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, your HTTP and FTP traffic is scanned by default for viruses, worms, and Trojans. Malware, such as spyware and other grayware, require a configuration change before they are detected. If you have a Plus License, you can block or allow URLs classified as phishing sites during work or leisure time.

Note Some categories, such as pornography, are blocked by default. Customers should review the categories blocked by default and make the appropriate adjustments. With a Plus License for URL Filtering and Blocking, URLs can be blocked with both global and/or user/group policies.

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 Hotmail, and Google.
File transfer (FTP) scanning of file transfers	Enabled using All Scannable Files as the scanning method.
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 500. • 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 (no scanning of 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 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 CSC SSM. You may change these settings. For example, you may want to scan by the "Specified file extensions" option instead of by the "All Scannable Files" option 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. You must configure these additional features if you purchased the Plus License, which entitles you to receive Web Reputation, URL blocking, and URL Filtering functionality (for both global and user/group policies).

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 extra time required to collect sufficient network packets to compose complete files for scanning. Table 4-1 summarizes the advantages and disadvantages of each method.

Table 4-2 Deferred Scanning Safety Comparison

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.

When the file is eventually scanned by CSC SSM, it may be found to contain malicious content. If so, CSC SSM takes following action:

- Sends a notification message, provided notifications are enabled
- Logs the event details
- Automatically blocks the URL from other users for four hours after malicious code detection. Access to the URL is restored after four hours elapses, and content from it will be scanned

If CSC SSM has been registered to a Damage Cleanup Services (DCS) server, a DCS clean-up request is issued under one of the following conditions:

- Someone (usually using a client PC) attempts to access a URL classified as Spyware, Disease Vector, or Virus Accomplice through URL Filtering (requires a Plus License).
- Someone (usually using a client PC) uploads a virus classified as a "worm."

DCS connects to the client to clean the file. For more information about DCS, see Appendix D, "Using CSC SSM with Trend Micro Damage Cleanup Services".

Spyware and Grayware Detection and Cleaning

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 creates two main problems to network administrators. It can compromise sensitive company information and reduce employee productivity by causing infected machines to malfunction. In addition to detecting and blocking incoming files that may install spyware, CSC SSM can prevent installed spyware from sending confidential data via HTTP.

If a client tries to access a URL classified as Spyware, Disease Vector, or Virus Accomplice, or a client PC uploads a virus classified as a worm as a webmail attachment, CSC SSM can send a request to Trend Micro Damage Cleanup Services (DCS) to clean the infected machine. DCS reports the outcome of the cleaning attempt (either successful or unsuccessful) to the CSC SSM server.

If the cleaning attempt is not successful, the client's browser is redirected to a special DCS-hosted cleanup page the next time the browser tries to access the Internet. This page contains an ActiveX control that again tries to clean the infected machine. If access permissions were the reason for the first failed cleaning attempt, the ActiveX control may be successful where cleaning via remote logon was unsuccessful.

For more information about DCS, see Using CSC SSM with Trend Micro Damage Cleanup Services, page D-1.

Note To avoid excessive cleanup attempts, CSC SSM only sends requests to clean up a target IP address once every four hours by default. If the client at that IP address continues to perform suspicious actions, then no further cleanup requests will be issued until this lockout period has expired. You can modify the length of this lockout period by going to `/opt/trend/isvw/config/web/intscan.ini` on the CSC SSM and changing the value of the `[DCS]/cleanup_lockout_hours` field. The value in this field is interpreted as the number of hours, and partial values (such as 0.5) are supported.

Detecting Spyware and Grayware

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 3-4 and the online help for these windows.

Scanning Webmail

As specified in Table 4-1, Webmail scanning for Yahoo, AOL, MSN Hotmail, 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 from scanning 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, enter a name for the Webmail site.

Step 4 In the Match field, enter the exact website name/IP address, a URL keyword, and a string.

Step 5 Choose the appropriate radio button to correspond with the text entered in the Match field.

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

Step 6 Click **Add**.

Step 7 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.

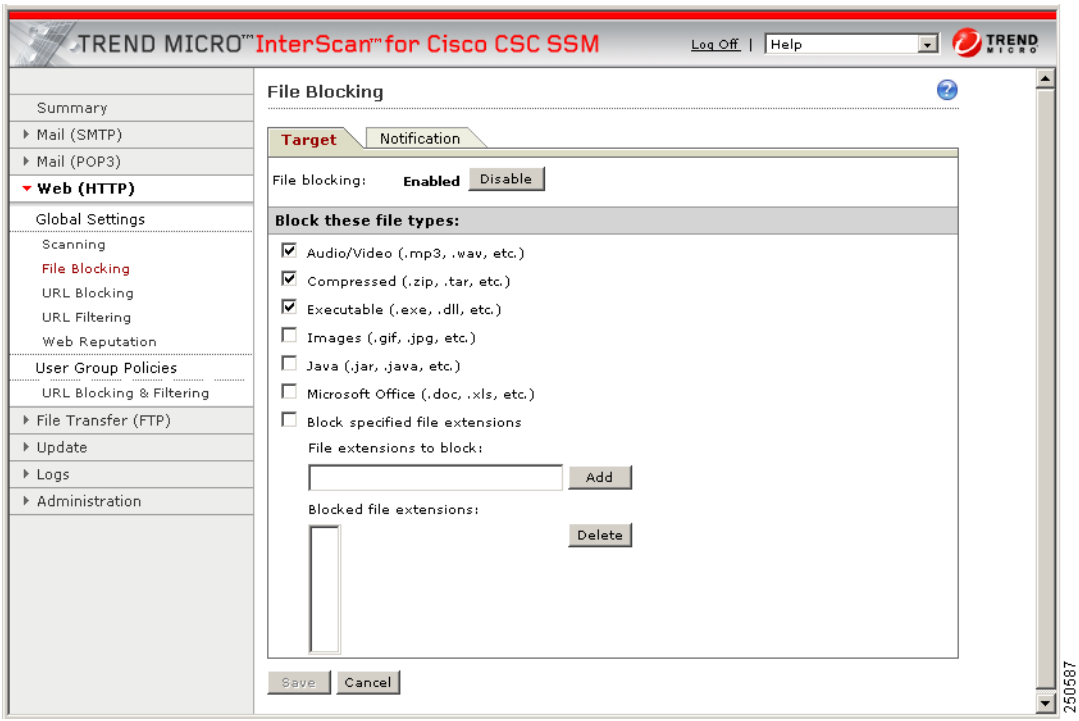
To configure file blocking, perform the following steps:

Step 1 To block downloads over 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 over 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**.

