User's Guide

Websense® Express

v1.0

Published May 16, 2007
Printed in the United States of America and Ireland.

Trademarks

WinPcap

Contents

CHAPTER 1 Introduction

Websense® Express gives your organization the ability to monitor and control network traffic to the Internet.

- Add a solid layer of security to your network, protecting it from potential spyware, malware, hacking, and other intrusions.
- Minimize employee downtime spent accessing Internet sites deemed objectionable, inappropriate, or not work-related.
- Minimize misuse of network resources and the threat of legal action due to inappropriate access.

This guide introduces Websense Express and its reporting tool, Websense Explorer.

- Learn how to use Websense Manager, the graphical interface to Websense Express Internet filtering tools, to start monitoring and filtering Internet usage right away (see *Introducing Websense Manager*, page 10).
- Find out how Websense Explorer's browser-based reports can help you refine your Internet filtering policies (see *Websense Explorer*, page 21).

Find additional tips, video tutorials, an extensive knowledge base, and additional product documentation at www.websense.com/supportwsx_en/.

Logging on to Websense Express

To start using Websense Express, log on to Websense Manager, the interface used to customize filtering behavior, monitor current filtering, and configure Websense Express software (see *Introducing Websense Manager*, page 10).

The first time you launch Websense Manager, you are asked to create a password. This is the **WebsenseAdministrator** password, used to log on to both Websense Manager and Websense Explorer.

Note

When you are prompted to create a password, the user name is not displayed. After this initial log on, the name WebsenseAdministrator appears in user name field of the password dialog box. This name cannot be changed.

1. Launch Websense Manager (**Start** > **Programs** > **Websense** > **Websense Manager**).
2. Enter the WebsenseAdministrator password, or, if no password exists, create a password and confirm it.

   You can change the WebsenseAdministrator password within Websense Manager using the **Server** > **Settings** > **Change Password** dialog box. See the Websense Manager Help system for more information.
3. Click **OK**.

   If this is the first time you have logged on to Websense Manager, you are prompted to enter a subscription key. Before entering your key, see *Entering the subscription key*, page 9, for important considerations.

Entering the subscription key

Websense provides a subscription key via email. Each key is valid for 1 Websense installation

Note

Before you enter your key, and thus launch a database download, consider this question: must Websense software go through a proxy server or proxying firewall to access the Internet and download the Master Database? If yes, you must configure Websense Express to use the proxy before you download the database.

Click **Cancel** when prompted for a subscription key, and then follow the instructions in Lesson 2 of the *Getting Started* tutorial.

You can choose when to enter your subscription key:

- Enter your key immediately after creating the WebsenseAdministrator password. The Master Database begins to download. This process occurs in the background and can last several minutes. The Master Database must be downloaded before Websense Express can filter clients (see *The Websense Master Database*, page 19).
- If you need to configure proxy settings, click **Cancel** to postpone entering your subscription key. See Lesson 2 of the *Getting Started* tutorial, or *Configuring download via proxy* in the Websense Manager Help system.

  No Internet filtering occurs until you enter a subscription key. In addition, warning messages appear in the Websense Status monitor until a valid key is entered.

After you enter your subscription key or click **Cancel**, you are prompted to launch the *Getting Started* Tutorial.

The *Getting Started* tutorial

Websense Express includes a tutorial to help you get up and running as quickly as possible. Websense highly recommends working through this tutorial. Learn how to:

- Verify that Websense Express can monitor and filter computers in the network.
- Download the Master Database.
- Work with sample filtering definitions included with your software.
- Create your own filtering definitions.
- Identify users and computers in your network and apply filtering policies to them.

Introducing Websense Manager

Websense Manager is the interface used to monitor current Internet usage filtering and customize filtering behavior (see *Chapter 2: Establishing Filtering Policies*).

You can access Websense Manager locally, from the Websense Express machine (**Start** > **Programs** > **Websense** > **Websense Manager**), or from a Web browser, by entering the following:

```
http://<IP or hostname>:8080/Manager
```

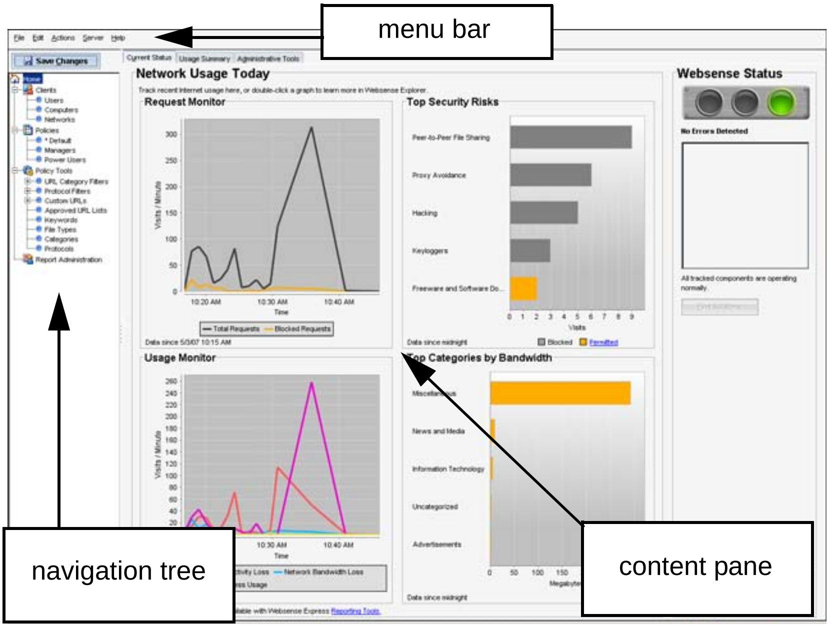
<IP or hostname> is the IP address or name of the Websense Express machine, and **8080** is the default port used for remote access to Websense Manager and Websense Explorer.

