Web Security Configuration

Administrator Guide

Symantec.cloud

Web Security Administrator Guide

Documentation version: 1.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Clients are advised to seek specialist advice to ensure that they use the Symantec services in accordance with relevant legislation and regulations. Depending on jurisdiction, this may include (but is not limited to) data protection law, privacy law, telecommunications regulations, and employment law. In many jurisdictions, it is a requirement that users of the service are informed of or required to give consent to their email being monitored or intercepted for the purpose of receiving the security services that are offered by Symantec. Due to local legislation, some features that are described in this documentation are not available in some countries.

Configuration of the Services remains your responsibility and entirely in your control. In certain countries it may be necessary to obtain the consent of individual personnel. Symantec advises you to always check local legislation prior to deploying a Symantec service. You should understand your company's requirements around electronic messaging policy and any regulatory obligations applicable to your industry and jurisdiction. Symantec can accept no liability for any civil or criminal liability that may be incurred by you as a result of the operation of the Service or the implementation of any advice that is provided hereto.

The documentation is provided "as is" and all express or implied conditions, representations, and warranties, including any implied warranty of merchantability, fitness for a particular purpose or non-infringement, are disclaimed, except to the extent that such disclaimers are held to be legally invalid. Symantec Corporation shall not be liable for incidental or consequential damages in connection with the furnishing, performance, or use of this documentation. The information that is contained in this documentation is subject to change without notice.

Symantec may at its sole option vary these conditions of use by posting such revised terms to the website.

Technical support

If you need help on an aspect of the security services that is not covered by the online Help or administrator guides, contact your IT administrator or Support team. To find your Support team's contact details in the portal, click **Support** > **Contact us**.

Contents

Chapter 1

Introduction

This chapter includes the following topics:

Other guidance on Web Security

These help topics provide further guidance on the Web Security Services.

Table 1-1 Help on Web Security

	Help page
Click to open the help page	Web Security Configuration Smart Connect Deployment Web Firewall Configuration Web Security Deployment

About Web Security

Web Security comprises the following services:

- Web AntiSpyware and AntiVirus
- Web URL Filtering

These Web Security services work by us scanning the web traffic that is diverted from the users' computers or company perimeter devices. On the Web Security servers, policies and settings configured for your site using the portal are applied to this traffic, which is permitted or blocked as appropriate.

Once the configuration is in place to apply this protection and control, the service is transparent to your users. They will notice little discernible effect on web browsing speed or user impact other than when pages are blocked for any reason.

Web browsing without Web Security services

In a typical office environment, where a firewall controls general Internet access and performs network address translation (NAT), the chain of events in retrieving a Web page is as follows.

The initial request for the Web page is made to the firewall, which checks its configuration. If access to the Web is permitted according to the firewall's rules, the firewall requests it from the Web server (or the firewall passes on the original request from the user). The Web server responds to the firewall with the page. Then the firewall responds to the user with the requested page. This extra barrier is transparent to the user, unless the page is blocked or denied for some reason.

Web browsing with Web Security services

In a typical office environment, where a firewall controls general Internet access and performs network address translation (NAT), when Web Security is deployed, there is an extra link in the chain of events.

The initial request for the Web page is made to the firewall. The firewall then requests the page, or the firewall passes on the original request from the user, to Web Security. Web Security checks the portal for the configuration that you have made and if the page is permitted, Web Security requests it from the Web server. The Web server responds to Web Security with the page. Web Security then responds to the firewall with the requested page, which then responds to the user by delivering the page.

The firewall and Web Security steps are transparent to the user, unless the page is blocked or denied for some reason at either device.

About web caching

A cache is used to store web pages that have been browsed, in case they are required again within a certain time. This is typically used to speed up web browsing. It is usually quicker to retrieve a page that is cached, rather than to download it again from the web site. Two major types of caching are available: Browser cache and External cache:

Browser cache

The browser cache is maintained by your Web browser and applies typically to any Web pages that have been browsed, apart from encrypted pages (accessed using HTTPS). Therefore, your browser automatically caches files when you download them. If you visit those pages again before you close Internet Explorer, for example, the local copy may be used rather than re-downloading the whole page again. Depending on your browser settings, it may check that the page has not changed since you last visited it. Normally this is transparent to the user, so an updated page is redownloaded and displayed, whereas an unchanged page is only displayed.

This cache facility is particularly noticeable when a user selects the Back button in their Web browser . Because they have browsed that page earlier in the same browsing session, it typically is retrieved from the cache rather than from the Internet.

The browser cache is configured within the preferences dialog of your browser, or these settings may be deployed across your site by various means.

In the context of Web Security, if a user is prevented from visiting a page at a certain time, and if that page is already in the cache, the cached version may be displayed. However, it cannot be updated until the permissions set up within the portal allow access to the Web site.

External web cache

An external web cache works in a similar way to a browser cache, but on a larger scale. It is operated and maintained on a separate server, either on your own network, or out on the Internet.

Note: Web Security acts like caching servers. This speeds the delivery of the web pages that Web Security scans. It also means that an additional external web caching server is unnecessary and ineffective.

We advise that you do not use an external web cache with Web Security. Using an external web cache has security implications, even if the caching server is on your

own local area network. The risk is that the web pages that Web Security should block are cached. Therefore your users can potentially retrieve the blocked web pages.

Frequently asked questions (FAQs) on Web Security

Table 1-2

Will users experience delays in browsing as a result of using these Web Security services?	There is little or no discernible delay in web browsing caused by the use of Web Security. Regional security servers combined with global load-balancing techniques ensure traffic is sent to a server that can deal with it promptly.
Can I customize user notifications and alerts?	When access is denied to a web site for any reason, an alert page is usually displayed in the user's web browser. This can be set up as required, using, for example details of what happened and advice for users as to what do next. For further details, see: See "Customizing user alerts for Anti-Spyware, Anti-Virus and URL Filtering" on page 14.
Do I need to lock down port 80 on my firewall?	Once redirection to the Web Security proxy service on port 3128 is set up and tested, port 80 should be blocked on the gateway firewall device. This ensures that all outgoing web traffic can only go via Web Security. This is especially important if the users' web browser proxy settings cannot be locked down. It forces users to keep the proxy settings in place if they want to be able to surf the net. This is also important in the case of a mixed environment where both PC and Mac users are being configured. PC users can have their settings locked down but the Mac users cannot be restricted in this way, so locking down port 80 on the firewall is essential.

Table 1-2 *(continued)*

Is Web Security relevant in the education sector? Can policies be configured to meet the requirements of schools?	The way in which Web Security can limit access to categorized sites means that you can limit access by category. For example, you could grant access to Kids, Education, News, butblock access to other sites. For the ultra-cautious, we have provided the category "Unclassified", which can be used to block anything we cannot assign a category to. This avoids problems caused when brand new sites which do not yet belong to the categories database are missed.
How can we protect ourselves from threats inherent in users accessing Web-based email?	There are two levels of protection. You can do one of the following: ■ Block access to all Webmail sites by category. ■ If the Webmail site does not use SSL, you can permit it, knowing that items downloaded by HTTP to the client PC are checked for malware and spyware.
Can Web Security protect against files downloaded from peer-to-peer (P2P) networks?	No. P2P networks work by using their default ports (e.g. 1214) and various other ports, including port 80 (used for normal HTTP web traffic), to try to bypass firewall protection. Several firewalls, including the built-in Windows XP SP2 firewall, may be able to successfully block P2P traffic under certain circumstances. Please see your firewall vendor's documentation for details.
Are there any special considerations for URLs containing '%20' instead of a 'space' character?	No. Any URLs entered under the **Specific URLs** tab must be entered in 'percent-encoded' format (if applicable - most URLs do not include these characters). Similarly, any URLs reported in the detailed or audit reports will be in percent-encoded format.

Table 1-2 *(continued)*

What is the maximum interval between someone making a change on the UI and it being applied to the environment? How long does it take after the initial provision of the services before any changes made to the configuration or policies take effect?	After the initial provision of the services, any changes to the configuration or policies will take around thirty minutes and usually not more than one hour We recommend that you test any major changes to your configuration after an appropriate time has passed, to verify that it is working as expected. If your changes have not been implemented within four hours, please contact the Support team.
I run my browser with some higher-than-normal security levels, namely: active scripting is disabled for normal Internet access and only enabled for Trusted sites. Will this cause any problems?	These settings mean that you can only access the portal if you list it as a Trusted Site. They may also mean that when you get the redirect for any malware or blocked URL, you may receive a Security Warning message. This is due to moving from a "regular" site to a Trusted Site - normally you will want to select **Yes** at such a message.
What is the address of the proxy server to use for Web Security?	Please refer to your provisioning documentation for these details or contact the Support team who will be able to arrange for this information to be re-sent to you.
I noticed that the Web URL Filtering categories list has changed. Will this affect my existing rules?	Any URL categories selected under the old settings will be mapped to the closest equivalent under the new settings. This maintains the same level of protection as previously. However, to take full advantage of the new categories available, we recommend that you review all your rules and select new categories where appropriate.

Chapter 2

Web AntiSpyware and AntiVirus

This chapter includes the following topics:

About Web AntiSpyware and AntiVirus

Web Security is designed to give your users the same high level of protection when they are web browsing that they enjoy with their email services, with added protection from spyware. Web AntiSpyware and AntiVirus provides all-round protection for your network from Internet threats.

Configuring the Web AntiSpyware and AntiVirus Service

The Web AntiSpyware and AntiVirus Service has very little to be configured. The service scans your web traffic to protect your users and alerts them if a web page has been blocked because of a malware threat.

Decide whether you want to scan SSL encrypted web traffic (web pages delivered via HTTPS).

See “About HTTPS Inspection” on page 56.

To locate the Web AntiSpyware and AntiVirus pages

- Select **Services** > **Web Security Services** > **Web Anti-Spyware & Anti-Virus**

For information on configuring User Alerts:

See "Customizing user alerts for Anti-Spyware, Anti-Virus and URL Filtering" on page 14.

See "Customizing user alerts for HTTPS Inspection" on page 65.

Customizing user alerts for Anti-Spyware, Anti-Virus and URL Filtering

The user alert notifies users in the following situations:

- When the user tries to open a web page that is blocked by AntiSpyware and AntiVirus
- As a result of a rule set in the URL Filtering service

Alerts can be configured for each service in the following locations:

- **Web Security Services** > **Anti-Spyware & Anti-Virus** > **User Alerts**
- **Web Security Services** > **URL Filtering** > **Alerts**

The default alert messages include two terms in square brackets, which are replaced with the URL of the page that contains the threat and the name of the malware threat that was detected. You can add your Support team contact details by customizing the alerts.

Note: If a large page (over 500 KB) is blocked because of a virus found within an archive, the connection is dropped. No normal notification message is sent because part of the page may already have been processed.

To customize a user alert for Anti-Spyware, Anti-Virus and URL Filtering

1. Select one of the following:
   - **Services** > **Web Security Services** > **Web Anti-Spyware & Anti-Virus**
   - **Services** > **Web Security Services** > **URL Filtering** > **Alerts**
2. In the **Users Alerts** tab, click **Use Custom**.