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

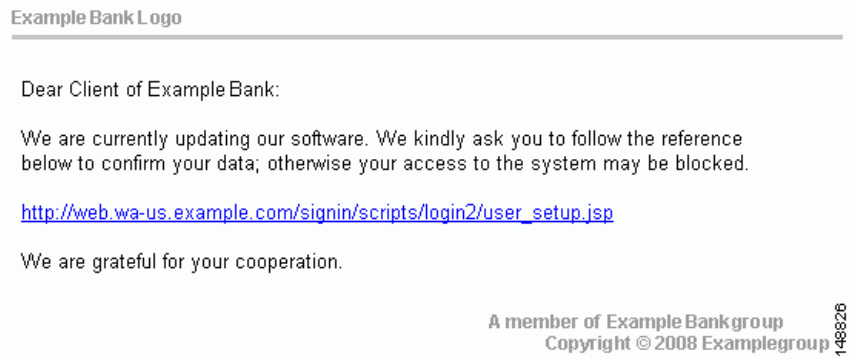
This section describes the URL blocking feature, and includes the following topics:

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. URL blocking policies, set by going to Web (HTTP) > Global Settings > URL Blocking, affect all users. URL blocking policies can also be set for specific users or groups. For more information, see the "URL Blocking and Filtering Policies for Users/Groups" section on page 4-21.

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 (including blocking URLs based on user group policies).

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. (See Figure 4-3.)

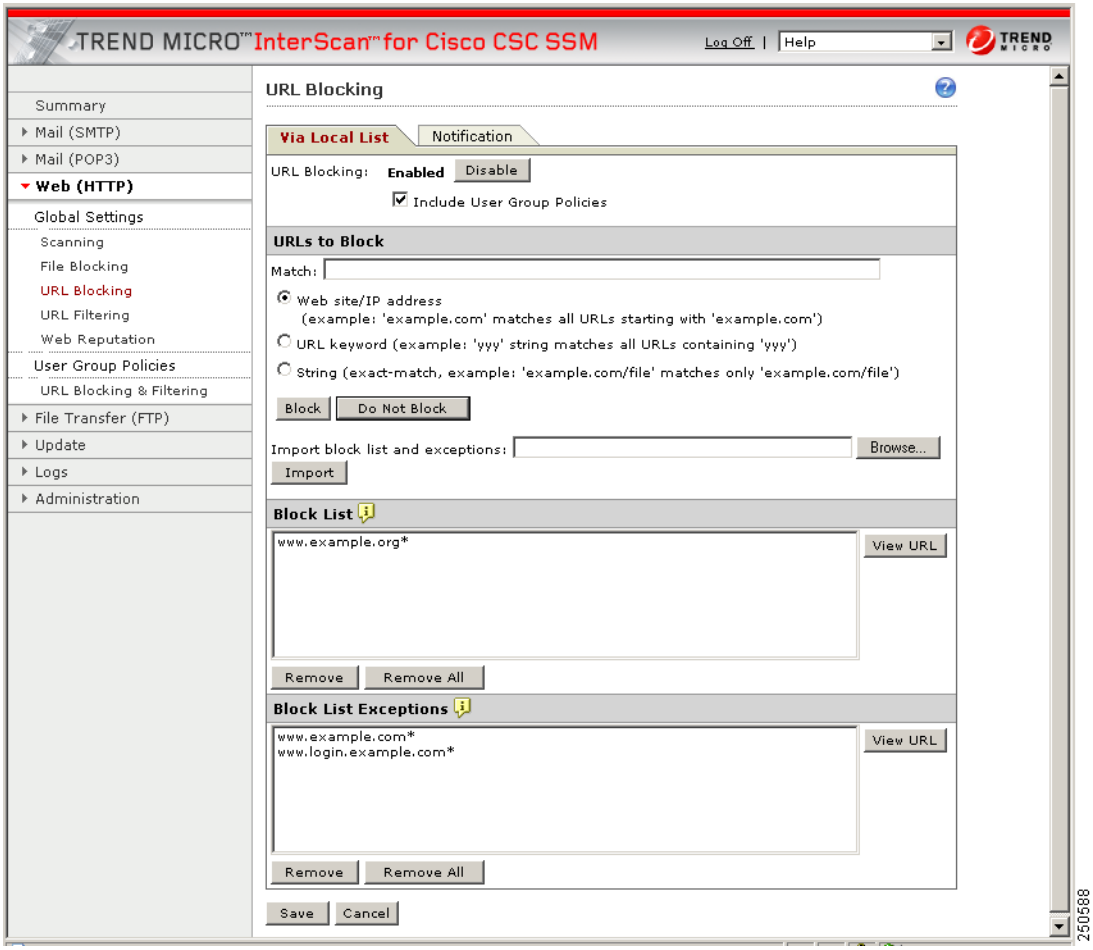
Step 2 On the Via Local List tab of the URL Blocking window, type the URLs you want to block in the Match field. You can specify the exact website name/IP address, a URL keyword, or a string.

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.

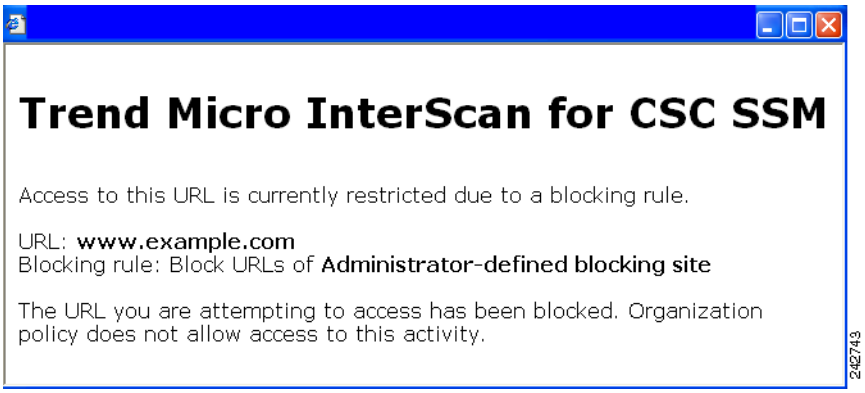
Figure 4-3 URL Blocking Window



URL Blocking Notifications

A configurable message informs the end user when CSC SSM detects an attempt to access a blocked URL via HTTP. A default notification message is provided, but other text and variables can be used to create a custom message. URL Blocking and URL Filtering use the same notification message.

Figure 4-4 URL Blocking and Filtering Default Notification Message



To configure the notification message, 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 Notification tab of the URL Blocking window, type your custom message.

Step 3 Use the variables or tokens listed in the online help to customize your message.

Step 4 Click **Restore Default** to return to the default message.

Step 5 Click **Save** to save your work in this screen.

URL Filtering

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, such as leisure and work time. URL filtering policies set by going to Web (HTTP) > Global Settings > URL Filtering affect all users. URL filtering policies can also be set for specific users or groups. For more information, see the "URL Blocking and Filtering Policies for Users/Groups" section on page 4-21.