Note

If port 8080 is in use, Websense software increments to the next available port. See the Knowledge Base for more information.

Only one person can log on to Websense Manager at a time.

The Websense Manager interface includes a menu bar, navigation tree, and content pane.



When you log on to Websense Manager, and any time you select **Home** in the navigation tree, the content pane displays the Home console. Use the Home console to monitor current filtering status, review recent filtering history, evaluate your configuration, and access administrative resources.

Getting started with the Home console

The Websense Manager Home console includes the following tabs:

- **Current Status**: Shows Websense system status and a general overview of current Internet filtering status. This tab also highlights user attempts to access sites in security risk categories.
- **Usage Summary**: Provides an overview of past network usage, with high-level overviews of who accessed the Internet, how many requests were blocked and permitted, and how many requests for security risk categories were blocked.
- **Administrative Tools**: Includes tools for evaluating current filtering settings, as well as links to useful resources.

Double-click any graph on the Current Status and Usage Summary tabs to launch Websense Explorer for more information. You are prompted to log on to Explorer using the WebsenseAdministrator password (created the first time you logged on to Websense Manager).

Explorer displays Internet usage data related to the chart you selected. You can retrieve specific information about which sites were requested and who requested them, see data charted over a longer time period, print report details, and more. See *Websense Explorer*, page 21.

You can also launch Websense Explorer by clicking the **Reporting Tools** link at the bottom of the Current Status and Usage Summary tabs.

The Current Status tab

The Current Status tab of the Websense Manager Home console provides a quick overview of Websense Express and usage filtering status. Monitor the volume of Internet requests, both by number of visits and by bandwidth usage, and keep abreast of potential network security risks. Keep up with changes in Internet usage patterns so that you can fine-tune filtering policies, as needed.

The Current Status tab includes these main sections.

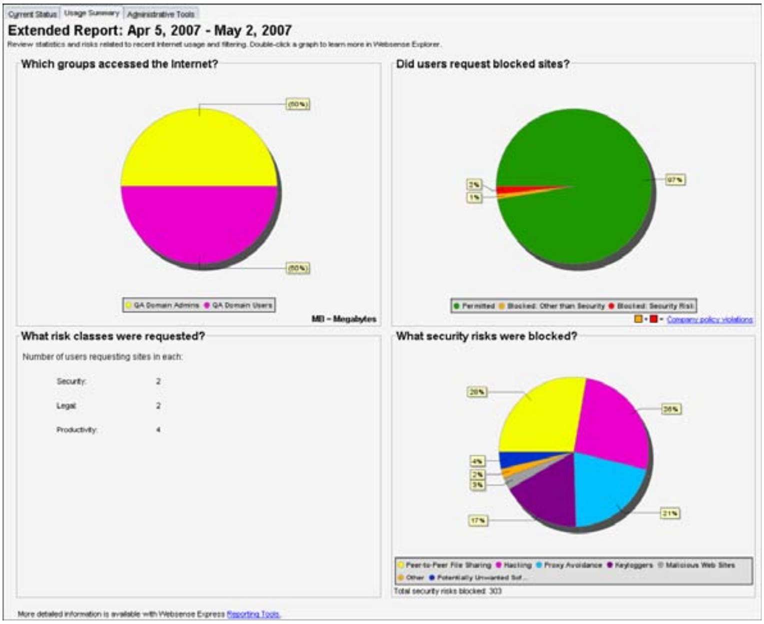
- The **Websense Status** monitor to the far right indicates current system status. If a problem is found in any monitored component, an error message appears. Click **Find Solution** for help resolving the problem.

  Use the **Support Portal** link below the status monitor to access the Websense support Web site, which includes links to tips, video tutorials, a Knowledge Base, and additional resources.
- The **Request Monitor** chart begins plotting blocked and permitted Internet requests as soon as you log on to Websense Manager. The graph initially updates every minute; after the first 5 minutes, it updates in 5 minute intervals.
- The **Usage Monitor** chart plots permitted Internet requests by risk class. Risk classes group URL categories by general type, for use by reporting tools.
- **Top Security Risks** lists the 5 most-requested categories in the Security Risk class.
- **Top Categories by Bandwidth** lists the 5 categories of Internet requests currently using the most network bandwidth.

After displaying data for 8 hours, the Request Monitor and Usage Monitor graphs reset. Data for the previous 8 hours is cleared, and new data appears as it is collected.

Double-click any chart on the Current Status tab to launch Websense Explorer and view Internet usage data related to the selected chart. You can also use the **Reporting Tools** link at the bottom of the tab to access Websense Explorer.

The Usage Summary tab

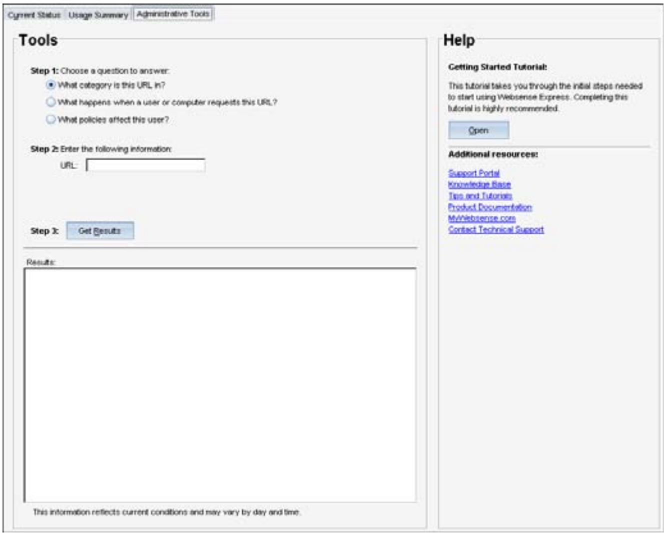


The Usage Summary tab of the Websense Manager Home console provides an overview of network usage in the recent past. A date range at the top of the page indicates the time period covered by the 4 charts that make up the summary.

