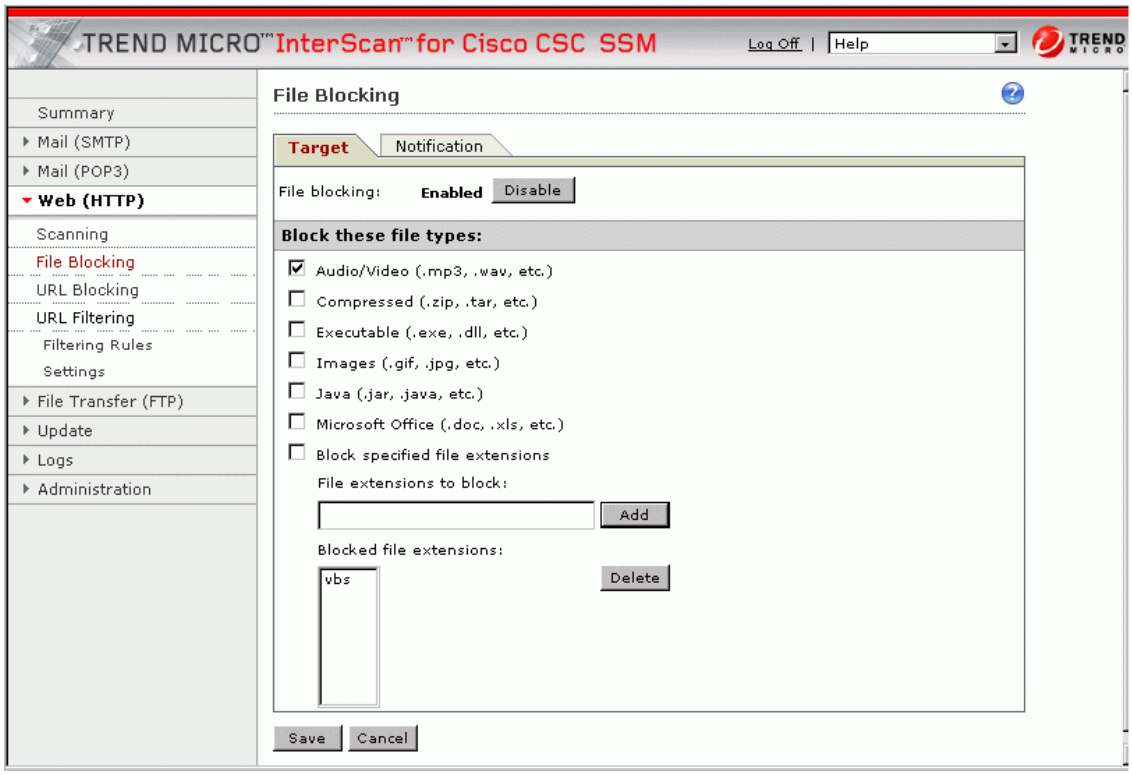
To configure file blocking, perform the following steps:

Step 1 To block downloads via HTTP, on the Configuration > Trend Micro Content Security > Web window in ASDM, click the **Configure File Blocking** link to display the File Blocking window.

Step 2 To block downloads via FTP, on the Configuration > Trend Micro Content Security > File Transfer window in ASDM, click the **Configure File Blocking** link.

Step 3 To block transferring of music files, on the Target tab of the File Blocking window, check the **Audio/Video** check box, as shown in Figure 4-1.

Figure 4-1 Enable File Blocking



Step 4 You can specify additional file types by file name extension. To enable this feature, check the **Block specified file extensions** check box.

Step 5 Then enter additional file types in the File extensions to block field, and click **Add**. In the example, .vbs files are blocked.

For more information about file blocking and for information about deleting file extensions you no longer want to block, see the online help.

Step 6 To view the default notification that displays in the browser or FTP client when a file blocking event is triggered, click the **Notifications** tab of the File Blocking window.

Step 7 To customize the text of these messages, select and redefine the default message. An optional notification to the administrator is available for HTTP file-blocking events, but is turned off by default. Check the **Send the following message** check box to activate the notification.

Step 8 Click **Save** when you are finished to update the configuration.