Note This feature requires the Plus License.

URL categories are organized into the URL filtering groups shown in Table 4-3.

Table 4-3 Grouping Definition for URL Categories

Category Group	Description
Adult	Sites that may be considered inappropriate for children
Business	Sites related to business, employment, or commerce
Communications and Search	Sites that provide tools and services for online communications and search
General	Sites not classified in other category groups, including unrated sites

Table 4-3 Grouping Definition for URL Categories (continued)

Category Group	Description
Internet Security	Potentially harmful sites, including sites known to have malware
Lifestyle	Sites about lifestyle preferences, including sexual, political, or religious orientations, as well as recreation and entertainment
Network Bandwidth	Sites that offer services that can significantly impact available network bandwidth

Note For URL Filtering to work correctly, the CSC SSM 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**.

URL Filtering Categories

Table 4-4 lists definitions of the URL Filtering categories and the assigned group.

Table 4-4 URL Filtering Category Definitions

Category Group	Category Type	Category Definition
Adult	Abortion	Sites that promote, encourage, or discuss abortion, including sites that cover moral or political views on abortion
Adult	Adult/Mature Content	Sites with profane or vulgar content generally considered inappropriate for minors; includes sites that offer erotic content or ads for sexual services, but excludes sites with sexually explicit images
Adult	Alcohol/Tobacco	Sites that promote, sell, or provide information about alcohol or tobacco products
Adult	Gambling	Sites that promote or provide information on gambling, including online gambling sites
Adult	Illegal Drugs	Sites that promote, glamorize, supply, sell, or explain how to use illicit or illegal intoxicants
Adult	Illegal/Questionable	Sites that promote and discuss how to perpetrate “nonviolent” crimes, including burglary, fraud, intellectual property theft, and plagiarism; includes sites that sell plagiarized or stolen materials
Adult	Intimate Apparel/ Swimsuit	Sites that sell swimsuits or intimate apparel with models wearing them
Adult	Marijuana	Sites that discuss the cultivation, use, or preparation of marijuana, or sell related paraphernalia
Adult	Nudity	Sites showing nude or partially nude images that are generally considered artistic, not vulgar or pornographic
Adult	Pornography	Sites with sexually explicit imagery designed for sexual arousal, including sites that offer sexual services

Table 4-4 URL Filtering Category Definitions (continued)

Category Group	Category Type	Category Definition
Adult	Sex Education	Sites with or without explicit images that discuss reproduction, sexuality, birth control, sexually transmitted disease, safe sex, or coping with sexual trauma
Adult	Tasteless	Sites with content that is gratuitously offensive and shocking; includes sites that show extreme forms of body modification or mutilation and animal cruelty
Adult	Violence/Hate/ Racism	Sites that promote hate and violence; includes sites that espouse prejudice against a social group, extremely violent and physically dangerous activities, mutilation and gore, or the creation of destructive devices
Adult	Weapons	Sites about weapons, including their accessories and use; excludes sites about military institutions or sites that discuss weapons as sporting or recreational equipment
Business	Auctions	Sites that serve as venues for selling or buying goods through bidding, including business sites that are being auctioned
Business	Brokerage/Trading	Sites about investments in stocks or bonds, including online trading sites; includes sites about vehicle insurance
Business	Business/Economy	Sites about business and the economy, including entrepreneurship and marketing; includes corporate sites that do not fall under other categories
Business	Financial Services	Sites that provide information about or offer basic financial services, including sites owned by businesses in the financial industry
Business	Job Search/Careers	Sites about finding employment or employment services
Business	Real Estate	Sites about real estate, including those that provide assistance selling, leasing, purchasing, or renting property
Business	Shopping	Sites that sell goods or support the sales of goods that do not fall under other categories; excludes online auction or bidding sites
Communica-tions and Search	Blogs/Web Communications	Blog sites or forums on varying topics or topics not covered by other categories; sites that offer multiple types of Web-based communication, such as email or instant messaging
Communica-tions and Search	Chat/Instant Messaging	Sites that provide Web-based services or downloadable software for text-based instant messaging or chat
Communica-tions and Search	Email Related	Sites that provide email services, including portals used by companies for Web-based email
Communica-tions and Search	Infrastructure	Content servers, image servers, or sites used to gather, process, and present data and data analysis, including Web analytics tools and network monitors

Table 4-4 URL Filtering Category Definitions (continued)

Category Group	Category Type	Category Definition
Communications and Search	Internet Telephony	Sites that provide Web services or downloadable software for Voice over Internet Protocol (VoIP) calls
Communications and Search	Newsgroups	Sites that offer access to Usenet or provide other newsgroup, forum, or bulletin board services
Communications and Search	Search Engines/ Portals	Search engine sites or portals that provide directories, indexes, or other retrieval systems for the Web
Communications and Search	Social Networking	Sites devoted to personal expression or communication, linking people with similar interests
Communications and Search	Web Hosting	Sites of organizations that provide top-level domains or Web hosting services
General	Computers/Internet	Sites about computers, the Internet, or related technology, including sites that sell or provide reviews of electronic devices
General	Education	School sites, distance learning sites, and other education-related sites
General	Government/Legal	Sites about the government, including laws or policies; excludes government military or health sites
General	Health	Sites about health, fitness, or well-being
General	Military	Sites about military institutions or armed forces; excludes sites that discuss or sell weapons or military equipment
General	News/Media	Sites about the news, current events, contemporary issues, or the weather; includes online magazines whose topics do not fall under other categories
General	Political	Sites that discuss or are sponsored by political parties, interest groups, or similar organizations involved in public policy issues; includes non-hate sites that discuss conspiracy theories or alternative views on government
General	Reference	General and specialized reference sites, including map, encyclopedia, dictionary, weather, how-to, and conversion sites
General	Translators (circumvent filtering)	Online page translators or cached Web pages (used by search engines), which can be used to circumvent proxy servers and Web filtering systems
General	Unrated	Sites that have not been classified under a category
General	Vehicles	Sites about motorized transport, including customization, procurement of parts and actual vehicles, or repair services; excludes sites about military vehicles

Table 4-4 URL Filtering Category Definitions (continued)