- **Which groups accessed the Internet?** shows the 6 groups (defined in your directory service) that used the most Internet bandwidth. Internet usage by all other groups is jointly summarized as **Other**. For more information about working with users and groups, see *Clients* > *Working with directory services* in the Websense Manager Help system.
- **Did users request blocked sites?** gives a quick overview of user compliance with Internet usage policies.
- **Which risk classes were requested?** indicates whether users are attempting to access sites in the security, legal, and productivity risk classes, and shows how many users requested sites in each class.
- **What security risks were blocked?** shows how frequently URL categories in the security risk class were blocked.

As on the Current Status tab, you can double-click any chart to launch Websense Explorer and retrieve additional Internet usage information, or click the **Reporting Tools** link at the bottom of the tab.

The Administrative Tools tab



The Administrative Tools tab of the Websense Manager Home console is divided into 2 sections.

- Use the **Tools** section to identify how sites are being filtered and how policies are being applied to specific users.
  - Click **What category is this URL in?** to find information about the category in which the site is found and whether the site has been defined as a custom URL. The results also contain a link you can use to contact Websense, Inc., to suggest a different category for the site.
  - Click **What happens when a user or computer requests this URL?** to find out whether a site is permitted, blocked, or blocked with a continue option in the policy currently active for the specified user or IP address. The tool also provides information about how the URL is categorized.

    This information is specific to the current time and day. Policies may apply different filtering rules at different times, and different policies may apply to a user at other times.

    - Click **What policies affect this user?** to find out which filtering policy or policies currently apply to any user in your directory service. (Multiple policies may apply if the user belongs to more than one group, and no user-specific policy has been assigned.)

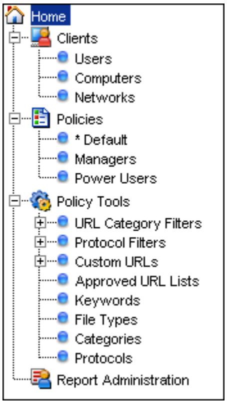
      As with the previous tool, the information returned is specific to the current day and time. Other policies may apply at other times.

  More information about using these tools is available in the *Getting Started* tutorial.

- Use the **Help** section to access information about Websense Express.
    - Click **Open** to launch the *Getting Started* tutorial, which takes you through the process of verifying network connectivity, downloading the Websense Master Database, and working with filtering policies.
    - Use the **Support Portal** link to open the main Websense Technical Support Web site.
    - Click **Knowledge Base** to get the latest information about Websense Express, and to find detailed articles about using Websense Express features.
    - Access **Tips and Tutorials** to find articles and short videos that demonstrate how to get the most from your Websense software.
    - Click **Product Documentation** to access this guide and other Websense documentation on the Web.
    - Go to **MyWebsense.com** to access product updates and patches, product news, and evaluations, as well as support resources.
    - Click **Contact Technical Support** to receive assistance from a Websense Technical Support representative.

Understanding the navigation tree

Use the navigation tree to access Internet filtering tools.



Click the plus symbol (+) next to a node to display its child entries. Click an entry to display its details in the content pane.

The navigation tree includes:

- **Clients**: A list of computers, networks, users, and groups to which filtering policies can be applied.
- **Policies**: The basis of filtering. Each policy identifies which set of filtering rules (in the form of URL category filters, approved URL lists, and protocol filters) applies during any given day or time.

  Websense Express includes sample policies. Edit these, or create new policies. Clients are filtered by the **Default** policy until another policy is assigned (see *Understanding filtering policies*, page 25).
- **Policy Tools**: The definitions that determine how you monitor and control Internet access.
  - **URL Category Filters**: Each filter is a list of all URL categories, with an action (such as permit or block) assigned to each one (see *Working with URL category filters*, page 26).
  - **Protocol Filters**: Each filter is a list of all protocols, with an action (such as permit or block) assigned to each one (see *Working with protocol filters*, page 36).

- **Custom URLs**: Provides 2 ways to change how a URL is filtered. Use the **Recategorized** list to move a URL from one category to another to change the way the site is filtered. To ensure that a URL is always permitted, add it to the **Not Filtered** list (see *Working with custom URLs*, page 43).
- **Approved URL Lists**: Each list defines sites to permit, regardless of other filtering settings. When you create an approved URL list and apply it in a policy, users governed by that policy can visit only sites that appear in the list. See *Using an approved URL list*, page 34, for more information.
- **Keywords**: A complete list of categories that you can use to define filtering based on certain words. When you define keywords for a category, then enable keyword blocking in a URL category filter, Websense Express blocks any site whose URL contains a keyword. See *Defining keywords*, page 31, for more information.
- **File Types**: A list of common file types, like audio files and compressed files. Each file type definition includes a series of file extensions (like MP3 and WAV) associated with that type of file. Use URL category filters to block any defined file type within a permitted category (see *Working with file type definitions*, page 33).
- **Categories**: A list of all current URL categories, both Websense-defined and custom. Use this interface to define custom categories (see *Adding a custom category*, page 45).
- **Protocols**: A list of all current protocols, both Websense-defined and custom. Use this interface to define custom protocols (see *Adding a custom protocol*, page 46).