   You can now edit the default text, for example to add your Support team contact details.
3. Enter the text for the alert. The content can include HTML tags for formatting or a link to an information page on your intranet, for example. You can use the following placeholders in the message that will be substituted with the relevant values depending on the circumstances under which the page is blocked:

- %U - the URL of the page that is blocked
- %V - the name of the virus or other malware threat that caused the page to be blocked
- %R - the name of the rule that was triggered to block the page
- %C-en-US– the category name, displayed in English
- %C-de-DE – the category name, displayed in German
- %C-ja-JP– the category name, displayed in Japanese

4 To see the message as it will appear to the user, click **Preview**.

5 Click **Save and Exit**.

A confirmation message is displayed.

Chapter 3

Web URL filtering

This chapter includes the following topics:

- About URL category changes
- Checking the URL categorization for a website
- Using example URL categories for testing purposes
- About reporting

Locating Web URL Filtering settings in the portal

You can set up a rich set of policy rules with the flexibility to suit the particular needs of your organization.

To locate the Web Security configuration pages in the portal

1. Click **Services** > **Web Security Services** > **Web URL Filtering**.

   The existing policy rules are displayed.

2. Click on an existing rule or click **New Rule**.

   The following pages are available: **Rule**, **Time**, **Groups**, **Quotas**, **URL Categories**, **Specific URLs**, **Content Types**.

3. You can also select other pages of settings that contribute to your policy rules:

   Click **Services** > **Web Security Services** > **Web URL Filtering** > **Custom Groups**, **Alerts**, and **URL Categorization**.

About configuring the URL Filtering service

Web URL Filtering enables you to control and report on your users' web browsing in line with your corporate security policy or other requirements.

You can set up a rich set of policy rules with the flexibility to suit the particular needs of your organization. Policy rules are set up to identify the action to be taken when a user's web request matches the defined conditions.

A rule is made up of the following components:

- A descriptive name
- A set of conditions that must be met to trigger the rule:
  - Time
  - Groups
  - URL Categories
  - Specific URLs

    - Content Types
- An action that is performed when a web request satisfies the conditions of the rule.

When you define conditions in more than one of the preceding groups, an AND relationship exists between them, with one exception: an OR relationship exists between URL Categories and Specific URLs conditions. In other words:

- *When* AND *who* AND *where* AND *what*

So:

- *Time* AND *Groups* AND *URL Categories OR Specific URLs* AND *Content Types*

You define each rule by combining a set of individual conditions that characterize a particular circumstance. The more conditions that are included in the rule, the more specific the rule becomes. For example, to block all users except members of the Marketing department from visiting streaming media or social networking web sites within work hours, you would create the rule as follows:

- Time condition - use time period 9am to 5pm on Monday to Friday AND
- Groups condition - apply to all groups except the Marketing group AND
- URL Category condition - check the streaming media checkbox OR
- Specific URLs condition - define and use a list of social networking URLs

You would define either **Block** or **Block & Log** as the action for this rule.

Note: There is no limit to the number of rules that you can define. However, the rule set is strictly order-dependent. For example, the first active ‘Block’ rule that reports a match is acted on and any subsequent ‘Allow’ rules are ignored.

Web Security best practice settings

When you are provisioned with Web Security, it is enabled with default settings. A policy rule is defined to block traffic to Web pages with URLs that are known to contain content in the following categories: Adult/Sexually Explicit, Illegal Activity, Spam URLs, and Spyware. This rule constitutes the best practice setting for the Web Security Service. You can configure further rules to reflect your organization's Acceptable Use Policy, but we recommend that you keep the default rule as a minimum default setting.

To configure the best practice rule

1 Click **Services** > **Web Security Services** > **Web URL Filtering**.

The **Policy Rules** page with a rule called **Default** is displayed.

2 To view the components of the rule, click the name of the rule.

The **Rule** tab is displayed showing the rule name and **Block & Log** action setting.

3 Click on the **URL Categories** tab.

The **Use URL Categories below** checkbox is selected and the following four categories are checked -**Adult/Sexually Explicit**, **Criminal Activity**, **Spam URLs**, and **Spyware**.

When configuring rules, note the following:

- Use distinct rule names and keep a record of your rule configurations so you can easily amend them later, if required.
  For example, it could be confusing if two rules handle the same traffic differently at certain times of the day and they are not named appropriately. Try to group similar rules together in the rule list; if one rule changes, it is easier to remember to change similar rules, if required.
- As with any live service setup, you are strongly advised to check thoroughly that the new configuration for accessing the web works satisfactorily before turning off the previous setup. This is normally best achieved by performing a limited deployment on several PCs and checking everything thoroughly before you roll out the deployment across your company. You may want to extend the basis of the test configuration beyond the scope described in this guide.
- When you first set up your rules relating to what is blocked or allowed, it is useful to set the rule to 'Block and Log', or 'Allow and Log.' Then you can verify that it operates as expected by looking in the detailed reports.
  When you are satisfied that everything is configured correctly, the 'Block and Log' can be reset to 'Block' (and 'Allow and Log' can be set to 'Allow'), knowing that it has already been tested. Note that if a rule is set to 'Block' (rather than 'Block and Log'), the blocked event will not appear in the detailed reports. It also does not contribute to the system statistics. 'Block' or 'Allow' (with no log) should therefore only be used when you do not need to track whether (or how often) the rule is applied.
- To use specific groups and users in your rules, you must download and install the Client Site Proxy. You can also synchronize directory information with us using the Group Synchronization Tool. Check that these components are installed and working as expected before configuring rules based on Group and User information.

See "Client Site Proxy tool" on page 80.
See "Viewing users and groups for Web Security" on page 22.

- The Web URL Filtering element of Web Security actively blocks access to certain Web sites when configured to do so. As a result, you might not be able to access some essential websites. To minimize the chance of this happening, we recommend that you specifically permit access to the following sites at the top of your policies list:

The portal	The URL for Web Security Services Configuration Management Portal
Websites	The URL for the Web Security Services supplier
	The URL for your organization's website
	The URL for the websites of any partners or subsidiaries of your organization
	The URL for your desktop antivirus vendor's website. To enable automatic downloads of antivirus signatures for your PCs
Spam Manager	spammanager-1.messagelabs.com, spammanager-3.messagelabs.com
	spammanager-4.messagelabs.com, spammanager-5.messagelabs.com

  Certain sites are always allowed (whitelisted) when you use Web Security. These sites cannot be blocked using Web Security policy rules. We recommend that you always permit access to relevant download sites, such as Windows updates, desktop software, and antivirus vendor software. Some of these sites may already be whitelisted on our infrastructure.
  These are the URLs allowed for Windows updates:

  - url-prefix http://update.microsoft.com/
  - url-prefix http://download.microsoft.com/
  - url-prefix http://v5.windowsupdate.microsoft.com/
  - url-prefix http://windowsupdate.microsoft.com/

  If you need to block any of these sites and cannot achieve this using your policy rules, you may be able to use the Client Site Proxy or your firewall. If you have difficulty blocking access to a particular site, contact the Support team.

- Place rules that should have no exceptions (such as *block spyware and porn*) at the top of the list.

- Avoid defining rules that 'allow' access based only on content type or file type. If such a rule exists higher up the list than a 'block' rule that applies to a particular site, then the 'allow' rule is applied, and the traffic that you want to block may be allowed.
  Similarly, if there is already a rule higher up the rules list that blocks the traffic from a particular Web site , the 'allow' rule would never be hit.

See "About URL categories" on page 31.

See "About URL category changes" on page 49.

See "Defining policy rules" on page 23.

Checklist - creating user-specific and group-specific URL filtering policies

To create user-specific and group-specific URL filtering policies

1. Click **Tools** > **Downloads**.
2. Download and install the Group Synchronization Tool.
3. Synchronize your Active Directory information using the Group Synchronization Tool.
4. Click **Users and Groups** > **Web & IM** > **Users** or **Groups**, and perform searches to check synchronized and custom group information.
5. Download and install the Client Site Proxy.
6. Click **Services** > **Web Security Services** > **URL Filtering** > **Policy Rules** > **New Rule**, and create your rules.
7. On the **Groups** tab assign the appropriate group to the rule.
8. Move the rule to the appropriate position in the policy rules stack.
9. Activate the rules by clicking on the rule status in the **Rule Status** column.

See "Viewing users and groups for Web Security" on page 22.

See "Custom groups" on page 22.

See "Client Site Proxy tool" on page 80.

See "Changing the order of rules in the list" on page 28.

See "About configuring the URL Filtering service" on page 17.

Custom groups

If you need rules that require information or identification of users outside the Active Directory, you can create a Custom Group within the Web URL Filtering service. This group can then be used in your rules.

To create a new custom group

1. Click **Services** > **Web Security Services** > **Web URL Filtering**.
2. Click **Custom Groups** and click **New Group**.
3. Enter a **Group Name**
4. Enter the **External IP** range **Name** to be used by the group, and give this range a name.
5. Click **Add**.

   At this point, you can add further Internal IP names and ranges that are applicable to that External IP Range.

To create a user list

1. Click the **Users** tab, and enter a new user name in the format domain\username.
2. Click **Add** to add the user to the list.
3. To add or remove the user to or from the group, select the user from the list and click **Add to Group** or **Remove selected from Group** (as appropriate).

Viewing users and groups for Web Security

The optional Synchronization Tool enables you to synchronize the user and group data that is held in your directory with Web Security.

Note: If you do not want to synchronize your groups, you can configure custom groups manually.

To display all groups

- Click **Users and Groups** > **Web & IM** > **Groups**.

  The groups are listed, along with the number of users that belong to each.

  Search for a specific group by typing in several characters of the group name.

  To display the group members, click the number of users in that group .

To display all users

- Click **Users and Groups** > **Web & IM** > **Users**.

  The users are listed, along with the number of groups they belong to.

  Search for a specific user by typing in several characters of their user name.

  To display the groups the user belongs to, click the number of groups for that user.

See "Custom groups" on page 22.

Defining policy rules

You can navigate between the Policy Rules pages without losing your changes. If you inadvertently click **Save and Exit** before you have finished creating a rule, a confirmation message is displayed. To continue editing the rule, click **Cancel**. The list of Policy rules is displayed. Click the rule name or select the option for the rule and click **Edit Selected**.

Any rules you create are inactive until you activate them.

A new rule is added to the bottom of the rule list. You need to move the rule to the appropriate position in the list.

To create a rule

1. Click **Services** > **Web Security Services** > **Web URL Filtering**.
2. Click **New Rule**. The Policy Rules window is displayed.
3. Enter an appropriate name for the rule.

   We recommend using meaningful names for your rules so that they are appropriate in the various contexts in which they are displayed, for example in detailed reports. Avoid the use of unacceptable language in a rule name because it will appear in statistics, reports, and X-Headers.
4. In the **Rule Action** drop-down, select the action to be taken if there is a match for this rule.

   For initial testing, the options that include logging are recommended, so that you can assess that the rules being captured are as you expect. When you are satisfied that everything works as expected, you should turn off logging for each rule.
5. Define the conditions for the rule. See:
   - See "Defining time period rule conditions" on page 24.
   - See "Defining group rule conditions" on page 25.

- See “Defining URL categories rule conditions” on page 25.
- See “Defining specific URL rule conditions” on page 26.
- See “Defining content types rule conditions” on page 27.
- See “Defining web quotas rules” on page 73.

6 When you have finished configuring all the tabs within the rule as required, click **Save and Exit**.

Note: If a rule is set only to **Block** or **Allow**, the block event does not appear in the detailed reports, and also does not contribute to the system statistics. **Block** or **Allow** (with no log) should therefore only be used when you do not need to track whether or how often the rule is applied.