Category Group	Category Type	Category Definition
Internet Security	Adware	Sites with downloads that display advertisements or other promotional content; includes sites that install browser helper objects (BHOs)
Internet Security	Cookies	Sites that send malicious tracking cookies to visiting Web browsers
Internet Security	Dialers	Sites with downloads that dial into other networks or premium-rate telephone numbers without user consent
Internet Security	Disease Vector	Sites that directly or indirectly facilitate the distribution of malicious software or source code
Internet Security	Hacking	Sites that provide downloadable software for bypassing computer security systems
Internet Security	Joke Program	Sites that provide downloadable “joke” software, including applications that can unsettle users
Internet Security	Made for AdSense sites (MFA)	Sites that use scraped or copied content to pollute search engines with redundant and generally unwanted results
Internet Security	Malware/Virus Accomplice	Sites used by malicious programs, including sites used to host upgrades or store stolen information
Internet Security	Password Cracking Application	Sites that distribute password cracking software
Internet Security	Phishing	Fraudulent sites that mimic legitimate sites to gather sensitive information, such as user names and passwords
Internet Security	Potentially Malicious Software	Sites that contain potentially harmful downloads
Internet Security	Proxy Avoidance	Sites about bypassing proxy servers or Web filtering systems, including sites that provide tools for that purpose
Internet Security	Remote Access Program	Sites that provide tools for remotely monitoring and controlling computers
Internet Security	Spam	Sites whose addresses have been found in spam messages
Internet Security	Spyware	Sites with downloads that gather and transmit data from computers owned by unsuspecting users
Internet Security	Web Advertisement	Sites dedicated to displaying advertisements, including sites used to display banner or popup ads
Lifestyle	Activist Groups	Sites that promote change in public policy, public opinion, social practice, economic activities, or economic relationships; includes sites controlled by service, philanthropic, professional, or labor organizations
Lifestyle	Alternative Journals	Online equivalents of supermarket tabloids and other fringe publications
Lifestyle	Arts/Entertainment	Sites that promote or provide information about movies, music, non-news radio and television, books, humor, or magazines

Table 4-4 URL Filtering Category Definitions (continued)

Category Group	Category Type	Category Definition
Lifestyle	Cult/Occult	Sites about alternative religions, beliefs, and religious practices, including those considered cult or occult
Lifestyle	Cultural Institutions	Sites controlled by organizations that seek to preserve cultural heritage, such as libraries or museums; also covers sites owned by the Boy Scouts, the Girl Scouts, Rotary International, and similar organizations
Lifestyle	For Kids	Sites designed for children
Lifestyle	Games	Sites about board games, card games, console games, or computer games; includes sites that sell games or related merchandise
Lifestyle	Gay/Lesbian	Sites about gay, lesbian, transgender, or bisexual lifestyles
Lifestyle	Humor/Jokes	Sites about motorized transport, including customization, procurement of parts and actual vehicles, or repair services; excludes sites about military vehicles
Lifestyle	Personal Websites	Sites maintained by individuals about themselves or their interests; excludes personal pages in social networking sites, blog sites, or similar services
Lifestyle	Personals/Dating	Sites that help visitors establish relationships, including sites that provide singles listings, matchmaking, or dating services
Lifestyle	Recreation/Hobbies	Sites about recreational activities and hobbies, such as collecting, gardening, outdoor activities, traditional (non-video) games, and crafts; includes sites about pets, recreational facilities, or recreational organizations
Lifestyle	Religion	Sites about popular religions, their practices, or their places of worship
Lifestyle	Restaurants/Dining/ Food	Sites that list, review, discuss, advertise, or promote food, catering, dining services, cooking, or recipes
Lifestyle	Society/Lifestyle	Sites that provide information about life or daily matters; excludes sites about entertainment, hobbies, sex, or sports, but includes sites about cosmetics or fashion
Lifestyle	Sport Hunting and Gun Clubs	Sites about gun clubs or similar groups; includes sites about hunting, war gaming, or paintball facilities
Lifestyle	Sports	Sites about sports or other competitive physical activities; includes fan sites or sites that sell sports merchandise
Lifestyle	Travel	Sites about travelling or travel destinations; includes travel booking and planning sites
Network Bandwidth	Internet Radio and TV	Sites that primarily provide streaming radio or TV programming; excludes sites that provide other kinds of streaming content
Network Bandwidth	Pay to Surf	Sites that compensate users who view certain Web sites, email messages, or advertisements or users who click links or respond to surveys

Table 4-4 URL Filtering Category Definitions (continued)

Category Group	Category Type	Category Definition
Network Bandwidth	Peer-to-Peer	Sites that provide information about or software for sharing and transferring files within a peer-to-peer (P2P) network
Network Bandwidth	Personal Network Storage/File Download Servers	Sites that provide personal online storage, backup, or hosting space, including those that provide encryption or other security services
Network Bandwidth	Photo Searches	Sites that primarily host images, allowing users to share, organize, store, or search for photos or other images
Network Bandwidth	Ringtones/Mobile Phone Downloads	Sites that provide content for mobile devices, including ringtones, games, or videos
Network Bandwidth	Software Downloads	Sites dedicated to providing free, trial, or paid software downloads
Network Bandwidth	Streaming Media/ MP3	Sites that offer streaming video or audio content without radio or TV programming; sites that provide music or video downloads, such as MP3 or AVI files

Filtering Rules, Exceptions, and Time

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 Rules** to display the URL Filtering: Rules window.

Step 2 Click **Enable** to enable the URL Filtering feature. (It is enabled by default.)

Step 3 Check the “Include User Group Policies” check box to included User Group Policies, if appropriate.

Step 4 On the Rules tab, review the subcategories listed under each category. (See Figure 4-5.) For example, “Illegal Drugs” is a subcategory of the “Adult” category. If your organization is a financial services company, you may want to filter this category. Check the “Illegal Drugs” check boxes for Work and Leisure time to enable filtering for sites related to illegal drugs. However, if your organization is a law enforcement agency, you should uncheck the “Illegal Drugs” subcategory.

Step 5 For each of the seven groups of categories, specify whether the URLs are blocked, and if so, during work time, leisure time, or both.

Figure 4-5 URL Filtering Rules Tab

Step 6 If you believe a particular URL has been misclassified, you can check the category of the URL and request it be reclassified by clicking the link in the Note section at the bottom of the page.