- **Report Administration**: A list of reporting roles that you define. Reporting roles determine who can access which aspects of Websense Express reporting tools. See *Establishing reporting roles* in the Websense Manager Help system for more information.

Configuring Websense Express settings

Websense Manager includes an interface, accessed via the **Server** > **Settings** menu option, used to configure a variety of Websense Express settings.

Configure **Alerts and Notifications**, customize the filtering **Block Messages** that users receive, define **Common Filtering** behaviors, set up a **Database Download** schedule, establish communication between Websense Express and your **Directory Service**, determine how much user information is recorded by Websense **Logging** tools, and more.

See *Configuring Websense Express* in the Websense Manager Help system for details.

The Websense Master Database

The Master Database houses URL category definitions, used to categorize Web sites, and protocol definitions, used to group Internet communications and file transfer protocols. These definitions provide the basis for filtering Internet content.

At installation, Websense Express includes a sample database that provides some filtering capabilities, but it is a good idea to download the full Master Database as soon as possible.

To download the Master Database, enter your subscription key the first time you log on to Websense Manager (see *Entering the subscription key*, page 9). The Master Database begins to download in the background.

If you need to perform additional configuration before downloading the Master Database, you can wait and enter your subscription key via the Websense Manager **Server** > **Settings** > **Database Download** dialog box, and then perform the download (see Lesson 2 in the *Getting Started* tutorial).

After initial download, Websense software downloads changes to the Master Database according to the schedule you establish (see *Filtering and the Websense Master Database* in the Websense Manager Help system).

Note

After you download the Master Database or updates to the Master Database, CPU usage can be 90% or more for 1-3 minutes while the database is loaded into local memory.

It is a good idea to schedule the download for off-peak times.

Websense Explorer

Websense Explorer provides an interactive interface to view Internet usage data that is generated by Websense Express and stored in the Log Database.

To read more about how you can use Explorer, see the *Websense Explorer Business Examples* paper on the Product Documentation Web site, available at http://www.websense.com.

Understanding Websense Explorer

Explorer gives you a look into the Log Database that contains information about how your employees are actually using the Internet.

Log Server receives incoming data about Internet usage from Websense Express and stores it in the Log Database, which is divided into partitions for reporting. Database partitions are a way to provide flexibility in reporting and better system performance. These partitions are managed in Database Administration where you can configure maintenance activities.

Websense Express components interact with Websense Explorer components to store data for reporting. See brief overviews of these components in online Help.

Role-based reporting

Role-based reporting gives users access to the Web-based reporting tools. Permissions are granted by the administrator.

For flexibility in report administration, you can configure user-specific reporting permissions. For example, grant one user in addition to yourself permission to report on all clients using Explorer and manage Log Database contents. Grant others permission to report on specific groups.

To configure reporting permissions, users must be defined in a directory service. Add users (clients) as report administrators in Websense Manager.

To set up reporting permissions, select **Actions** > **Add Role** in Websense Manager.

Explorer reporting permissions are:

- **Hide user names in reports**: Makes report entries anonymous in reports the administrator runs.

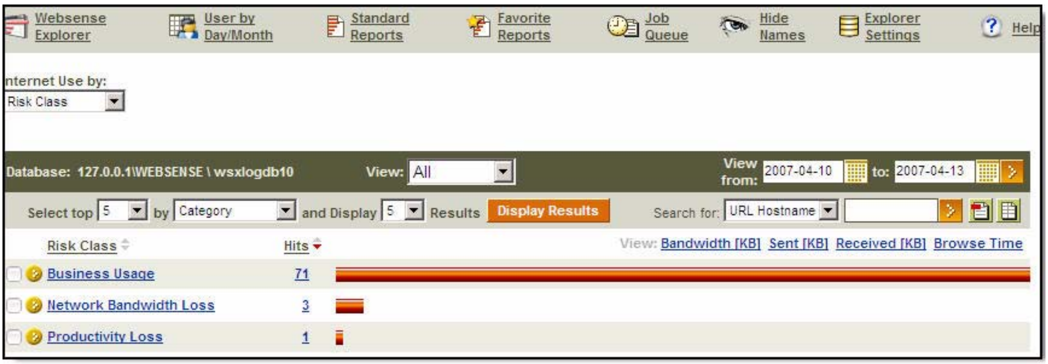
- **Save Favorite Reports**: Allows the administrator to create and save report criteria for repeated use.
- **Schedule Favorite Reports**: Allows the administrator to set Favorite Reports to run at regular intervals and be emailed to others.
- **Database Administration**: Allows the administrator to use Database Administration to manage Log Database contents and configure Internet Browse Time reports. See *Administering the Database*.

Set up with access permissions to all Web-based Reporting tools, and set up with administrators attached to them.

The Main Page in Explorer

Websense Explorer is installed as part of Websense Express. Use Explorer to view the Log Database from your Web browser. The Log Database

Start defining all reports from Explorer’s Main Page. There are drill-down options from some report results, but your initial choices will be made from the main page.



Explorer main page

Online Help

Select the **Help** option within the program to display detailed information about using the product.

IMPORTANT

Default Microsoft Internet Explorer settings may block operation of the Help system. If a security alert appears, select **Allow Blocked Content** to display Help.

If your organization's security standards permit, you can permanently disable the warning message on the Advanced tab of the **Tools** > **Internet Options** interface. (Check **Allow active content to run in files on My Computer** under Security options.)