URL Blocking

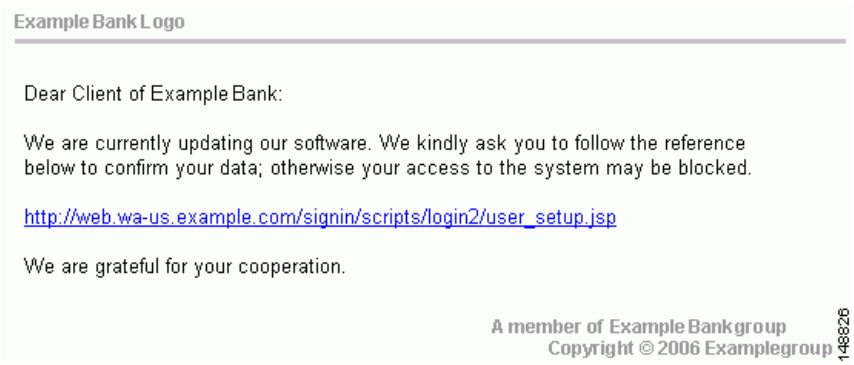
This section describes the URL blocking feature, and includes the following topics:

The URL blocking feature helps you prevent employees from accessing prohibited websites. For example, you may want to block some sites because policies in your organization prohibit access to dating services, online shopping services, or offensive sites.

Note This feature requires the Plus License.

You may also want to block sites that are known for perpetrating fraud, such as phishing. Phishing is a technique used by criminals who send e-mail messages that appear to be from a legitimate organization, which request revealing private information such as bank account numbers. Figure 4-2 shows an example of an e-mail message used for phishing.

Figure 4-2 Example of Phishing



By default, URL blocking is enabled. However, only sites in the TrendMicro PhishTrap pattern file are blocked until you specify additional sites for blocking.

Blocking from the Via Local List Tab

To configure URL blocking from the Via Local List tab, perform the following steps:

Step 1 On the Configuration > Trend Micro Content Security > Web window in ASDM, click **Configure URL Blocking** to display the URL Blocking window.

Step 2 On the Via Local List tab of the URL Blocking window, type the URLs you want to block in the Match field. You can specify the exact website name, a URL keyword, and a string.

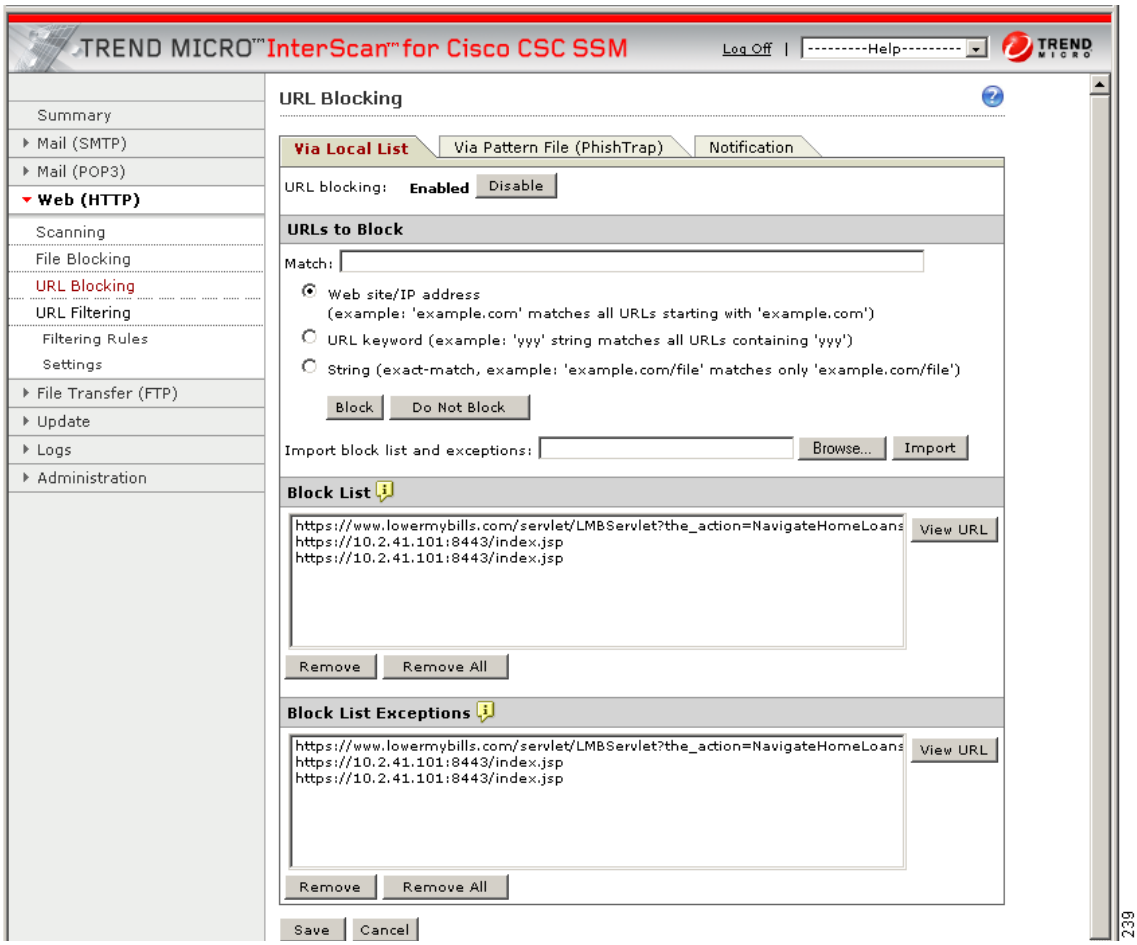
See the online help for more information about formatting entries in the Match field.