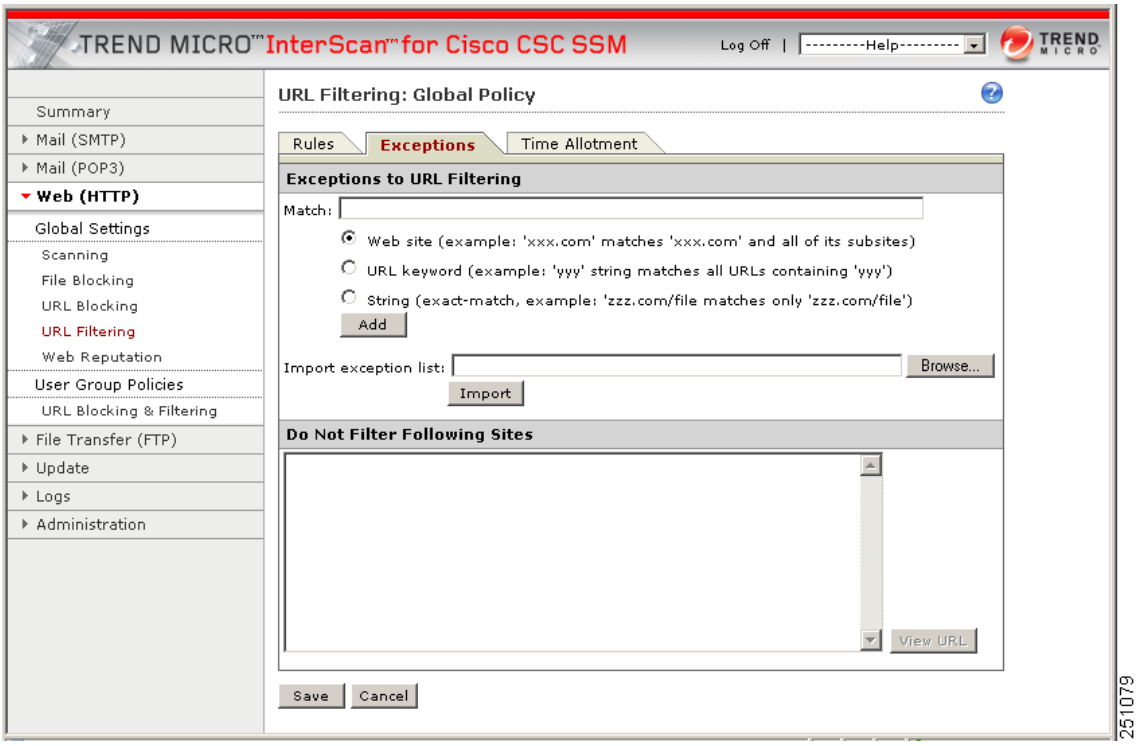
Step 7 If there are sites within the enabled subcategories that you do not want filtered, click the **Exceptions** tab. (See Figure 4-6.)

Step 8 Type the URLs you want to exclude from filtering in the Match field. You can specify the exact website name or IP address, a URL keyword, and a string.

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

Note You can also import a list of URL filtering exceptions. The imported file must be in a specific format. See the online help for instructions.

Figure 4-6 URL Filtering Exceptions Tab



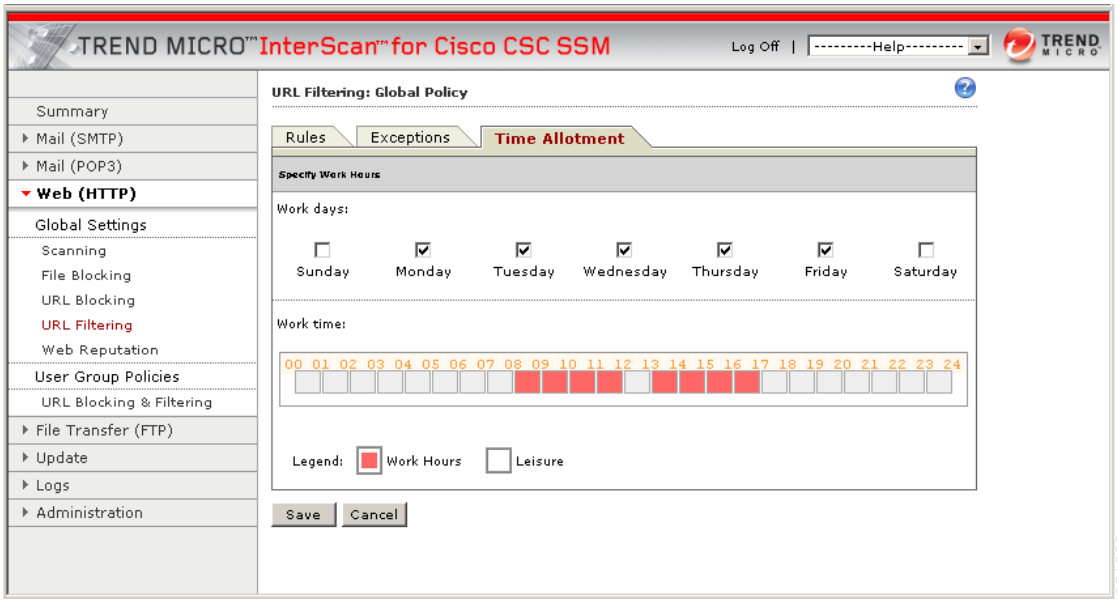
Step 9 Click **Add** after each entry to move it to the "URL to the Do Not Filter the Following Sites" list. Entries remain as exceptions until you remove them.

Step 10 Click the **Time Allotment** tab.

Step 11 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. Figure 4-7 shows 8:00 a.m. through 12:00 a.m. and 1:00 p.m. through 5:00 p.m. as work time.)

- For setting work days, check the check box for the days of the week to be designated as work days.
- For setting work time, click the hours to be designated as work time.

Figure 4-7 URL Filtering Time Allotment Tab



Step 12 Click **Save** to update the URL filtering configuration.

Web Reputation

Web Reputation guards end-users against emerging Web threats. Because a Web Reputation query returns URL category information (used by URL Filtering), CSC SSM does not use a locally stored URL database. Web Reputation requires a Plus License.

Web Reputation also assigns reputation scores to URLs. For each accessed URL, CSC SSM queries Web Reputation for a reputation score and then takes the necessary action, based on whether this score is below or above the user-specified sensitivity level.

CSC SSM has a feature that enables the device to automatically provide feedback on infected URLs, which helps improve the Web Reputation database. If enabled, this feedback includes product name and version, URL, and virus name. (It does not include IP address information, so all feedback is anonymous and protects company information.) Web Reputation results are located in the Web Reputation log (Logs > Query > Web Reputation) and the Summary > Web (HTTP) tab.

Using Trend Micro Web Reputation technology (part of the Smart Protection Network), you perform website scanning at varying levels of protection (low, medium, and high) and add websites to the Exceptions List (yourcompany.com, for example) so that websites can be viewed without scanning or blocking.

Note Pre-approving websites must be done carefully. Not scanning or blocking a website could pose a security risk.

Anti-phishing Using Web Reputation

CSC SSM provides anti-phishing through Web Reputation and URL Filtering. Both features require a Plus License.

- Phishing sites blocked by URL Filtering are blocked by the Phishing category and will give a "Phishing" message
- Phishing sites blocked by Web Reputation will provide a "low reputation" message.

Web Reputation Database

The Web Reputation database resides on a remote server. When a user attempts to access a URL, CSC SSM retrieves information about this URL from the Web Reputation database and stores it in the local cache. Having the Web Reputation database on a remote server and building the local cache with this database information reduces the overhead on CSC SSM and improves performance.