Technical Support

Websense, Inc., is committed to customer satisfaction. Go to the Websense Technical Support Web site any time for the latest release information, to access the Knowledge Base or product documentation, or to create a support request. These pages can be accessed from the Websense corporate Web site:

www.websense.com/

Response times are generally within one business day.

CHAPTER 2 Establishing Filtering Policies

When you enter your subscription key, Websense Express starts to download the Websense Master Database. This database includes the URL category and protocol definitions that form the basis for Internet usage filtering.

Once the database download process is complete, Websense Express begins filtering Internet requests using the **Default** policy. This policy applies to all clients whenever no other policy applies. Initially, the **Default** policy applies the **Basic Security** URL category filter and **Typical** protocol filter.

- The **Basic Security** URL category filter blocks sites in URL categories that are considered serious security risks, such as Malicious Software and Keyloggers. It does not block sites in other categories, even those like Adult Material and Gambling that may pose legal liability or productivity risks.
- The **Typical** protocol filter blocks protocols in the Instant Messaging / Chat, P2P File Sharing, and Proxy Avoidance protocol groups.

Understanding filtering policies

Websense Express filtering is based on policies. A policy is a schedule that determines how URL categories and protocols are filtered at certain times. Policies can include a combination of the following:

- **URL category filters** apply a filtering action to each URL category
- **Approved URL lists** define specific sites that users can access
- **Protocol filters** apply a filtering action to each protocol

URL category filters, approved URL lists, and protocol filters are scheduled into policies by time of day and day of week.

You can create a variety of policies, then apply different policies to different users to create custom filtering restrictions. You might create:

- One policy that blocks access to all but business-related sites during working hours, but allows access to sports, shopping, and entertainment sites after normal business hours and on weekends.
- A second policy that allows access to all sites except those in the Security Risk and Legal Liability risk classes at all times.
- A third policy that provides unfiltered access to all Internet sites, 24 hours a day, 7 days a week.

The Default policy

The **Default** policy provides an immediate way to manage Internet access throughout your organization. The **Default** policy also acts as a safety net, applying filtering restrictions to users when no other policy has been assigned.

You can edit the **Default** policy, but it cannot be deleted, and must apply 24 hours a day, 7 days a week.

Initially, the Default policy applies the **Basic Security** URL category filter and the **Typical** protocol filter at all times.

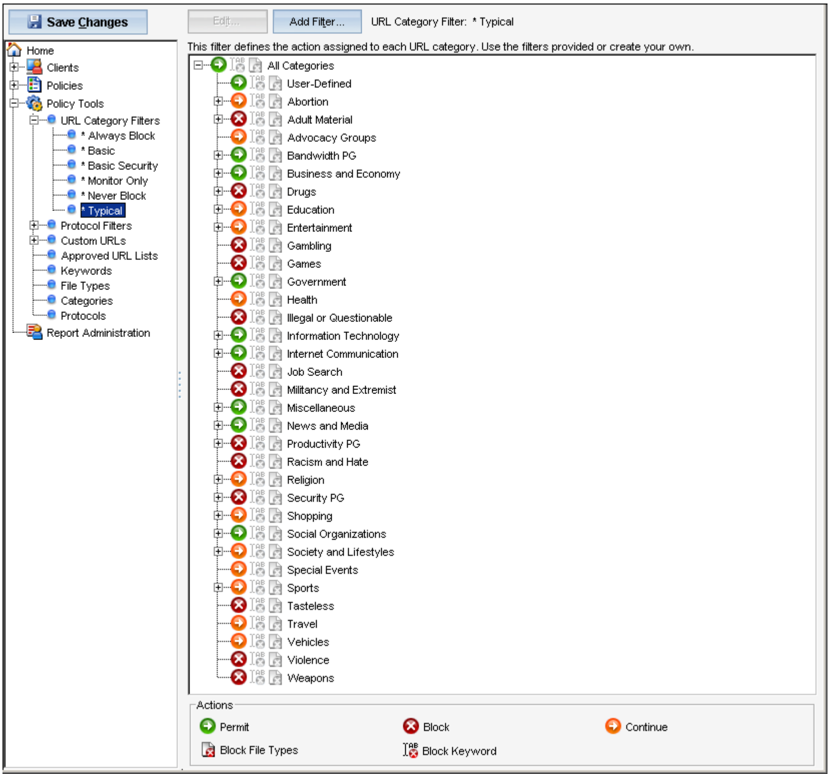
You can edit the **Default** policy to enforce other URL category or protocol filters, according to a schedule you establish. For more information, see *Working with policies*, page 39.

Working with URL category filters

Websense Express includes a variety of permanent URL category filters. These are marked with an asterisk (*) in Websense Manager to indicate that they cannot be edited or deleted.

- **Always Block**: Blocks access to all Internet and intranet sites.
- **Basic**: Blocks commonly-restricted categories, including Adult Material, Gambling, Illegal or Questionable, and the Security PG.
- **Basic Security**: Blocks sites classified as serious security risks, but does not block sites that may pose legal liability or productivity risks.
- **Monitor Only**: Permits all categories, and allows logging and reporting on all categories.

- **Never Block**: Allows total, unrestricted access to all sites.
- **Typical**: Provides a more nuanced approach to filtering, blocking sites in some categories, allowing users to choose the Continue option for some categories (see *The Continue option*, page 30), and blocking the rest.



Any of these filters can be used as a template for creating custom URL category filters.

Adding a URL category filter

Create as many URL category filters as you need to fine-tune filtering for your organization. Add each filter to a policy to determine when it applies and which clients it governs.

1. Right-click in the navigation tree, and then select **Add URL Category Filter**. The Add URL Category Filter dialog box appears.
2. Enter a unique name for the new URL category filter, and then click **OK**.