Note: The rule is currently **Inactive** in the **Rule Status** column. Typically, this is the correct setting until all the conditions of the rule have been defined. When the rule is fully defined, activate it.

See “Setting rules to active” on page 29.

See “Changing the order of rules in the list” on page 28.

Defining time period rule conditions

If a rule is only to be applicable at certain times of the day, add a time period condition. For example, there may be a requirement for the same traffic to be handled differently based on normal working hours and lunch times. The Web Security network is global, so we need to know which time zone this rule is applicable to. All rules should be set to the same time zone.

When you set up web quota rules, it may be useful to set up different Quotas for different Time Periods. For example, you may want to restrict users web browsing to a minimum during peak business hours. Web quotas are reset daily at 00:00 in your default time zone.

All policies must be set to the same time zone.

To define time period rules

1 Click **Services** > **Web Security Services** > **Web URL Filtering**.

2 Select the required rule or click **New Rule**. The **Policy Rules** window is displayed.

3 Click on the **Time** tab for the rule.

4 Select **Use Time Periods Below**.

5 Select the time zone.

6 Set up the days and times as appropriate.

In the **Edit times of the day** section, the **End time** entry must always be later than the **Start time** entry. To set up a rule that spans midnight, define two time periods: one covering the period up to midnight (for example, 19:00 - 00:00), and one covering the period from midnight (for example, 00:00 - 07:00).

Note: If you need to configure users in different time zones, please contact the Support team.

See "Defining web quotas rules" on page 73.

Defining group rule conditions

Groups that are created in the Custom Groups section or synchronized using the Synchronization Tool can be assigned to a rule.

To define group rules

1 Click **Services** > **Web Security Services** > **Web URL Filtering**.

2 Select the required rule or click **New Rule**.

3 In the **Policy Rules** window, click the **Groups** tab for the rule.

4 Click **Use Groups**.

5 Search for your custom and directory groups, and add them to the **Custom Groups Assigned to this rule** panel.

Defining URL categories rule conditions

To define URL categories rule conditions

1 Click **Services** > **Web Security Services** > **Web URL Filtering**.

2 Select the required rule or click **New Rule**. The **Policy Rules** window is displayed.

3 Click on the **URL Categories** tab.

4 Click **Use URL Categories below**.

5 Select the categories to use for the rule.

Note: The **Unclassified** category covers any web sites that have not been categorized yet, typically because they are new. Normally, these should be selected in a **block** rule near the top of the policies list. If a web site is not classified yet, it could be undesirable, so you should not allow traffic to it.

Defining specific URL rule conditions

There may be specific URLs that you want to block or allow regardless of the category they are in. A separate rule can be set up for each of these and the specific URLs can be entered on this tab.

We recommend that you define an **allow** rule as the first entry in the rule list, which specifically allows traffic to the URL of the portal at all times. This is to ensure that you can always amend your Web Security configuration when you need to.

To define specific URL rule conditions

1. Click **Services** > **Web Security Services** > **Web URL Filtering**.
2. Select the required rule or click **New Rule**. The **Policy Rules** window is displayed.
3. Click on the **Specific URLs** tab.
4. Click **Use Specific URLs below**.
5. To specify a URL, enter its domain name (without the protocol -'http://' or 'https://') in the **Add New URL** box. Click **Add**.

   The URL appears in the **URLs in this profile** list on the right. The domain name may be followed by a path (e.g. 'www.exampleURL.com/subsection') to apply the rule to a certain section of a web site. The domain name can include a leading wildcard * to match all subdomains (for example, *.exampleURL.com).

   Any URLs that this rule covers must be in the right-hand list (**URLs In This Profile**). They can be moved between the **Available URLs** list and the **URLs in this profile** list by checking their boxes and clicking **Add** or **Remove**.

Certain sites are always allowed ('whitelisted') when Web Security is in use. These sites cannot be blocked using Web Security policy rules. We recommend that you always permit access to relevant download sites, such as Windows updates, desktop software, and antivirus vendor software. Some of these sites may already be whitelisted on our infrastructure.

If you need to block any of these sites and cannot achieve this using your policy rules, you may be able to use the Client Site Proxy or your firewall. If you have difficulty blocking access to a particular site, we suggest that you contact the Support team.

Defining content types rule conditions

Typically, the **Content Types** tab is used in a block rule. If used in an allow rule, it would be too easy to permit undesirable traffic simply based on it using a normally acceptable MIME type. The page is in two important sections: **MIME Types** and **File Types**.

Content types and file types specified on this tab are additive. This means that, for the same rule, specifying a content type of PDF and a file type of EXE means the rule will match requests resulting in either PDF data or an EXE file being returned.

To define MIME type conditions

1. Content type refers to the type of data the web server declares that it is sending to the browser (the IANA MIME type). Selecting one of these options indicates that the rule applies to (typically, to block) data of this type.

   Click **Services** > **Web Security Services** > **Web URL Filtering**.

2. Select the required rule or click **New Rule**. The **Policy Rules** window is displayed.
3. Click on the **Content Types** tab.
4. Click **Use Content Types below**.
5. Select the MIME types to use for the rule. The MIME types are grouped into categories. Check the box by any that you require to be blocked.

To block a MIME type that is not listed, enter it as a custom MIME type in the **Add new MIME type** box, and click **Add**. Check the box by the new MIME type. Custom MIME types can be deleted from the list if no longer required in any policies, or left unchecked if not required in this rule.

Note: Custom content types MUST be entered in the form of recognized IANA MIME types (i.e. type/subtype).

To define file type conditions

1. Using file type conditions in a rule enables the files with a specified file extension to be blocked. That is, the extension of the apparent file name of a resource being downloaded from a web site. In the first instance, this is checked against the terminal portion of the URL, so a rule matching the extension ‘exe’ would match a URL of ‘www.exampleURL.com/games/fun.exe’. In the case that the object being downloaded is an archive file (for example, a .zip file), the file extensions are also checked against the files within the archive.

   Click **Services** > **Web Security Services** > **Web URL Filtering**.
2. Select the required rule or click **New Rule**. The **Policy Rules** window is displayed.
3. Click on the **Content Types** tab.
4. Click **Use Content Types below**.
5. In the **File Types** section, check the box next to any file types that you require to be blocked.
6. To block a file with an extension that is not listed, enter it as a **Custom File Type** and click **Add**. Check the box by the new file type. It can be deleted from the list if no longer required in any policies, or left unchecked if not required in this rule.

Note: The ‘doc.url’ and ‘doc.exe’ file types and similar ‘double’ extensions are sometimes used to deceive users. They may think they are clicking on a ‘doc’ file, rather than a link to a web site or program. While malware is blocked by the Web AntiSpyware and AntiVirus Service, these extensions should still be blocked in a rule of their own at all times, positioned near the top of the policies list.

Changing the order of rules in the list

You can move a rule up or down the list to its appropriate position bearing in mind the ‘first match’ principle within the policies list.

To change the order of rules

1. Click **Services** > **Web Security Services** > **Web URL Filtering**.
2. Click the up or down **Change Priority** button on any rule to move it as required.

Setting rules to active

When a rule is in the appropriate place in the list, activate it by clicking the **Inactive** text in the **Rule Status** column.

If a rule is no longer required, it can be set to **Inactive** in the **Rule Status** column. To delete it completely, click the option to the left of the rule name, click **Delete Selected**, and confirm the deletion.

Setting up a rule for a new group of users created in Active Directory

To set up a rule for a new group of users created in Active Directory

1. Log on to the portal.
2. If not already done, download and install the Group Synchronization Tool.
3. Synchronize your Active Directory information using the Group Synchronization Tool (see the *Synchronization Tool Administrator Guide*).
4. If not already done, download and install the Client Site Proxy.
5. Click **Users and Groups** > **Web & IM** > **Groups** and check that the group has been synchronized and has the appropriate users.
6. Click **Services** > **Web Security Services** > **Web URL Filtering** > **Policy Rules** > **New Rule**.
7. On the **Groups** tab assign the appropriate Directory Group to the rule.
8. Select the other required rule options (such as URL categories or time periods).
9. Save the new rule.
10. Move the rule to the appropriate position in the policy rules stack.
11. Activate the rule by clicking on the rule status in the Rule Status column (this toggles the status between **Active** and **Inactive**).

See "Viewing users and groups for Web Security" on page 22.

See "Client Site Proxy tool" on page 80.

See "About configuring the URL Filtering service" on page 17.

See "Custom groups" on page 22.

See "Changing the order of rules in the list" on page 28.

Setting up a rule for a group based on internal IP addresses

To set up a rule for a group of users based on their internal IP addresses

1. Log on to the portal.
2. If not already done, download and install the appropriate Client Site Proxy.

   See “Client Site Proxy tool” on page 80.
3. Click **Services** > **Web Security Services** > **Web URL Filtering** > **Policy Rules**.
4. Click on **New Group**.

   See “Custom groups” on page 22.
5. Enter a name for the group.
6. Enter an externally facing IP or IP range, providing a name for the IP.
7. Enter the related internal IP or IP range, providing a name.
8. Save the Group.
9. Click **Services** > **Web Security Services** > **Web URL Filtering** > **Policy Rules**.
10. Click on **New Rule** and enter an appropriate name for the rule.
11. On the **Groups** tab assign the Group that you created to the rule.

    See “Defining group rule conditions” on page 25.
12. Select the other required rule options (such as URL categories or time periods).
13. Save the new rule.
14. Move the rule to the appropriate position in the policy rules stack.

    See “Changing the order of rules in the list” on page 28.
15. Activate the rule by clicking on the rule status in the Rule Status column (this toggles the status between **Active** and **Inactive**).

Note: As an alternative to the Client Site Proxy, you can use a web gateway that is configured to insert HTTP X-Forwarded-For information

Getting detailed information on user activity as related to a particular policy rule

Run a detailed report on your Web Security user activity.

For further details on reporting, see the Online Help.

See "About reporting" on page 55.

About URL categories

Web Security uses the following categories for URL Filtering.