Step 3 To move the URL to the Block List, click **Block** after each entry. To specify your entry as an exception, click **Do Not Block** to add the entry to Block List Exceptions. Entries remain as blocked or exceptions until you remove them.

Note You can also import a block and exception list. The imported file must be in a specific format. See the online help for instructions.

Figure 4-3 shows an example of the URL Blocking window.

Figure 4-3 URL Blocking Window



Blocking from the Via Pattern File (PhishTrap) Tab

To configure URL file blocking from the Via Pattern File (Phishtrap) Tab, perform the following steps:

Step 1 On the Configuration > Trend Micro Content Security > Web window in ASDM, click the **Configure URL Blocking** link to display the URL Blocking window.

Step 2 Then click the **Via Pattern File (PhishTrap)** tab.

Step 3 By default, the Trend Micro PhishTrap pattern file detects and blocks known phishing sites, spyware sites, virus accomplice sites (sites associated with known exploits), and disease vectors (websites that exist only for malicious purposes). To submit sites that you think should be added to the PhishTrap pattern file, use the **Submit the Potential Phishing URL to TrendLabs** fields. TrendLabs evaluates the site and may add the site to this file if such action is warranted.

Step 4 To review the text of the default message that appears in the browser when an attempt is made to access a blocked site, click the **Notification** tab. The online help shows an example. Customize the default message by highlighting and redefining it.

Step 5 Click **Save** when you are finished to update the configuration.

URL Filtering

This section describes how to configure the URL filtering feature, and includes the following topics:

The URLs defined on the URL Blocking windows described previously are either always allowed or always disallowed. The URL filtering feature, however, allows you to filter URLs in categories, which you can schedule to allow access during certain times (defined as leisure time) and disallow access during work time.

Note This feature requires the Plus License.

There are six URL filtering categories as follows:

- Company-prohibited
- Not work related
- Research topics
- Business function
- Customer defined
- Others

By default, company-prohibited sites are blocked during both work and leisure times.

Filtering Settings

To configure the URL filtering feature, perform the following steps:

Step 1 On the Configuration > Trend Micro Content Security > Web window in ASDM, click **Configure URL Filtering Settings** to display the URL Filtering Settings window.