3. In the URL Category Filter Model dialog box, select an existing URL category filter to use as a template, and then click **OK**.

   The new URL category filter is added to the navigation tree under **Policy Tools** > **URL Category Filters** and selected. Information about the new filter appears in the content pane.

   The new URL category filter is an exact copy of the model with a different name.

4. Click **Save Changes** above the navigation tree.
5. Customize the new filter (see *Editing a URL category filter*), add it to a policy (see *Editing a policy*, page 40), and then assign the policy to clients (see *Assigning a policy to clients*, page 42).

Editing a URL category filter

Edit custom URL category filters to change the filtering settings for any or all categories.

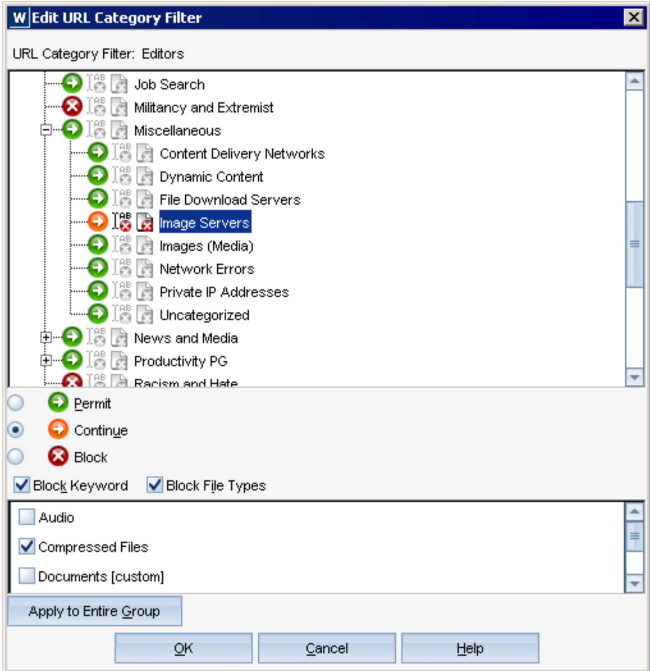
Note

You can select a Websense-defined URL category filter to see the filtering actions it applies, but cannot edit the filter.

When you select **Always Block** or **Never Block**, no related information appears in the content pane.

1. Expand **Policy Tools** > **URL Category Filters**, if necessary, and select a custom URL category filter in the navigation tree. Settings for the filter appear in the content pane.

2. Click **Edit**. The Edit URL Category Filter dialog box appears.



3. Select a category, and then select the policy action to apply.

Policy Action	Function
Permit	Permits access to all sites in the selected category.
Block	Blocks access to all sites in the selected category.
Continue	Lets the user continue and view the site for a limited amount of time. For more information, see *The Continue option*, page 30.
Block Keyword	Blocks sites whose URLs contain keywords assigned to a URL category (see *Implementing keyword blocking*, page 30).
Block File Types	Blocks files having extensions associated with file types assigned to the URL category (see *Implementing file type blocking*, page 32).

4. To apply the same filtering action to all subcategories in a parent category, click **Apply to Entire Group**.
5. Repeat for each category to modify.

   If you are applying the same action to multiple categories, Shift-click or Ctrl-click to select the categories, and then apply the action.
6. Click **OK** to close the Edit URL Category Filter dialog box.
7. Click **Save Changes** above the navigation tree.

If the URL category filter is used in an existing policy, changes that you make to the filter go into effect automatically. If the URL category filter is not used in any policy, add it to a policy as described in *Editing a policy*, page 40.

The Continue option

When you create or modify a URL category filter, you can assign the permit, block, or continue actions to each category.

When affected users request a site that has been assigned the continue action, they receive a block page with a Continue button. If the user clicks **Continue**, Websense Express permits the site, and the page is displayed until the browser is closed or another site is requested.

Clicking **Continue** starts a timer. During the configured time period (60 seconds by default), the user can visit other sites in Continue categories without encountering another block page. To change the default time period, go to **Server** > **Settings** > **Common Filtering** and edit the **Continue timeout** field.

Once the time period ends, browsing to another Continue site results in a Continue block page.

Implementing keyword blocking

Keywords offer protection against sites that have not been explicitly added to the Master Database or a custom URLs list. Keywords can be associated with any URL category, including custom categories.

When the **Block Keyword** setting is active for a category, Websense software blocks **any** site whose URL contains an associated keyword, even if the site falls into another URL category.

For example, if keyword blocking is applied to the Sports category, and the keyword “nba” is associated with Sports, the URL **sports.espn.go.com/nba/**

is blocked. URLs not normally associated with the Sports category that also contain the string “nba”, such as **www.nba.az** (used by a financial institution in Azerbaijan) are also blocked. In such a case, the block page indicates that the file is blocked as belonging to the Sports category, because the URL contains a keyword defined for that category.