Table 3-1 URL Categories

Category Name	Description
Abortion	Sites that provide information or arguments in favor of or against abortion, including the following: ■ Describing abortion procedures ■ Offering help in obtaining or avoiding abortion
Adult/Sexually Explicit	Sites that contain sexually explicit material for the purpose of arousing a sexual or prurient interest. This category includes the following: ■ Sex chat rooms ■ Sex portals ■ Pornography thumbnails and 'pic post' sites ■ Online magazines ■ Picture galleries ■ Phone sex and live video ■ Adult services ■ Escort services ■ Strippers ■ Mistresses ■ Adult personal advertisements

Table 3-1 URL Categories *(continued)*

Category Name	Description
Advertisement and Popups	Sites that provide Internet advertising services, including the following: ■ Pay-per-click advertising ■ Sponsored advertisements ■ Search engine marketing ■ Pop-up, pop-under, and banner advertisements
Alcohol	Alcohol-related sites, including the following: ■ Promoting or selling alcoholic beverages ■ Supplying recipes or paraphernalia to make alcoholic beverages ■ Glorifying, touting, or otherwise encouraging alcohol consumption or intoxication
Anonymizer	Sites that offer anonymous access to web sites, often used to bypass corporate and school proxy controls as well as parental control filtering solutions.
Art Nudes	Non-pornographic sites with tasteful and artistic display of the naked body. These sites are not sexually oriented.
Arts	Sites that include the following: ■ Art galleries ■ Artists ■ Museums ■ Visual arts ■ Performing arts ■ Theater ■ Painting ■ Drawing ■ Sculpture ■ Photography
Blogs	'Blog' sites providing commentary on particular subjects including news, politics, and online diaries, that contain the following content types: ■ Text ■ Photo ■ Audio ■ Video

Table 3-1 URL Categories *(continued)*

Category Name	Description
Business	Sites sponsored by or devoted to individual businesses not covered by any other categories. This category includes the following industries: ■ Aerospace ■ Defense ■ Agriculture ■ Biotech ■ Chemical This category also includes the following: ■ Consumer goods and services ■ Industrial goods and services ■ Textiles ■ Transportation and logistics
Caches and Archives	This category filters cached content by extracting the user's original requested URL and comparing it with the URL categorization policies. This category covers the following: ■ Major search engines (for example, Google and Yahoo) ■ Popular cached content sites
Chat	Sites that enable users to chat to other users online, using the following: ■ Text-based chat ■ Internet Relay Chat ■ Instant Messaging ■ Visual chat rooms
Computing and Internet	Sites that provide information about computers, the Internet, and telecommunications, including the following: ■ Software solutions and services ■ Computer and telecommunications hardware, devices, and gadgets ■ Internet and phone access services ■ Technology news

Table 3-1 URL Categories *(continued)*

Category Name	Description
Content Delivery Networks	Websites that are used to deliver software updates and other high-bandwidth applications to corporate customers. This category also includes corporate image servers.
Cult	Sites that promote prominent organized modern religious groups that are identified as cults by three or more authoritative sources. This category includes the following: ■ The Church of Satan ■ Aum Shinrikyo ■ The Hare Krishna movement ■ The Family ■ The Unification Church ■ The Branch Davidians ■ Scientologists.
Dynamic	Sites that have dynamically changing content with the possibility of generating, displaying, or offering links to inappropriate material, including the following: ■ Search engines ■ Directory services ■ Hosting ■ Portals ■ Blogs
Education	Education-related sites including the following: ■ Educational facilities ■ Faculty or alumni groups ■ Public and private schools ■ Home-schooling ■ Universities ■ Colleges
Energy	Sites that represent companies involved with the production and distribution of energy, including the following: ■ Oil ■ Gas ■ Electricity ■ Alternative energy ■ Energy discovery, production, and distribution

Table 3-1 URL Categories *(continued)*

Category Name	Description
Enterprise Webmail	Sites that provide online email services for select communities of users, including the following: ■ Software for providing webmail ■ ISP email and hosting services ■ Business, school, or institutional web email services This category does not include webmail from larger providers (for example, Google, Yahoo, and Hotmail)
Entertainment	Sites related to the entertainment industry including the following: ■ Official web sites of movies ■ Film studios ■ TV stations ■ Fan sites about celebrities and fictional characters ■ Entertainment news and reviews ■ Show times ■ Online shopping for entertainment products such as DVDs, movie and concert tickets
Fashion and Beauty	Sites that emphasize, promote, or provide information on how to achieve physical attractiveness, allure, charm, beauty or style with respect to personal appearance. This category includes the following: ■ Clothes ■ Shoes ■ Hair ■ Make-up ■ Fashion accessories
File Storage and Backup	Sites that allow users to upload files for personal online storage on Internet servers for backup or exchange. This category includes sites for documents or other information, but not photo sharing sites.

Table 3-1 URL Categories *(continued)*

Category Name	Description
Finance and Investment	Finance-related sites including the following: ■ Establishing, planning, researching, or managing personal finances and investments ■ Personal finance and investment portals ■ Buying, trading, or selling financial instruments, commodities, futures, mutual funds, stocks, and equities online or offline ■ Stock quotes, tickers, and fund rates
Food and Dining	Sites that provide information about the following: ■ Food ■ Recipes ■ Speciality food shops ■ Catering ■ Food delivery ■ Restaurant sites, guides, and reviews
Forums and Messageboards	Sites that enable users to participate in the discussion of numerous topics, often with online communities. This category includes the following: ■ Monitored and unmonitored web forums ■ Message boards ■ Discussion forums ■ Bulletin boards
Freeware and Software Download	Sites that offer the download of software online, including the following: ■ Freeware ■ Shareware ■ Open source software

Table 3-1 URL Categories *(continued)*

Category Name	Description
Gambling	Sites that allow users to place bets or participate in a betting pool including the following: ■ Lotteries ■ Obtaining assistance for placing bets ■ Participating in games of chance ■ Casinos ■ Betting ■ Handicappers ■ Sports gambling ■ Bookies ■ Charity gambling ■ Gambling directories
Games	Sites related to computer or video games, game downloads and online game sites, including the following: ■ Computer or video game manufacturers ■ Sites hosting multi-player games ■ Forums and messageboards related to video games ■ Online games
Gore	Sites that display graphic violence and the infliction of pain or injuries, including the following: ■ Gross violence towards humans or animals ■ Scenes of dismemberment, torture, massive blood and gore ■ Sadism and other types of excessive violence
Government	Sites that are sponsored by government branches or agencies, including the following: ■ Local and state government ■ Health and social services ■ Elections ■ Employment ■ Public safety and services ■ Embassies and consulates

Table 3-1 URL Categories *(continued)*

Category Name	Description
Hacking	Sites that promote or provide the means to practice illegal or unauthorized acts of computer crime using technology or computer-programming skills. This category includes the following: ■ Hacker magazines ■ Password, software, or other 'cracks' for download or trading ■ Sites offering software license keys ■ Tools and scripts for hacking
Health and Medicine	Sites that provide information or advice on the following: ■ Personal health or medical services ■ Health insurance, procedures, or devices ■ Information on diets, nutrition, therapies, and counseling services
Hobbies and Recreation	Sites that provide information on private pastimes, including the following: ■ Genealogy ■ Collectibles ■ Crafts
Hosting Sites	Sites that provide individuals or organizations with online systems for storing information, images, video, or any content accessible from the web. This category includes the following: ■ Free or paid hosting ■ Virtual private server hosting ■ Online backup or file storage

Table 3-1 URL Categories *(continued)*

Category Name	Description
Illegal Activity	Sites with illicit content or instructions for threatening or violating the security of property or privacy of people. This category includes the following: ■ Child pornography and pedophilia sites* ■ Theft of money , goods and phone services ■ Lock-picking and burglary ■ Fraud, identity theft, and stealing credit card numbers ■ Telephone crime ■ Evading or circumventing the law * All child-oriented erotic sites are registered with global advocacy groups, including the following: ■ Australian Broadcasting Authority (AU) ■ Bundesministerium für Inneres (AT) ■ Internet Watch Foundation (UK) ■ Interpol ■ Meldpunt (NL) ■ National Center for Missing and Exploited Children (US)
Illegal Drugs	Sites that promote, offer, sell, supply, encourage or advocate the use, cultivation, manufacture, or distribution of illegal drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia.
Image Search	Websites that provide resources for photo and image searches, including the following: ■ Online photo albums ■ Digital photo exchanges ■ Image hosting sites
Intimate Apparel and Swimwear	Sites that display or offer the sale of the following: ■ Lingerie, negligee, and other intimate apparel ■ Bikinis and thongs that are marketed as beachwear rather than swimwear ■ Galleries and videos of bikini models

Table 3-1 URL Categories *(continued)*

Category Name	Description
Intolerance and Hate	Sites that advocate hostility or aggression toward individuals or groups on the basis of race, religion, gender, nationality, ethnic origin, or other involuntary characteristics, including the following: ■ Racism, anti-Semitism ■ White power, white separatism ■ Homophobia, ■ Misogyny, anti-feminism ■ Holocaust denial sites.
Job Search	Sites that provide assistance or tools to help to find employment, including the following: ■ Job search engines ■ Resume banks ■ Recruiters ■ Staffing and temp agencies ■ Referral services ■ Sites promoting career fairs and expos
Kids Sites	Sites that provide a safe Internet experience for children under 12 years of age. Category includes the following: ■ Activities and crafts ■ Coloring and artwork ■ Interactive learning ■ Popular books ■ Children's books publishers ■ Comic heroes ■ Fan sites made for children ■ Age-appropriate gaming portals ■ Age-appropriate singers and pop groups ■ Age-appropriate clubs, leagues, associations, zoos, and other organizations

Table 3-1 URL Categories *(continued)*

Category Name	Description
Law Site	Sites that offer legal content and services, including the following: ■ State and regional laws ■ Criminal and civil law ■ Lawyers and attorneys ■ Legal services and law firms ■ Consultation in particular areas such as personal injury
Lifestyles	Sites that contain general material relevant to sexual orientation, such as the following: ■ Gay ■ Lesbian ■ Bisexual ■ Transgender This includes pages that address or support sexual orientation lifestyle choices, and may be dedicated to the following: ■ Groups ■ Discussions ■ Issues ■ Clubs ■ Personal home pages
Mature	Sites that contain sexually explicit information that is not of a medical or scientific nature. This category includes the following: ■ Discussions or descriptions of sexual techniques or exercises ■ Sexual relationship counseling ■ Products to improve one's sex life ■ Explicit discussions of sex and sexuality ■ Sexual orientation issues ■ Lingerie sales ■ Nudism ■ Naturism
Military	Sites that are sponsored by military branches or agencies as well as official and personal sites related to military history, ideology, or specific branches of the military.

Table 3-1 URL Categories *(continued)*

Category Name	Description
Mobile Phone Downloads	Sites that offer a range of add-ons for handheld devices, including the following: ■ Ringtones ■ Wallpapers ■ Games ■ Videos
Motor Vehicles	Sites that relate to motor vehicles, dealers, sales, and clubs, including the following: ■ Manufacturers of cars, trucks, motorcycles, and other forms of transportation ■ Automotive dealers ■ Online shopping for cars, motorcycles, parts, and accessories ■ Motoring clubs, and associations
Music	Sites related to the music industry, including the following: ■ Radio web sites ■ Band and artist pages ■ Music fan sites ■ Music reviews ■ Music studios ■ Venues ■ Record labels ■ Promotional sites ■ Lyrics ■ Tablature ■ Sheet music
Neutral	Sites that have not yet been categorized, or may never be categorized, into one of the standard categories, but that have been examined and found to not contain offensive content.