The Web Reputation database is updated with the latest security information about web pages. If you believe the reputation of a URL is misclassified or you want to know the reputation of a URL, use the following URL to notify Trend Micro:

http://reclassify.wrs.trendmicro.com/submit-files/wrsonlinequery.asp

Settings

Setting the security sensitivity level prevents users from being misdirected to malicious websites and provides administrators the ability to set the protection level.

Web Reputation settings involve specifying the following:

- Enable or disable Web Reputation
- Select the appropriate security sensitivity level for your company
- (Optional) Provide anonymous feedback on infected URLs to Trend Micro

Security Sensitivity Level

Upon receiving a Web Reputation score, CSC SSM determines whether the score is below or above the preferred threshold. The threshold of sensitivity level is defined by the user. Medium is the default sensitivity setting. Trend Micro recommends this setting because it blocks most web threats while not creating many false positives.

To set the sensitivity level, perform the following steps:

Step 1 Go to the **Web (HTTP) > Global Settings > Web Reputation > Settings** tab.

Step 2 Click **Enable** to enable Web Reputation (Enabled is the default setting.)

Step 3 Specify the URL blocking sensitivity level. Select from the following:

- **High** — Blocks more websites, but risks blocking non-malicious websites
- **Medium** — (default) Balances risks between High and Low settings
- **Low** — Blocks fewer websites, but risks not blocking potentially malicious websites

Step 4 Click **Save**.

Feedback Option

Web Reputation scan results can be fed back to an external backend Rating Server. The Feedback option is disabled by default.

To enable the feedback option, perform the following steps:

Step 1 Go to the **Web (HTTP) > Global Settings > Web Reputation > Settings** tab.

Step 2 Check the "Send anonymous feedback on infected URLS to Trend Micro" check box.

Step 3 Click **Save**.

Exceptions

Listing a website within the Web Reputation approved list allows CSC SSM to bypass any malicious code scans on the listed site. Web Reputation scanning exceptions can be defined by entering the complete website URL or IP address, a URL keyword, a string, or by importing an existing exception list of URLs.

Caution Lack of scanning could cause security holes if a website on the Approved list has been hacked and had malicious code injected.

To specify Web Reputation exceptions, perform the following steps:

Step 1 Go to the **Web (HTTP) > Global Settings > Web Reputation > Exceptions** tab.

Step 2 Do one of the following:

- Enter text in the Match file, specify the match type, and then click **Add.**

Note The default option is Web site/IP address.

- Import the URL approved list. For more information about importing the URL exceptions list, see the online help topic named "HTTP URL Filtering Settings - URL Filtering Exceptions".

Step 3 Click **Add**.

Step 4 Click **Save**.

After you have specified a URL as an exception to Web Reputation, you can include it in Web Reputation scanning by selecting the URL in the Approved List and clicking **Remove** to remove it from the list. Click **Remove All** to delete all URLs in the Approved List.

URL Blocking and Filtering Policies for Users/Groups

CSC SSM has a policy framework that allows the association of URL Filtering and Blocking policies to specific groups or individual users based on the user or group identity. This feature includes:

- Identification settings
- Microsoft Active Directory service support
- Policy item management
- User/Group-based log and report

Note Both URL Filtering and URL Blocking require a Plus License.

CSC SSM supports up to 20 URL Filtering and Blocking policies for users and groups. The Domain Controller Agent software can be deployed on a Domain Controller Server or Windows machine that is on the Intranet. The agent communicates with CSC SSM over a secure, TCP port and works with Microsoft Active Directory.

Before using user/group policies for URL Filtering and Blocking, enable the following:

- Select a method of user/group identification by going to: **Administration > Device Settings > User Id Settings**. For more information about User ID settings, see the "Configuring User ID Settings" section on page 6-3.
- Download and install the Domain Controller Agent. For more information, see the "Installing the Domain Controller Agent" section on page 6-6.
- Add the Domain Controller Agent and Domain Controller information. For more information, see the "Adding A Domain Controller Agent or Server to CSC SSM" section on page 6-7.
- Enable URL Filtering at the global level by going to: **Web (HTTP) > Global Settings > URL Filtering**, and check the 'Include User Group Policies" check box.
- Enable URL Blocking at the global level by going to: **Web (HTTP) > Global Settings > URL Blocking**, and check the 'Include User Group Policies" check box.

The All Policies tab on the URL Blocking & Filtering Policies screen displays existing policies and provides the following information:

- Policy Type — Lists the policy by type, either Filtering or Blocking
- Policy Name — Shows the descriptive name assigned to identify the policy
- Status — Indicates if the policy is enabled (green check) or disabled (red check)
- Priority — Indicates the order in which the policies will be enforced. For example, if a policy has an exception and has a higher priority than another policy, this policy will override the rules of the lower priority policy. Any global policies configured under URL Filtering or URL Blocking will always have the lowest priority.

The Policies by User/Group tab offers search capabilities for existing policies. Editing policies is possible from this screen by clicking the policy name.

Add/Edit URL Blocking Policies for Users/Groups

URL blocking is an important tool for managing employee Internet use in your organization. With URL blocking, you can prohibit access to URLs that may distract employees from productive use of their time or may even result in legal liability. The process of adding a blocking policy for groups or users begins with choosing a template and creating an account.

If "Global Policy - URL Blocking" appears in the list of policies, this policy was configured on the Web (HTTP) > Global Settings > URL Blocking screen. Priority settings can be changed for user and group policy by going to Web (HTTP) > User Group Policies > URL Blocking & Filtering. Go to the far right column in the table that lists the policies, and click the up and down arrows to adjust the priority. Global policies will always have the lowest priority.

Prerequisites

Before a blocking policy can be added, do the following:

- URL Blocking must be enabled on the global level by going to Web (HTTP) > Global Settings > URL Blocking.
- A method of user/group identification must be selected by going to Administration > Device Settings > User ID Settings screen, and the Domain Controller Agent must be installed and configured. For more information, see the "Configuring User ID Settings" section on page 6-3.