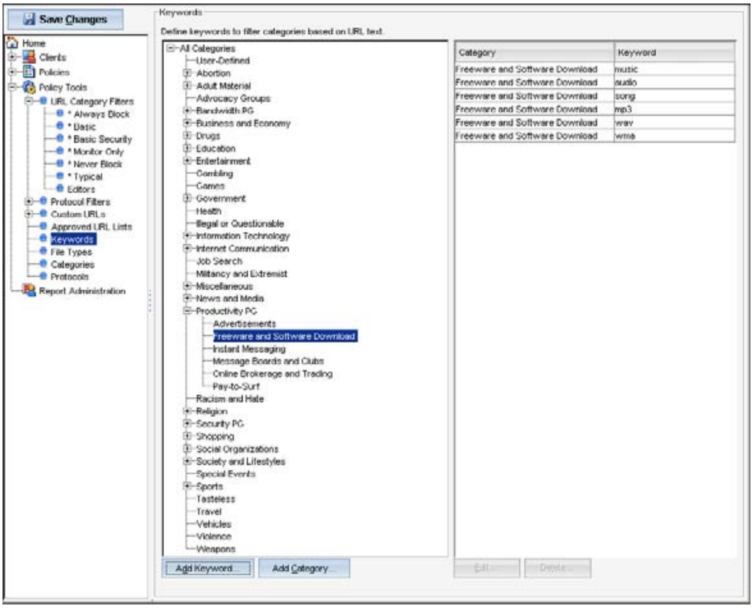
Keyword blocking may result in unintended blocking. For example, blocking the keyword *sex* blocks access to sites such as **www.sex.com** (an adult material site), but can also block search engine requests for words like *sextuplets* or *City of Essex*, which have the word embedded in them.

Defining keywords

1. Select **Keywords** in the navigation tree to display the keyword editor.
2. Select a category from the list.
3. Click **Add Keyword**. The Add Keyword dialog box appears.
4. Enter the keywords for the selected category.
   - Define each keyword on a separate line.
   - Do not use spaces between words. URL and CGI strings do not contain spaces between words. Websense Express matches exact words or character strings that you have entered as keywords.
   - Enter a backslash (\) before certain special characters, including the backslash character itself, or a period (.), comma (,), question mark (?), asterisk (*), or plus sign (+).

     For example, to block all URLs or CGI strings that include the characters *.cfm*, enter **\.cfm**. If you do not use the backslash, Websense software ignores the period, and matches any URL or CGI string that includes *cfm*.

5. Click **OK**. Each keyword and its associated category is listed in the content pane.



6. Repeat steps 2 - 6 for each category to which to add keywords.
7. Click **Save Changes** above the navigation tree.
8. To use these keywords in filtering, apply keyword blocking in one or more active URL category filters (see *Editing a URL category filter*, page 28).

Implementing file type blocking

You can refine your URL category filters with filtering based on file extensions, restricting access to particular file types from sites in certain categories. For example, permit the category **Entertainment**, but block video files from sites in the **Entertainment** category.

Note

To implement full filtering for video *and* audio Internet media, combine protocol-based filtering with file type filtering. In this case, protocol filtering handles streaming media, while file type filtering handles files that can be downloaded and then played.

Websense software provides several predefined file types, or groupings of file extensions used for similar purposes.

Implement filtering policies using predefined file types, modify the existing file type definitions, or create new file types. Websense file types are continually updated in the Master Database.

> **Note**
> If you use file type blocking to block images, such as GIF or JPEG files, that make up only part of an otherwise permitted page, the image region on the page appears blank. It does not contain a block message.

Working with file type definitions

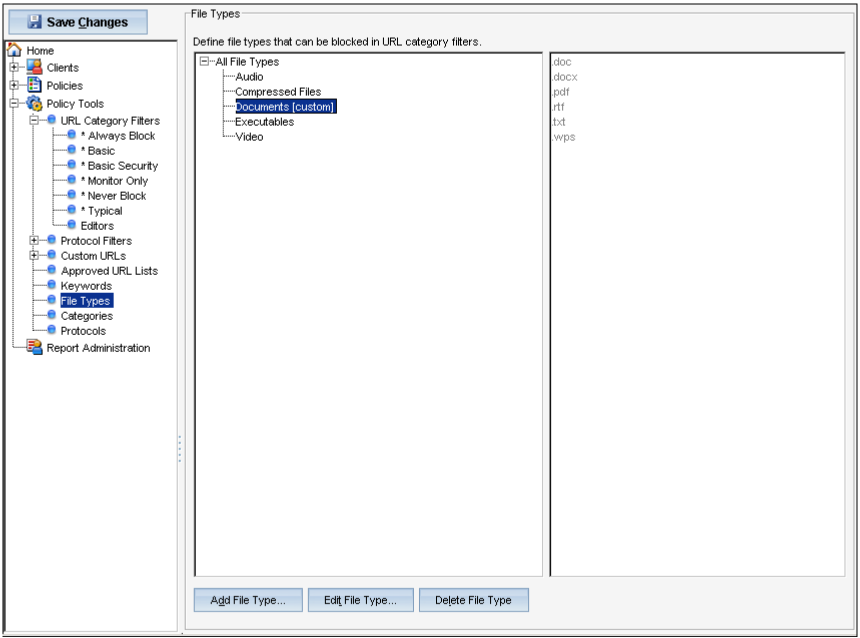
Add up to 32 file types (groups of file extensions). For example, a *Documents* file type might contain *doc*, *odt*, *pdf*, *rtf*, and *txt* extensions.

1. Expand **Policy Tools** > **File Types** in the navigation tree. A list of file types appears in the content pane.

   File types that you define are labeled **[custom]** in the list.
2. Click **Add File Type**. The Add File Type dialog box appears.
3. Enter a unique **File Type Name**.
4. Type the file extensions, 1 per line, to include in this file type definition. You do not need a dot (".") before each extension.

> **Note**
> If you define a custom file type that includes an extension also defined in a Websense file type, your custom entry takes precedence. If such a file is blocked, it is filtered and logged as the type you defined, not as the Websense type. You can have only 1 custom definition for each extension.

5. Click **OK**. The new file type appears in the **File Types** list.



6. Click **Save Changes** above the navigation tree.
7. To use these file types in filtering, apply file type blocking in one or more active URL category filters (see *Editing a URL category filter*, page 28).