Table 3-1 URL Categories *(continued)*

Category Name	Description
News	Sites that primarily report, inform, or comment on current events or issues of the day, including the following: ■ Sports ■ Weather ■ Editorials ■ Human interest news
Nudity	Sites that offer depictions of nude or semi-nude human forms, and are not sexually oriented. This category includes the following: ■ Nude lifestyle ■ Nudism ■ Naturism
Occult	Sites that promote or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, curses, magic powers or supernatural beings, including the following: ■ Magic spells and curses ■ "black" and "white" magic ■ Witchcraft rituals and activities ■ Herbs, tools, or paraphernalia for casting spells ■ Summoning demons ■ Other magical behavior or activities
Peer-To-Peer	Sites that make files available for other users to download over the Internet or smaller private networks. This category includes the following: ■ Centralized Peer-to-Peer Networks (for example, Limewire) ■ Serverless P2P networks (for example, Gnutella) ■ Decentralized client-based networks (for example, KaZaA, eMule, BitTorrent)

Table 3-1 URL Categories *(continued)*

Category Name	Description
Personals and Dating	Sites that promote or provide opportunity for establishing or continuing romantic or sexual relationships, including the following: ■ Dating portals and directories ■ Personal advertisements ■ Cyber relationships, dating services, and international introductions
Pets	Sites and forums related to the care, maintenance, purchase, rescue, or breeding of any animal for companionship and enjoyment, including the following: ■ Pets and pet related sites ■ Pet care ■ Pet products ■ Animal rescue ■ Pet breeding ■ Dog breeds
Philanthropic and Professional Organizations	Sites that are owned by non-profit organizations, including organizations in the following areas: ■ Environment ■ Humanitarian aid ■ Animal protection ■ Education ■ The arts ■ Social issues ■ Charities ■ Health care ■ Politics ■ Religion ■ Research ■ Sports or other endeavors
Phishing and Fraud	Sites that impersonate legitimate business sites, for the purpose of eliciting financial or other private information for users, including the following: ■ Phone service theft advice ■ Other cheating sites

Table 3-1 URL Categories *(continued)*

Category Name	Description
Placeholder	Sites that are typically owned by domain name registrars, domain brokers, or Internet advertising publishers, including the following: ■ Domains for sale ■ Parked domains ■ Expired domains ■ Domains under construction ■ Sites that are "coming soon"
Plagiarism	Sites that are made available for students to plagiarize content from, including the following: ■ School reports ■ Research and term papers on popular school topics
Politics	Sites that relate to the following: ■ Politicians ■ Election campaigns ■ Political organizations and publications ■ Official home pages of politicians and political parties ■ Personal sites about politics and grass-root movements
Portal	Sites that offer a broad array of resources and services, such as email, forums, search engines, and online shopping malls. Portals typically publish their own content or collate multiple sources of information for many areas such as the following: ■ News ■ Entertainment ■ Sports ■ Technology ■ Finance
Real Estate	Sites that are commercial in nature and involved in the real estate business, including the following: ■ Individual brokers and agents ■ Real estate companies ■ Real estate search and property location services ■ Real estate tips and advice

Table 3-1 URL Categories *(continued)*

Category Name	Description
Reference	Sites that contain personal, professional, or educational references, including the following: ■ Dictionaries ■ Encyclopedias ■ Thesauruses ■ Maps ■ Language translation
Religion	Sites that are about religion as any set of beliefs and practices that have the function of addressing the fundamental questions of human identity, ethics, death, and the existence of the Divine.
Science	Sites that provide research materials in the natural and life sciences.
Search	Sites that support the following: ■ Searching the Internet ■ Searching newsgroups ■ Indices and directories of Internet resources
Self-Harm	Sites that describe or discuss ways in which to self harm including the following: ■ Eating disorders ■ Self-harm and self-injury
Sex Education	Sites that provide educational information on the following: ■ Reproduction and sexual development ■ Sexually transmitted diseases (STDs) ■ Contraception ■ Safe sexual practices ■ Sexuality ■ Sexual orientation
Shopping	Sites that provide the means to purchase products or services online, including the following: ■ Internet malls ■ Online auctions ■ Department and retail stores' online catalogs

Table 3-1 URL Categories *(continued)*

Category Name	Description
Social Networking	Sites that enable a group of people to communicate and interact on the Internet. This category includes the following: ■ Social networking, chat, and instant messaging ■ Forums and message boards ■ Hosting of home pages and other user-generated content
Spam URLs	Website URLs found in spam email, including the following: ■ Computing ■ Finance and stocks ■ Entertainment ■ Games ■ Health and medicine ■ Humor and novelties ■ Personal and dating ■ Products and services ■ Shopping ■ Travel
Sports	Sites that promote or provide information about spectator sports. including the following: ■ Professional and collegiate sports teams ■ Player and fan sites ■ Scores and schedules ■ News, statistics, and discussion
Spyware	Sites that provide or promote information gathering or tracking that is unknown to, or without the explicit consent of, the end user or organization, including the following: ■ Sites that carry malicious executables or viruses ■ Third-party monitoring ■ Malware with ‘phone home’ destinations
Streaming Media	Sites that host streaming media including the following: ■ Television ■ Movies ■ Video ■ Radio

Table 3-1 URL Categories *(continued)*

Category Name	Description
Suicide	Sites that describe or promote suicide, including the following: ■ Newsgroups, chat rooms, and message boards ■ Descriptions, instructions, and depictions of methods, systems and computers
Tobacco	Tobacco-related sites, including the following: ■ Offering tobacco for sale ■ Promoting or encouraging the consumption of tobacco. This category includes the following: ■ Retailers ■ Manufacturers ■ Products ■ Paraphernalia ■ Smoking lessons
Travel	Sites that promote or provide opportunity for travel planning, including the following: ■ Finding and making travel reservations ■ Travel portals and packages ■ Air travel and carriers ■ Tickets, reservations, charters and rentals for cars trains, buses, boats, and motorcycles
Unclassified	Sites that are not categorized in the Web Security database, possibly for the following reasons: ■ The site has only recently been created ■ The site has not been in use
Violence	Sites that advocate or provide instructions for causing physical harm to people or property through the use of weapons, explosives, pranks, or other types of violence, including the following: ■ Explosives and bombs ■ Descriptions or instructions for killing people

Table 3-1 URL Categories *(continued)*

Category Name	Description
Voice Over IP	Sites that enable users to make telephone calls over the Internet or obtain information or software for this purpose, including the following: ■ VOIP ■ PC-to-PC, PC-to-phone, and phone-to-phone services connecting over TCP/IP networks
Weapons	Sites that describe or offer for sale weapons, including the following: ■ Guns, ammunition, firearm accessories ■ Knives ■ Martial arts ■ Descriptions, reviews, and specifications of weapons ■ Weapons retailers, and manufacturers ■ Weapon auctions, and trading centers ■ Instructions for manufacturing weapons
Webmail	Sites that provide free Web-based email services, accessible through any Internet browser (for example, Yahoo, Hotmail, and Google)
Wedding	Sites related to the traditions, customs, planning, and products involved in a marriage or commitment ceremony as well as in civil unions, including the following: ■ Wedding planning ■ Wedding products ■ Alternative commitment ceremonies

See "Checking the URL categorization for a website " on page 53.

About URL category changes

The categories in the Web Security URL Filtering service have been modified since the service was first released.

Any URL categories selected under the old settings are mapped to their closest equivalent categories under the new settings. These new settings are appropriate to maintain the same level of protection as previously. However, to take full advantage of the new categories available, we recommend that you review all your rules and select the new categories where appropriate.

For full details of the new categories, see the following:

See “About URL categories” on page 31.

See “Checking the URL categorization for a website ” on page 53.

The old categories, and their closest equivalent new categories, are as follows:

Table 3-2 Old categories mapped to new names

Old category name	New category name
Adult/Sexually Explicit	Adult/Sexually Explicit
Adult/Sexually Explicit	Art Nudes
Adult/Sexually Explicit	Lifestyles
Adult/Sexually Explicit	Mature
Adult/Sexually Explicit	Nudity
Advertisement and Popups	Advertisement and Popups
Alcohol and Tobacco	Alcohol
Alcohol and Tobacco	Tobacco
Arts	Arts
Blogs and Forums	Blogs
Blogs and Forums	Forums and Messageboards
Business	Business
Business	Energy
Caches and Archives	Caches and Archives
Chat	Chat
Computing and Internet	Computing and Internet
Criminal Activity	Illegal Activity
Downloads	File Storage and Backup
Downloads	Freeware and Software Download
Education	Education
Education	Science

Table 3-2 Old categories mapped to new names *(continued)*

Old category name	New category name
Entertainment	Entertainment
Entertainment	Music
Fashion and Beauty	Fashion and Beauty
Finance and Investment	Finance and Investment
Food and Dining	Food and Dining
Gambling	Gambling
Games	Games
Government	Government
Government	Law Site
Government	Military
Hacking	Hacking
Health and Medicine	Health and Medicine
Hobbies and Recreation	Hobbies and Recreation
Hobbies and Recreation	Pets
Hosting Sites	Hosting Sites
Illegal Drugs	Illegal Drugs
Infrastructure	Content Delivery Networks
Intimate Apparel and Swimwear	Intimate Apparel and Swimwear
Intolerance and Hate	Intolerance and Hate
Job Search and Career Development	Job Search
Kids Sites	Kids Sites
Motor Vehicles	Motor Vehicles
News	News
Peer-to-Peer	Peer-to-Peer
Personals and Dating	Personals and Dating

Table 3-2 Old categories mapped to new names *(continued)*

Old category name	New category name
Personals and Dating	Social Networking
Philanthropic and Professional Organizations	Philanthropic and Professional Organizations
Phishing and Fraud	Phishing and Fraud
Photo Searches	Image Search
Politics	Politics
Proxies and Translators	Anonymizer
Real Estate	Real Estate
Reference	Law Site
Reference	Reference
Religion	Abortion
Religion	Cult
Religion	Occult
Religion	Religion
Ringtones and Mobile Phone Downloads	Mobile Phone Downloads
Search Engines	Portal
Search Engines	Search
Sex Education	Sex Education
Shopping	Shopping
Society and Culture	Wedding
Spam URLs	Spam URLs
Sports	Sports
Spyware	Spyware
Streaming Media	Streaming Media
Travel	Travel
Unclassified	Unclassified

Table 3-2 Old categories mapped to new names *(continued)*

Old category name	New category name
Violence	Gore
Violence	Self-Harm
Violence	Suicide
Violence	Violence
Weapons	Weapons
Web-based Email	Enterprise Webmail
Web-based Email	Webmail
(No corresponding old category)	Voice Over IP
(No corresponding old category)	Placeholder
(No corresponding old category)	Neutral
(No corresponding old category)	Dynamic
(No corresponding old category)	Plagiarism

Checking the URL categorization for a website

The **URL Categorization** query tool enables you to view the categories that are assigned to a specific website. You can also request a category to be changed.

Some websites may be categorized differently for different subdomains. For example, http://finance.yahoo.com has a different categorization than http://shopping.yahoo.com.

If any website appears to be in an inappropriate category, you can submit a request for recategorization. Your request ensures that the website is reviewed. You will receive a response within two working days.

Note: The **URL Categorization** query tool is available as a portlet on the Dashboard, as well as within the configuration pages for Web URL Filtering service.

To check the URL categories for a website

1. In the portal, click **Web Security Services** > **Web URL Filtering** > **URL Categorization**.
2. In the box, enter the full URL to check and click **Categorize**.

   Include http:// or https:// in the URL, as appropriate.

   The URL categories for the website are listed. Or the site is shown as uncategorized.

To request a category to be changed

1. In the portal, click **Web Security Services** > **Web URL Filtering** > **URL Categorization**.
2. In the box, enter the full URL to check and click **Categorize**.

   Include http:// or https:// in the URL.

   The URL categories for the website are listed. Or the site is shown as uncategorized.
3. Click **Recategorize**.

   A **Recategorize URL** form opens. Your account details are shown.
4. Complete the following:

URL	The full URL of the website to be checked. The URL is already completed for you.
Proposed Category	Select the category that the website should use.
Justification	State the reasons why the website should be recategorized.
Email Address	The email address that the email response to the request is sent. The email address that is associated with your login account is entered for you. You can change the email address, as required.