Step 2 On the URL Categories tab, review the subcategories listed and the default classifications assigned to each category to see whether the assignments are appropriate for your organization. For example, “Illegal Drugs” is a subcategory of the “Company-prohibited” category. If your organization is a financial services company, you may want to leave this category classified as company-prohibited. Check the **Illegal Drugs** check box to enable filtering for sites related to illegal drugs. However, if your organization is a law enforcement agency, you should reclassify the “Illegal Drugs” subcategory to the “Business function” category. See the online help for more information about reclassification.

Step 3 After you have reviewed and refined the subcategory classifications, check the associated subcategory to enable all the subcategories for which you want filtering performed.

Step 4 If there are sites within some of the enabled subcategories that you do not want filtered, click the **URL Filtering Exceptions** tab.

Step 5 Type the URLs you want to exclude from filtering in the Match field. You can specify the exact website name, a URL keyword, and a string.

See the online help for more information about formatting entries in the Match field.

Step 6 To move the URL to the Do Not Filter the Following Sites list, click **Add** after each entry. Entries remain as exceptions until you remove them.

Note You can also import an exception list. The imported file must be in a specific format. See the online help for instructions.

Step 7 Click the **Schedule** tab to define the days of the week and hours of the day that should be considered work time. Time not designated as work time is automatically designated as leisure time.

Step 8 Click **Save** to update the URL filtering configuration.

Step 9 Click the **Reclassify URL** tab to submit suspect URLs to TrendLabs for evaluation.

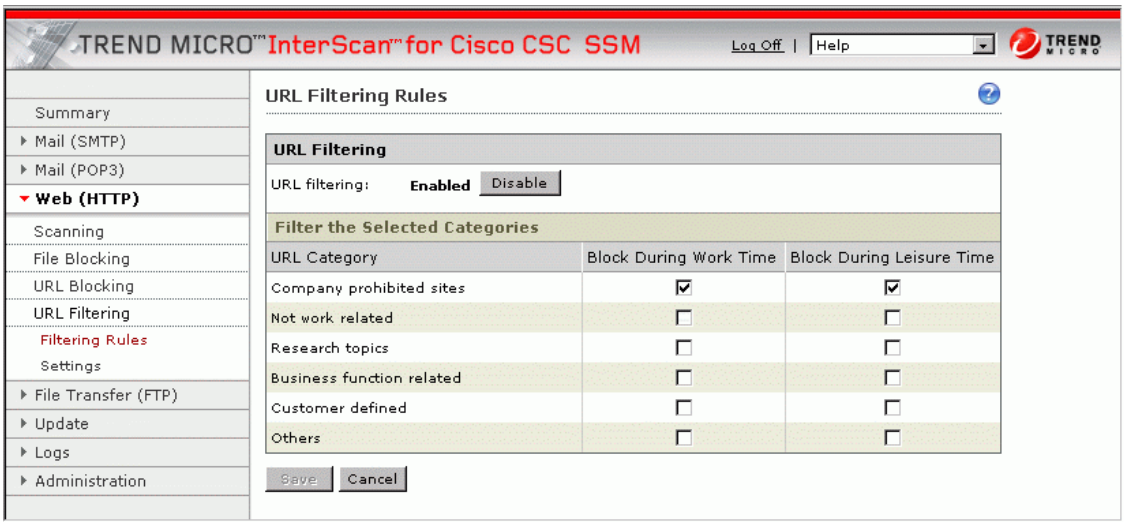
Filtering Rules

After you have assigned the URL subcategories to correct categories for your organization, defined exceptions (if any), and created the work and leisure time schedule, assign the filtering rules that determine when a category is filtering.

To assign the URL filtering rules, perform the following steps:

Step 1 On the Configuration > Trend Micro Content Security > Web window in ASDM, click the **Configure URL Filtering Rules** link to display the URL Filtering Rules window, shown in Figure 4-4.

Figure 4-4 URL Filtering Rules Window



Step 2 For each of the six major categories, specify whether the URLs in that category are blocked, and if so, during work time, leisure time, or both. See the online help for more information.

Step 3 Click **Save** to update the configuration.

Note For URL Filtering to work correctly, the CSC SSM module must be able to send HTTP requests to the Trend Micro service. If an HTTP proxy is required, configure the proxy setting by choosing **Update** > **Proxy Settings**. The URL Filtering component does not support the SOCKS4 proxy.