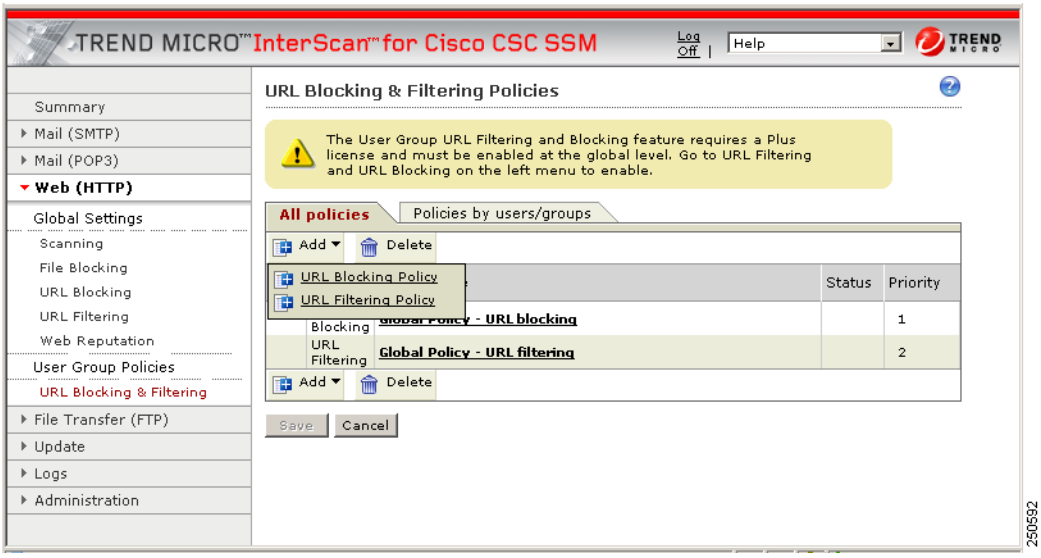
Selecting a Template

To select a template for the first rule of a URL Blocking Policy, perform the following steps:

Step 1 Go to the **Web (HTTP) > User Group Policies > URL Blocking and Filtering > All policies** tab.

Step 2 Click **Add** and select **URL Blocking Policy**. (See Figure 4-8.)

Figure 4-8 To Add a User Group Policy



Step 3 (Optional) Check the **Enable policy** check box to have the policy enabled as soon as it is created. (See Figure 4-9.)

Note To enable the policy later, see the "Enabling a User/Group Blocking Policy" section on page 4-24.

Step 4 Go to the Template section of the URL Blocking Policy: Add Policy page.

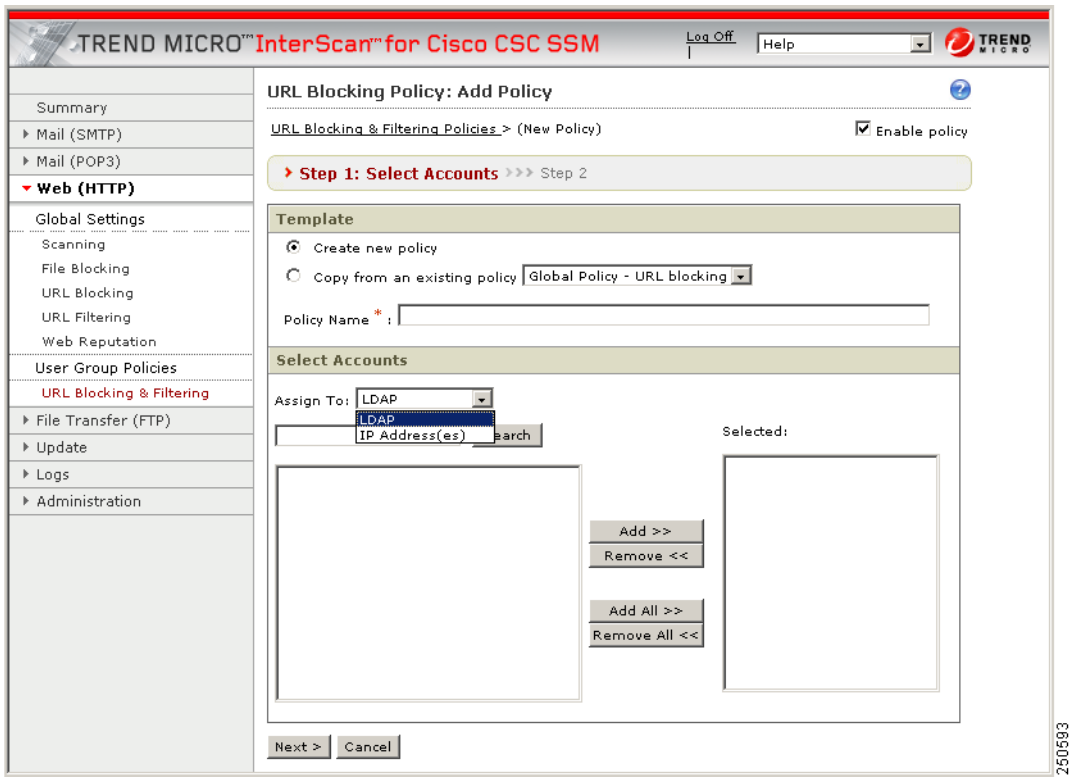
Step 5 Select one of the following options:

- Create a new policy
- Copy from an existing policy. If this option is chosen, use the drop-down list to select the policy to use as a template.

Step 6 Type a descriptive policy name.

Step 7 Select accounts according to the "Creating Accounts" section on page 4-26.

Figure 4-9 Selecting a Template and User ID Method



Creating Accounts

To create accounts, perform the following steps:

Step 1 Select a template according to the "Selecting a Template" section on page 4-26, then create the account.

Step 2 In the Select Accounts section, select the method of user or group identification you will use: LDAP and/or IP address(es). (See Figure 4-9.) This selection must match the user identification method selected by going to Administration > Device Settings > User ID Settings.

Note If no users or groups display, the Domain Controller Agent may not be well configured.

Step 3 To select users:

- For LDAP identification, select the radio button for either the entire LDAP list or use the search function to find a specific name or group.
- For IP address identification, enter a range of IP addresses, a single IP address, or a host name.

Step 4 Click the user name, group name or IP address, and then click **Add** to add users, groups, or IP addresses to the **Selected** field.

Step 5 Click **Next** to continue creating your policy.

Step 6 Continue with the "Step 2: Specify Block Rule via Local List" page to create a blocking policy as described in "Blocking from the Via Local List Tab" section on page 4-7.

Step 7 Click **Finish**. The new policy displays in the policy list of the All Policies tab.

Allowing or Blocking Specific URLs

Blocking URLs, importing lists of blocked URLs, and exceptions to the blocking are described in the "Blocking from the Via Local List Tab" section on page 4-7. Format and other descriptions are available in the online help.

URL blocking is implemented in two ways:

- You define specific URLs to be blocked (via local list).
- URLs are blocked by the Trend Micro scan engine (via pattern file).

The "Step 2: Specify Block Rule via Local List" page is similar to Figure 4-3 and used in Step 6 of the Creating Accounts procedure. It allows you to specify sites that you want to allow or prohibit access to for specific users or groups in your organization via a local list.