5. Click **Submit**.

   You should receive an email response to your request within two business days.
6. Click **Close**.

Using example URL categories for testing purposes

For initial testing purposes, we recommend that you set up some test rules. These test rules should use URL categories that are unlikely to offend any users who have access to test web sites that you intended to block.

To set up your list of categories, use the URL Categorization tool to check the URL categories that are assigned to several web sites of your choice,.

To test your URL filtering rules

1. Set up a rule that allows access to a specific URL category, and verify that you can access some web sites that are assigned to that category.
2. Set up a rule to block access to a URL category, and verify that you are denied access to some web sites in that category.
3. When you are satisfied that the logic of your rules works as expected, you can replace your test categories with the actual ones you want to block or allow in your rules. You can then be confident that they are set up correctly.

See "Checking the URL categorization for a website " on page 53.

About reporting

Extensive reporting features are available in the portal; graphically through the services dashboards, and through summary reports (PDF), detailed reports (CSV), and audit report (PDF). You can also define scheduled reports to be emailed to a recipient that you define, on a regular basis.

Where the URL Filtering categories available for use in rules have changed, bear in mind that the reporting period you select may include information from the old and the new categories.

Chapter 4

Support for HTTPS Inspection

This chapter includes the following topics:

About HTTPS Inspection

HTTPS Inspection adds support for the scanning of SSL encrypted Web traffic to your Web Security services. In the portal, you configure HTTPS Inspection to your requirements, and activate the service. By default HTTPS Inspection is turned off.

When you implement HTTPS Inspection, SSL encrypted web traffic is routed through the Web Security service infrastructure. With HTTPS Inspection turned on, the following occurs:

- SSL encrypted web traffic is scanned for malware
- SSL encrypted web traffic is included in the time and the bandwidth quotas that you establish in your URL Filtering policy rules
- SSL encrypted web traffic is included in your Web URL Filtering policies
See "About HTTPS Inspection and Web URL Filtering" on page 57.

To configure HTTPS Inspection, you choose whether to exclude a website from HTTPS Inspection. You also choose whether you want your users to be able to access sites with certificate errors. By default, when you activate HTTPS Inspection, sites with certificate errors are blocked When a user tries to access a site with a certificate error, a user alert is displayed. You can customize the alert to suit your requirements.

You can choose to include SSL encrypted web traffic in the Web Security audit, detailed, and summary reports. The key statistics that appear on the Dashboard for Web Security include SSL encrypted web traffic

About HTTPS Inspection and Web URL Filtering

Without HTTPS Inspection, URL filtering of HTTPS requests can still occur. When a URL with an HTTPS protocol name is accessed in the browser, a `CONNECT` request is made with the initial domain. So, for *https://www.example.co.uk/login* the initial domain *www.example.co.uk* is used as the request URI. Web URL Filtering uses the request URI in your policies. For example, if you create a block rule with an entry of **.example.co.uk/**, the URL *https://www.example.co.uk/login* is still blocked even without HTTPS Inspection. To clarify, the `CONNECT` URI doesn't contain the path, only the domain (i.e., www.example.co.uk), and the domain is compared to the pattern for policy enforcement.

However, without HTTPS Inspection a more specific URL is not blocked. A block rule with an entry of **.example.co.uk/login** does not block *https://www.example.co.uk/login*. The block fails because the full URL is not made available by the `CONNECT` request to our policy validation engine. With HTTPS Inspection enabled, the full URL is available for validation. In this example, Web URL Filtering is able to block access to *https://www.example.co.uk/login* and display a user alert.

The same principle applies to filtering by URL category. Without HTTPS Inspection, the URL made available for validation against the URL category is the domain contained in the `CONNECT` request, and not the full URL. With HTTPS Inspection,

the full URL is validated against the URL category in the filtering rule. When you turn on HTTPS Inspection, the results of URL filtering by category may vary.

Implementation considerations for HTTPS Inspection

HTTPS Inspection is compatible with both on-site and roaming implementations of Web Security.

Web Security does not provide compatibility with SSL transparent proxy. This type of deployment often requires the implementation of other network devices that are not required in our normal deployment. Adding equipment presents potential compatibility issues, as all network devices must work together.

Table 4-1 HTTPS Inspection - considerations in use

Issue	Description
Customization of user alerts with non-secure content	You can customize the user alert that you display to your users when they try to access a website with a certificate error. When you customize an alert, you might add links to branding elements, such as your company logo. This content may be non-secure. If you include HTTP content in the custom user alert, a warning appears. The warning asks if the user wants to view both secure and non-secure data. If the user chooses yes, the full user alert is displayed with both secure and non-secure content . If they choose no, only the secure parts of the alert are shown. See "Customizing user alerts for HTTPS Inspection" on page 65.
Applications that use client-side authentication	Applications that use client-side authentication may cause an issue. An example of such an application is the Dropbox desktop application, also known as the Dropbox client. When you connect directly to the cloud infrastructure, the Dropbox client is unable to accept our certificate, and reports an error. Note, however, that you can access your Dropbox account through a web browser that uses the appropriate certificate store.

Table 4-1 HTTPS Inspection - considerations in use *(continued)*

Issue	Description
Use of self-signed certificates	If your organization uses a self-signed certificate to authenticate a site, Web Security blocks the site and displays a user alert. To avoid this issue, add the site to the list of sites that you want your users to be able to access. Adding the site in this step is advisable even if there is a problem with the site's certificate. See "Allowing access to sites with certificate errors" on page 64.
User alert is not displayed in some circumstances	This issue can occur when a user tries to download a file that a Web URL Filtering policy has blocked. An alert is not displayed to inform the user that your organization's Web URL filtering policy has prevented access to the file. This issue has been reported with the Norton Zone secure file sharing service, Google's Gmail service, and it may affect other services.

Implementing HTTPS Inspection - process overview

The following table provides an overview of the procedure for implementing HTTPS Inspection:

Table 4-2 Steps for implementing HTTPS Inspection

Step	Action	Details
Step 1	Review your business requirements for HTTPS Inspection	You can exclude a site, or a category of site, from HTTPS Inspection. When you exclude sites from HTTPS Inspection, encrypted web traffic for these sites bypasses the Web Security infrastructure, and is not scanned for malware of included in your Web URL Filtering policy rules. You can allow your users to browse specific sites with certificate error. See "About HTTPS Inspection" on page 56. See "About HTTPS Inspection and Web URL Filtering" on page 57.
Step 2	Review the compatibility requirements for HTTPS Inspection	See "Implementation considerations for HTTPS Inspection" on page 58.

Table 4-2 Steps for implementing HTTPS Inspection *(continued)*

Step	Action	Details
Step 3	Download the Symantec Web Security.cloud Root CA from the portal and install it on all browsers.	You install the certificate in the certificate store of all browsers in your organization that connect to our infrastructure. This step is necessary to ensure that the browser authenticates the Symantec Web Security.cloud Root CA and does not report a certificate error. See "Downloading the Symantec Web Security.cloud Root CA" on page 61.
Step 4	Configure HTTPS Inspection to your requirements.	To configure HTTPS Inspection, do the following: ■ Enter the websites that you want to exclude from HTTPS Inspection. You can add individual sites to a list or create a list of URL categories. All sites that belong to that URL category are excluded from HTTPS Inspection. See "Excluding sites from HTTPS Inspection" on page 63. See "Excluding URL categories from HTTPS Inspection" on page 62. ■ Enter the websites that you want to allow your users to access, even if there is a problem with a site's certificate. For these sites, the certificate errors are not displayed to the user. See "Allowing access to sites with certificate errors" on page 64.
Step 5	Review the alert that is displayed when a user tries to access a site with a certificate error.	You can use the default user alert or replace it with your own version. See "Customizing user alerts for HTTPS Inspection" on page 65.
Step 6	Turn on HTTPS Inspection	In the portal, you configure HTTPS Inspection and turn it on. See "Activating HTTPS Inspection" on page 67.
Step 7	Use the reporting functionality in the portal to view data on SSL encrypted web traffic.	You can include SSL encrypted web traffic in your Audit, Detailed, and Summary reports. When you activate HTTPS Inspection, SSL encrypted web traffic is included in the Web Security service statistics on the Dashboard. See "About reporting and HTTPS Inspection" on page 67.

Downloading the Symantec Web Security.cloud Root CA

When you activate HTTPS Inspection, SSL-encrypted web traffic is routed through the Web Security infrastructure. Before you turn on HTTPS Inspection for your Web Security service, you must do the following:

- Download the Symantec Web Security.cloud Root CA from the portal.
- Install the certificate on all of the web browsers that are connected to the Web Security service.

  Take this step to ensure that the Symantec Web Security.cloud Root CA is correctly authenticated by your users' browsers. If you do not install the certificate on each browser, users receive a certificate error when they access a website using HTTPS.

To download the Symantec Web Security.cloud Root CA from the portal

1. In the portal, click **Tools** > **Downloads**
2. Click the link for the **Symantec Web Security.cloud Root CA** and save the certificate to a suitable location.

You must install the certificate on all browsers that connect to the Web Security service infrastructure. You can install the certificate by using a number of different methods, as listed here.

Manually adding the Symantec.cloud root certificate to the certificate store

1. Run **MMC.exe**.
2. Choose **File** > **Add/Remove snap-in**.
3. Select **Certificates** and click **Add**.
4. Choose **Computer Account** and click **Next**.
5. Select **Local computer** and click **Finish**.
6. Click **OK** to add the Certificates snap-in to MMC.
7. Expand **Trusted Root Certification Authorities**, right-click **Certificates**, and choose **Import**.
8. At the welcome page click **Next**.
9. Browse to locate the certificate file, select the file name, and click **Next**.
10. Ensure that the certificate is placed in the **Trusted Root Certification Authorities** store, and click **Next**.
11. Click **Finish** to import the certificate.

Automatically adding the Symantec.cloud root certificate to the certificate store using Group Policy

1. Edit the appropriate group policy. For example, **Default domain policy**.
2. Navigate to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies** > **Trusted Root Certification Authorities**.
3. Right-click **Trusted Root Certification Authorities** and choose **Import**.
4. Browse to the copy of the Symantec.cloud root certificate and click **Next**.
5. Confirm that the certificate is placed in the correct certificate store, and click **Next**.
6. Click **Finish** to import the certificate into the Group Policy.

   The Group Policy setting takes effect after the affected computers have been restarted.

The **Google Chrome** web browser uses the local certificate store on each users' computer. Google Chrome is compatible with either method of manually importing a certificate or automatically importing a certificate with Group Policy.

The **Mozilla Firefox** web browser does not use the computer's certificate store, but instead has its own store for root certificates.

Manually adding the Symantec.cloud root certificate to Mozilla Firefox

1. Open an instance of your Mozilla Firefox browser.
2. On the Firefox home page, click on **Settings** and then click the **Advanced** tab.
3. Click on **View Certificates**.

   The Certificate Manager window opens.
4. Select the **Authorities** tab, click **Import**, and browse to the certificate file and click **OK**.

   The Downloading Certificate window opens.
5. Check the **Trust this CA to identify websites** check box and click **OK**.
6. Click **OK** to close the Certificate Manager window.
7. Click **OK** to close the Options window.

Excluding URL categories from HTTPS Inspection

You can apply a URL categorization policy to your HTTPS Inspection policy. For example, you can decide to inspect all sites with a URL category of Webmail, but

choose not to inspect sites with a category of Finance and Investment. You can continue to update this list after you have activated HTTPS Inspection.

Note: You can choose to exclude a URL category from HTTPS Inspection. SSL-encrypted web traffic for the sites that belong to an exclusion category passes through our infrastructure but is not decrypted. Non-encrypted (HTTP) web traffic for the sites also continues to pass through our infrastructure.

To exclude a URL category from HTTPS Inspection

1. Select **Services** > **Web Security Services** > **HTTPS**.
2. In the **Ignore SSL encrypted web traffic - by URL category** section, click **Edit URL Categories**.

   The **Edit URL Categories** dialog is displayed.
3. Select the categories that you want to exclude from HTTPS Inspection.
4. Click **Ok** to save the list.

Excluding sites from HTTPS Inspection

You can create a list of sites that you want to exclude from HTTPS Inspection. For example, you might need to ensure that SSL connections to sites holding personal or sensitive information are not intercepted to comply with regulations concerning data privacy in your country.You can continue to update this list after you have activated HTTPS Inspection.

Note: When you exclude a site from HTTPS Inspection, SSL encrypted web traffic for the site does not pass through our infrastructure. Non-encrypted web traffic for the site continues to pass through our infrastructure.

To exclude a site from HTTPS Inspection

1. Select **Services** > **Web Security Services** > **HTTPS**.
2. In the **Ignore SSL encryted web traffic - by website or IP address** section, click **New**.

   The **Add Website/IP Address** dialog is displayed.
3. Complete the **Website/IP address** and **Description** fields. Note the following:
   - You can add the site as a web address or as an IP address
   - You do not need to add https:// to the start of the web address or IP address.

- You can use the asterisk (*) wildcard in the web address.
  For example, type **.example.com* to specify all the sites for the *example.com* domain. The wildcard must appear before the domain name and you can use only one wildcard in the address.

4 Click **Add** to save the entry to the list.

Note: The maximum number of sites that you can add to this list is 1000.

---

5 To activate the site set the ON/OFF switch in the **Active** column to ON.

Allowing access to sites with certificate errors

You can enter a list of sites that you want your users to be able to access, even if there is a problem with the site's certificate. For these sites, no user alert is displayed and the user is able to browse the site. The user is not presented with any warning and is therefore not aware that there is a problem with the site's certificate.

Warning: Consider the security implications of allowing your users to ignore certificate errors for a site. A certificate authenticates the identity of the company behind a site. A certificate error can indicate that the certificate is fake, compromised, or has been tampered with.

For the sites on the exceptions lists, SSL encrypted web traffic is still routed through our Web Security infrastructure.

To allow your users to access specific sites with certificate errors

1 Select **Services** > **Web Security Services** > **HTTPS**.

2 In the **Allow access to sites with certficate errors** section, check the **Enable site bypass list** checkbox.

3 Click **Allow** to confirm.

4 Click **New** to display the **Add Website/IP Address** dialog.

5 Complete the **Website/IP Address** and **Description** fields. Note the following:

- You can add the site as a web address or as an IP address
- You do not need to add https:// to the start of the web address or IP address.
- Use of the asterisk (*) wildcard in the web address or IP address is not supported.

6 Click **Add** to save the site to the exceptions list.

Note: The maximum number of sites that you can add to this list is 1000.

7 To activate the site set the ON/OFF switch in the **Active** column to ON.

Blocking access to sites with certificate errors

Note: When you activate HTTPS Inspection at your organization, all sites with certificate errors are blocked by default.

When a user tries to access a site with a certificate error, a user alert is displayed. The alert informs the user that there is a problem with the site's certificate.

To block access to all sites with certificate errors

1 Select **Services** > **Web Security Services** > **HTTPS**.

2 In the **Allow access to sites with certficate errors** section, review the setting of the **Enable site bypass list** checkbox.

- If the **Enable site bypass list** checkbox is unselected, all sites with certificate errors are blocked, and a user alert is displayed
- If the **Enable site bypass list** checkbox is checked, you can enter sites that you want your users to access in an exceptions list.

3 To block access to all sites with certificate errors, uncheck the **Enable site bypass list** checkbox.

4 Click **Block** to confirm.

The bypass list is hidden and you can no longer add or remove entries. However, any sites that you have added to the list, whether active or inactive, are retained in memory. If you check **Enable site bypass list** once again, the list reappears in the HTTPS Inspection page.

Customizing user alerts for HTTPS Inspection

We provide a default user alert. When you turn on HTTPS Inspection, this alert is automatically used. You cannot turn off user alerts. The default behavior is for the system to block a site with a certificate error and display a user alert. You can enter exceptions to this behavior and allow your users to access a site with certificate errors.

You can create your own custom alert to display when a user tries to access a site with a certificate error. For example, you might want to add the following to the message:

- Your organization's branding elements, for example, a company logo
- A link to your organization's policy for use of the web.

Note that when you add HTTP content to the alert, a warning message is displayed, before the alert is shown to the user.

See "Implementation considerations for HTTPS Inspection" on page 58.

To customize a user alert

1. Select **Services** > **Web Security Services** > **HTTPS**.
2. In the **Allow access to sites with certificate errors** section, click **Edit User Alert**.

   The **HTTPS Inspection: User Alerts** dialog is displayed.
3. Review the default alert. This message is displayed to the user when they browse a site with a certificate error.
4. To customize the alert, select **Use Custom notification message** from the drop-down. The text for the default alert is displayed for you to update.
5. To create an alert in a different language, select from the drop-down. For example, to create an alert in Japanese, select **ja-JP**. When the alert is displayed to the user the following appear in Japanese:
   - The reason for the certificate error
     You add the reason for the error to the alert in the following step.
   - The URL category of the site that generated the certificate error
     You add the URL category in the following step.
6. Make the required changes to the text. You can format the text with HTML tags, to bold and center the title of the message, for example. You can add placeholders to provide additional information to the message. Choose from the following placeholders:
   - URL
     Adds the URL of the site that generated the certificate error.
   - Reason
     Adds the reason for the certificate error, for example *Self signed SSL certificate*, or *Certificate has been revoked*.
   - URL category

Adds the URL category name of the website that generated the certificate error.

7 Click **Save** to save your custom alert.

Activating HTTPS Inspection

In the portal, you configure HTTPS Inspection and turn it on.

To activate HTTPS Inspection

1 Select **Services** > **Web Security Services** > **HTTPS**.

2 Configure the service to your requirements.

3 At the top of the **HTTPS Inspection** page, set the ON/OFF switch to ON.

About reporting and HTTPS Inspection

You can choose to include SSL encrypted web traffic in your Web Security audit, detailed, and summary reports. For some reports, an HTTP column appears on the report, and the entry indicates whether the entry is HTTP or HTTPS. For other reports the content is aggregated, and encrypted and non-encrypted traffic is included in the same line.

If you have turned on HTTPS Inspection, the statistics that are displayed on the Dashboard for your Web Security service include SSL encrypted web traffic. For example, with HTTPS Inspection turned on, the URL requests which triggered a block rule data item includes requests made to sites with the HTTPS protocol name.

To include SSL encrypted web traffic in your reports

1 Click **Reports** > **Report Requests**.

2 Do one of the following:

- Choose an existing detailed, audit, or summary report
- Click **Request a new report**, provide a name for the report and click **Continue**.

3 In the **Web data** section, select **advanced settings** for the required report type.

The **Apply optional filters to this data** dialog is displayed.

4 In the **Protocol** section, choose from the following options

- Both
  Include statistics for both HTTP and HTTPS traffic.

- HTTPS
  Include statistics for HTTPS traffic only.
- HTTP
  Include statistics for HTTP traffic only.

5 Click **Add** to save the settings for your report.

6 Complete the report request, specifying the reporting period, the method of delivery, and so on.

7 In the **Confirm request** step, click **Submit request**.

See “Activating HTTPS Inspection” on page 67.

Chapter 5

Web quotas

This chapter includes the following topics:

About web quotas

Web quotas are a function within Web Security to enable administrators to restrict the amount of time (in hours and minutes) or the volume of data (in MB) for their end users to browse the web. Users are permitted to access the web at any time of day that the policy rules permit, but not to spend excessive amounts of time or bandwidth browsing the web.

Web quotas can be set for individual users, or as a single setting for all users at the organization, as preferred.

About bandwidth quotas

Bandwidth quotas are imposed based on the size of content downloaded or uploaded.

- A rule may specify a file type (extension or content type). Bandwidth is accumulated against only those types.
- Bandwidth is only accumulated against the actual size of the file downloaded; it does not include any updated bandwidth, headers, or protocol overhead.
- Bandwidth is only accumulated if a complete file is delivered to the user; files blocked due to infections or a user canceling are not accumulated.

About time quotas

Time quotas are imposed based on the sum of the browsing session times.

- The minimum time quota activity period is three minutes.
- Idle time does not count against a quota.

Note: If a web request is received, another request is received one minute later, and then no further requests are received, the user consumes four minutes of time quota.

About continuous browsing

If an HTTP request is made before the end of the previous session, the session is considered continuous. If an HTTP request is made after the end of the last session, so that the two sessions do not overlap, the sessions are considered distinct and the period between these sessions is considered idle time (that is, time not spent browsing).

- Streaming media that involves a single request accumulate only one three-minute block of time against the quota limit, even if the request is streamed for several hours.
- Once a user has exceeded their quota for a rule, content prohibited by that rule is blocked commencing with the next matching access.

A single browsing session may last for three minutes or for many hours, depending on the frequency of activity. The session ends three minutes after the last request is received. The time quota consumed is then based on the total duration of that session. The next session starts when everything in the previous session has downloaded and there has been some idle time before the next request is received.

A web application that regularly polls the Internet continues to count against a time quota. For example, an application that polls every two minutes starting at 00:00 and finishing at 00:56 consumes 59 minutes of time quota, and the session ends at 00:59. This counts as one continuous session.

A request for streaming content consumes only one three-minute session of time quota regardless of the actual time spent streaming the requested material. However, the streaming data contributes to any bandwidth quota that may be in operation. All web requests for content contribute to a bandwidth quota, regardless of the content type.

About canceled downloads

In the event that a user cancels an in-progress download, the bandwidth already delivered to the user is not counted against the quota.

About file types

If a file type (extension or content type) is specified in the quota rule, time or bandwidth is accumulated against all files of that type.

If specific file types are not specified in a rule, the following file types accumulate time or bandwidth against the quota limit:

- HTML/text
- Video and audio media types (including streaming media)
- Flash

About the web browser state

The state of the web browser (for example whether it is closed or open; or using multiple tabs or multiple instances) is irrelevant. Quotas are based on the web requests that are made.

Enabling web quotas

The web quotas functionality is always available, and does not need to be specifically enabled. To use Quotas, you must set up appropriate rules in your web policy with the action set to **Quota** or **Quota & Log**. For information on setting up these rules:

Disabling web quotas

To disable the web quotas feature, reset all the relevant rules in the policy to Inactive.

To deactivate a quota rule

1. Click **Services** > **Web Security Services** > **Web URL Filtering**.
2. Click on **Policy Rules**
3. Select the required rule
4. In the **Rule Status** column, click **Active**.

   The rule status changes to Inactive.

   Making a rule Inactive retains all its settings. Set the rule to Active again if you want to turn it on again.