Enabling a User/Group Blocking Policy

When the URL blocking function is disabled at the global level, end users can access any domains or URLs from your network via HTTP. When URL blocking is enabled at the global level, all users in your network are prevented from accessing certain domains and URLs. User/group policies allow you to select the domains and URLs that can be viewed by specific users or groups.

Note A URL Blocking policy can be enabled at the time of creation or later. For more information, see the "Selecting a Template" section on page 4-26.

To enable a URL Blocking Policy, perform the following steps:

Step 1 Verify that the URL Blocking feature is enabled at the global level by going to **Web (HTTP) > Global Settings > URL Blocking**.

Step 2 Go to the **Web (HTTP) > User Group Policies > All Policies** tab.

Step 3 Click the name of the policy to be enabled.

Step 4 Check the check box to immediately enable the policy.

Step 5 Click **Save**.

Step 6 Uncheck the check box to disable a policy and then click **Save**.

Editing a User/Group Blocking Policy

To edit a specific user group blocking policy, perform the following steps:

Step 1 Go to the **Web (HTTP) > User Group Policies > All Policies** tab**.**

Step 2 Click the blocking policy name.

Step 3 Edit the blocking policy on the Accounts and/or Via Local List tabs.

Step 4 Click **Save**.

Adding or Editing URL Filtering Policies for Users/Groups

URL Filtering for users/groups allows you to filter categories of websites such as “Adult” or “Social,” that specific users or groups of users can access. Site classification will vary from one organization to the next, depending on the business being conducted. For example, the sub-category “violence/hate crime” may not be work related in a manufacturing company, but may be defined as work related in a news reporting organization.

Some company prohibited sites may always be blocked (on the HTTP URL Filtering Rules screen) during both work time and leisure time, but if you want to allow employees to use chat sites during leisure time, you can specify those sites be blocked only during work time.

If a “Global Policy - URL Filtering” policy already exists, it was configured by going to Web (HTTP) > Global Settings > URL Filtering and was applied to all users. User or group policy will always have a higher priority than the global policy. Priority settings can be changed for user and group policy by going to Web (HTTP) > User Group Policies > URL Blocking & Filtering screen. Go to the far right column in the table that lists the policies, and click the up and down arrows to adjust the priority. Global policies will always have the lowest priority.

Prerequisites

Before a filtering policy can be added, the user must:

- Enable URL Filtering must be enabled on the global level by going to the Web (HTTP) > Global Settings > URL Filtering screen.
- Select a method of user/group identification by going to the Administration > Device Settings > User ID Settings screen. For more information, see the “Configuring User ID Settings” section on page 6-3.

- Download and install the Domain Controller agent. For more information, see the "Installing the Domain Controller Agent" section on page 6-6
- Add the Domain Controller Agent IP address.
- Auto-detect or manually add the Domain controller server.
- Configure the proxy setting by going to Update > Proxy Settings, if an HTTP proxy is required.

Note For URL Filtering to work properly, the CSC SSM must be able to send HTTP requests to the Trend Micro service.

Selecting a Template

To select a template for the first rule of a URL Filtering Policy, perform the following steps:

Step 1 Go to the **Web (HTTP) > User Group Policies > URL Blocking and Filtering (All policies** tab).

Step 2 Click **Add** and select **URL Filtering Rule**.

Step 3 Go to the Template section of the URL Filtering Policy: Add Policy screen, similar to what is shown in Figure 4-7.

Step 4 Select one of the following options:

- Create new policy
- Copy from an existing policy. If this option is chosen, use the drop-down list to select the policy to use as a template.

Step 5 Enter a descriptive policy name.

Step 6 Create an account according to the steps in the "Creating Accounts" section on page 4-26.

Creating Accounts

To create accounts, perform the following steps:

Step 1 Select a template according to the steps in "Selecting a Template" section on page 4-26.

Step 2 In the accounts section (similar to what is shown in Figure 4-9), select the method of user or group identification you will use: LDAP or IP address. This selection must match the user identification method selected by going to Administration > Device Settings > User ID Settings. Both methods of identification (LDAP and IP address) can be used if the identification method is configured correctly.

Step 3 To select users:

- For LDAP identification, select the radio button for either the entire LDAP list or use the search function to find a specific name or group.
- For IP address identification, enter a range of IP addresses, a single IP address, or a host name.

Step 4 Select the user name, group name, IP address or range of IP addresses, and then click **Add** to add users, groups or IP addresses to the Selected field.

Step 5 Click **Next**.

Step 6 Continue to the "Step 2: Specify the URL Filtering Rules" screen, using the instructions in "Filtering Rules, Exceptions, and Time" section on page 4-15.

Step 7 Click Finish. The new policy displays in the policy list of the All Policies tab.

Adding User Group Filtering Policy Rules

This screen allows you to define rules for user or group policies that allow or disallow access to categories, or parts of categories, of URLs during work or leisure time. The categories are:

- Computers/Bandwidth
- Computers/Harmful
- Computers/Communications
- Adults
- Business
- Social
- General

For information about how to set your policy rules, see the "Filtering Rules, Exceptions, and Time" section on page 4-15 and follow Steps 4 through 6.

Note Work and leisure time parameters are configured in the Web (HTTP) > Global Settings> URL Filtering screen. For more information, see the "Filtering Rules, Exceptions, and Time" section on page 4-15, step 10. Notification messages are configured in the Global Settings for URL Blocking. For more information, see the "URL Blocking Notifications" section on page 4-8.

Specifying Exceptions to the User Group Filtering Policy

The "URL Filtering Policy: Add Policy (Step 3: Specify Exceptions)" screen, similar to what is shown in Figure 4-6, allows you to identify URLs that are excluded from filtering. For example, you may have elected to assign the sub-category "shopping" to the work-time filtered category. However, your Finance Department needs access to URLs of certain vendors offering online shopping service to purchase office supplies, furniture, software, hardware and other business equipment, airline tickets, and so on. Identify those vendors as exceptions to allow access to their URLs.

For more information about how to set your policy rules, see the "Filtering Rules, Exceptions, and Time" section on page 4-15 and follow steps 7 through 9. Online help also provides detailed instructions.

Editing a User/Group Filtering Policy

To edit a specific user group filtering policy, perform the following steps:

Step 1 Go to the **Web (HTTP) > User Group Policies > All Policies** tab**.**

Step 2 Click the filtering policy name.

Step 3 Edit the filtering policy on the Accounts, Rules, and/or Exceptions tabs.

Step 4 Click **Save**.

Deleting a User Group Blocking or Filtering Policy

Policies can be deleted from the Web (HTTP) > User/Group Policies > URL Blocking & Filtering screen. To delete a policy, perform the following steps:

Step 1 Check the check box at the beginning of the row for the policy to be deleted.

Step 2 Click the **Trashcan** icon to delete the policy. (See Figure 4-8.)