Note: Deleting any required settings from a Quota rule results in the rule being disabled. Appropriate settings must be reentered before the rule can be set to Active.

About configuring web quotas

Web quotas are configured using Web URL filtering policy rules.

Rules can be set to Quota or Quota & Log. Logging is recommended for the initial setting, so that you can monitor that the rules are operating as you expected. Once you are satisfied that the Quota rules are doing what you require, you can turn off the logging while maintaining the same Quota restrictions, if you want.

Once a rule has been set to either **Quota** or **Quota & Log**, the Quotas tab is enabled. This setting lets you set the details of the time or bandwidth Quotas to be

applied for the users or groups to whom that rule applies. Time and bandwidth Quotas can be applied in the same rule.

For instructions on how to set up a Quota rule:

See "Defining web quotas rules" on page 73.

About web quota restrictions

The following restrictions apply to web quotas:

- A time quota cannot be set to more than 24 hours.
- A time quota cannot be set to longer than the time period for which the rule is active. For example, a two-hour time quota cannot be set for a rule only active between 12:00 and 13:00 (1 hour).
- A bandwidth limit cannot exceed 1 PB (1,000,000,000 MB).
- Quotas are not applied to HTTPS content, unless you activate HTTPS Inspection.
  See "About HTTPS Inspection" on page 56.
- Files larger than 0.5 MB are streamed back to the user while being downloaded to the Web Security server for inspection.
  If such a request is blocked due to quota enforcement, the file being streamed back is truncated and the user receives an incomplete, corrupted download. Bandwidth is not accumulated against any rule.
- For a request to save a web link as a file that is made after the quota has expired and the request is blocked, the notification message is saved as the file.
- User quota limits will only be accumulated against custom or synchronized users. If a group contains non-user members (such as IP addresses), user quotas will not be accumulated against the non-user members.

Defining web quotas rules

To set up a rule to apply web quotas restrictions to your users

1. Click **Services** > **Web Security Services** > **Web URL Filtering**.
2. Select the required rule or click **New Rule**. The **Policy Rules** window is displayed.
3. Click the **Rule** tab.
4. Enter an appropriate rule name.
5. In the **Rule** action drop-down list, select either **Quota** or **Quota & Log**. The **Quotas** tab is enabled.

6 Click the **Quotas** tab.

If any time periods have been configured under the **Time** tab, they are displayed in the **Time Period** box and can be selected for the Quota to be applied to.

7 In the **Apply Quota** section, do one of the following:

- Click **Per User** to apply this Quota rule for individual users
- Select **Shared for all users** to use a single Quota setting for all users.

8 If you want to restrict users by the amount of time they spend browsing the web, check **Apply time quota** box. Then specify the **hours** and **minutes** for the total browsing time. This time is either applied for each individual user or is the total time allowance for all users, depending on whether **Per user** or **Shared for all users** was selected previously.

9 To set this Quota rule to restrict users by the amount of bandwidth they use when browsing, check **Apply bandwidth quota** and specify the **MB** of data permitted to be transferred, in whole megabytes. This bandwidth either applied for each individual user or is the total bandwidth allowance for all users, depending on whether **Per user** or **Shared for all users** was selected previously.

If both time and bandwidth are selected for this Quota rule, whichever limit is reached first is applied.

10 Complete the entries under all the other tabs as appropriate, then click **Save and Exit**. A message is displayed to confirm that your rule has been set up.

11 Click **Policy Rules** to view the complete list of rules in your web policy. In the **Rule Status** column, this new rule is shown as **Inactive** until you click it to make it **Active**.

Note: The default **Time Zone** displayed is used for resetting the Quota amounts at 00:00 daily.

See "Defining time period rule conditions" on page 24.

About users and groups for quotas

The Quotas feature uses the same custom and synchronized groups that are set up for use with Web Security policies. If you are configured to use web roaming, the same policies apply to users when they are in the office or are roaming.

The following links direct you to further information about users, groups and how to manage them.

- To understand the general principles of users and groups in Web Security:
  See "Checklist - creating user-specific and group-specific URL filtering policies" on page 21.
- For details of importing user and group information from your Active Directory (AD).
- For details of setting up users and groups manually.

Configuring web quota alerts

When a user is blocked from web browsing as a result of their quota limit of time or bandwidth being reached, a message is displayed in their web browser .

To set the quota alert message to be displayed

1. Click **Services** > **Web Security Services** > **Web URL Filtering** > **Alerts** > **Quota Alerts**.
2. To use the system default message, select the **Use Default** radio button.
3. To use your own custom message, click **Use Custom**.
4. To configure the custom message, type your text in the **Custom User Message** box. Use HTML to format the message and insert links, if required. For example, it may be useful to insert a link for a user to send an email to your system administrator or the Support team.

Note: A user sees this custom message only when their web browsing has been blocked after they reach their Quota limit. As a result, they cannot follow any links to external web sites.

Monitoring web quotas

To monitor your users' utilization of their allocated Quotas, set the appropriate rules to the **Quota & Log** action. The reports can then be viewed in the usual way.

To change a Quota rule's action to include logging

1. Click **Services** > **Web Security Services** > **Web URL Filtering**.
2. In the **Rule** column, click the name of the required rule to edit it.
3. Under the **Rule** tab, in the **Rule Action** drop-down list, click **Quota & Log**
4. Select **Save and Exit**.

Resetting web quotas

Web Quotas are reset automatically daily at 00:00 (in the default timezone).

You can reset the quota allowances for rules or users to permit browsing beyond the Quota limit of time or bandwidth.

To reset web quotas for a rule or all rules

1. Click **Services** > **Web Security Services** > **Web URL Filtering** > **Policy Rules**.

   The list of rules is displayed.

2. To clear the quotas for all rules, click **Clear All Quotas** at the top of the list of rules.

   This option is only enabled if there is at least one Quota-based rule that is set up. Clearing the Quotas has no effect on any non-Quota rules.

3. To clear the quotas for a particular rule, click the option next to that rule to select it. Then click **Clear Quotas For Selected** at the top of the rules list.

   This option only appears if there is at least one Quota-based rule that is set up. Clearing the Quotas has no effect on any non-Quota rules.

4. At the confirmation box, click **OK** to proceed with clearing the Quotas. The Quotas are cleared immediately, and there is no need to click **Save and Exit** only to clear the Quotas.

To reset web quotas for a user or all users in custom groups

1. Click **Services** > **Web Security Services** > **Web URL Filtering** > **Custom Groups**.
2. Click on the group that contains the users to reset qutoas for.
3. Select the **Users** tab.
4. Check the checkbox for all the users to have their Quotas reset, or the checkbox on the header line to select all users.
5. Click **Clear Quotas For Selected**.

   This option is only enabled if there is at least one Quota-based rule set up. Clearing the Quotas has no effect on any users who are not included in any Quota-based rules.

6. At the confirmation box, click **OK** to proceed with clearing the Quotas. The Quotas are cleared immediately, and there is no need to click **Save and Exit** only to clear the Quotas.

To reset web quotas for a user or all users in a synchronized group

1. Click **Services** > **Web Security Services** > **Web URL Filtering** > **Group Synchronization** > **Users**.
2. Check the checkbox for all the users to have their quotas reset, or the checkbox on the header line to select all users.
3. Click **Clear Quotas For Selected**.

   This option is only enabled if there is at least one Quota-based rule set up. Clearing the Quotas has no effect on any users who are not included in any Quota-based rules.
4. At the confirmation box, click **OK** to proceed with clearing the Quotas. The Quotas are cleared immediately, and there is no need to click **Save and Exit** only to clear the Quotas.

How quotas are calculated

The following table describes how web quota limit are calculated and how certain events or conditions. For example, canceled downloads affect the quotas.

Bandwidth	Bandwidth quotas are imposed based on the size of content downloaded or uploaded. ■ A rule may specify a file type (extension or content type). Bandwidth is accumulated against only those types. ■ Bandwidth is only accumulated against the actual size of the file downloaded; it does not include any updated bandwidth, headers, or protocol overhead. ■ Bandwidth is only accumulated if a complete file is delivered to the user; files blocked due to infections or a user canceling are not accumulated.
Time	Time quotas are imposed based on the sum of the browsing session times. ■ The minimum time quota activity period is three minutes. ■ Idle time does not count against a quota. **Note:** If a web request is received, another request is received one minute later, and then no further requests are received, the user consumes four minutes of time quota.

Continuous browsing	If an HTTP request is made before the end of the previous session, the session is considered continuous. If an HTTP request is made after the end of the last session, so that the two sessions do not overlap, the sessions are considered distinct and the period between these sessions is considered idle time (that is, time not spent browsing). ■ Streaming media that involves a single request accumulate only one three-minute block of time against the quota limit, even if the request is streamed for several hours. ■ Once a user has exceeded their quota for a rule, content prohibited by that rule is blocked commencing with the next matching access. A single browsing session may last for three minutes or for many hours, depending on the frequency of activity. The session ends three minutes after the last request is received. The time quota consumed is then based on the total duration of that session. The next session starts when everything in the previous session has downloaded and there has been some idle time before the next request is received. A web application that regularly polls the Internet continues to count against a time quota. For example, an application that polls every two minutes starting at 00:00 and finishing at 00:56 consumes 59 minutes of time quota, and the session ends at 00:59. This counts as one continuous session. A request for streaming content consumes only one three-minute session of time quota regardless of the actual time spent streaming the requested material. However, the streaming data contributes to any bandwidth quota that may be in operation. All web requests for content contribute to a bandwidth quota, regardless of the content type.
Canceled downloads	In the event that a user cancels an in-progress download, the bandwidth already delivered to the user is not counted against the quota.
File types	If a file type (extension or content type) is specified in the quota rule, time or bandwidth is accumulated against all files of that type. If specific file types are not specified in a rule, the following file types accumulate time or bandwidth against the quota limit: ■ HTML/text ■ Video and audio media types (including streaming media) ■ Flash
Web browser state	The state of the web browser (for example whether it is closed or open; or using multiple tabs or multiple instances) is irrelevant. Quotas are based on the web requests that are made.

Troubleshooting web quotas

The following considerations may help resolve any difficulties with configuring and using web quotas:

- The system disables any web quotas that are not configured correctly or fully. You must correct any problems before you can make the rule Active.
- Time limits can be set at five-minute intervals. A user cannot exceed the total time permitted in any time-based rules for a day.
- The time zone must be specified in the **Time** tab. A day is considered to start at 00:00 in this time zone, regardless of where the user is located in the world.
- Bandwidth limits are set at 1-MB intervals. This limit is either for each individual user, or shared for all the users, set in the rule where the Quota is applied.

Chapter 6

Tools for Web Security

This chapter includes the following topics:

Client Site Proxy tool

The Client Site Proxy (CSP) is the component of Web Security which captures information specific to the user computer making requests to the Internet. To accomplish this, the CSP does the following: authenticates the user making a web request against the local domain; captures and encrypts details of the domain name, user name, and local IP address; and adds them to the HTTP request as custom HTTP headers. This information is used with information held by the service on users to then apply policy specifically to the user as defined in the portal.

You should download and install the Client Site Proxy first. This proxy is required for configuration and reporting at user and group level.

To download the Client Site Proxy

1. Click **Tools** > **Downloads**.
2. In the **Client Site Proxy** section, select the version you require and click **Download**.
3. Follow the on-screen instructions.

For further information on the Client Site Proxy, see the Online Help.