To change a file type definition, click **Edit File Type** and use the Edit File Type dialog box to add or remove file extensions. You can add file extensions to any file type, custom or Websense-defined, but can only delete custom file extensions.

Any time you make a change, remember to click **Save Changes** above the navigation tree.

Using an approved URL list

Approved URL lists provide a very precise method of defining filtering policies. Approved URL lists permit a limited set of Web sites for the clients governed by the policy that enforces the list.

When an approved URL list is active in a policy, only sites on the list are permitted for clients governed by the policy. For example, if the Finance policy has an approved URL list that includes only selected financial Internet sites, and this policy governs the Accounting group, then members of Accounting can access only URLs on the list.

When a user is governed by an approved URL list, a block page is returned for any requested URL not included on that approved URL list.

Adding an approved URL list

1. Right-click in the navigation tree, and select **Add Approved URL List**. The Add Approved URL List dialog box appears.
2. Enter a unique name for the approved URL list (for example, **HR Sites**).
3. Click **OK**.

   The approved URL list is added to the **Approved URL Lists** node in the navigation tree. Details for the new list appear in the content pane.
4. Enter the URLs to be included in this approved URL list. For HTTP sites, you do not need to enter the protocol.

   Each URL must be on a separate line.

   Include the protocol for any non-HTTP site. If the protocol is omitted, Websense software filters the site as an HTTP site.

   > **Note**
   >
   > Websense software recognizes approved URLs exactly as they are entered. This means that if you generally block search engines, but include **www.google.com** as an approved URL, users must type the full address to access the site. If a user types just google.com, the site is blocked. If you enter **google.com**, all sites with google.com in the address (such as maps.google.com) are permitted.

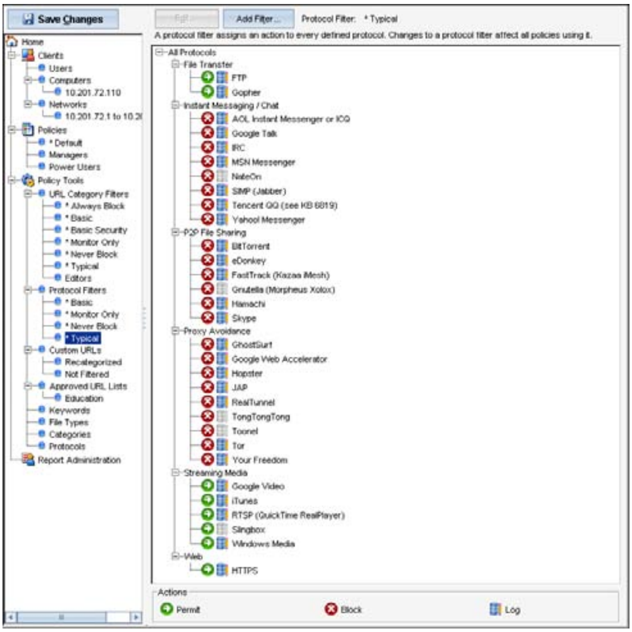
5. Click **Save Changes** above the navigation tree.
6. Add the approved URL list to a policy (see *Editing a policy*, page 40), and then assign it to users (see *Assigning a policy to clients*, page 42).

Working with protocol filters

Just as URL category filters provide the basis for Internet site filtering, protocol filters are the basis for filtering Internet content by protocol.

Websense Express includes 4 predefined protocol filters. These are marked with an asterisk (*) in Websense Manager to indicate that they cannot be edited or deleted.

- **Basic**: Blocks commonly-restricted protocols, especially those used for peer-to-peer file sharing and proxy avoidance.
- **Monitor Only**: Permits all protocols, and allows logging and reporting on all protocols.
- **Never Block**: Allows total, unrestricted access to all protocols.
- **Typical**: Blocks instant messaging, peer-to-peer file sharing, and proxy avoidance protocols. The **Typical** protocol filter is initially assigned to the **Default** policy.



Adding a protocol filter

1. Right-click in the navigation tree, and then select **Add Protocol Filter**. The Add Protocol Filter dialog box appears.
2. Enter a name for the new protocol filter, and then click **OK**. The Protocol Filter Model dialog box appears.
3. Select an existing protocol filter on which to base the new filter, and then click **OK**.

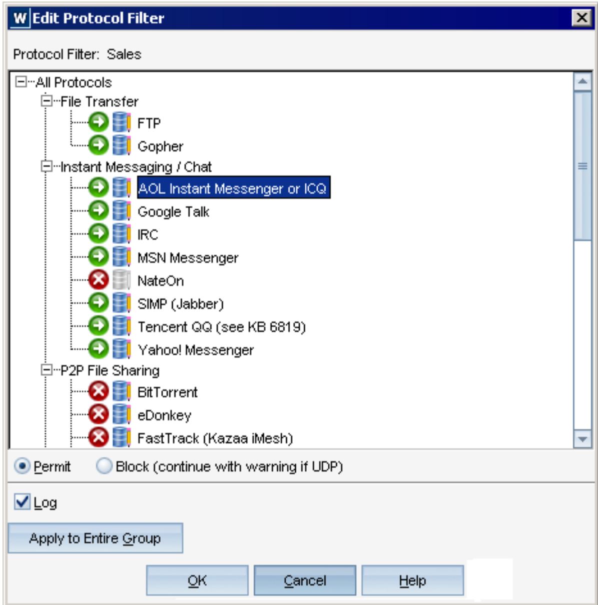
   The protocol filter you just created appears in the navigation tree, under **Policy Tools** > **Protocol Filters**.
4. Edit the new protocol filter. It remains a replica of the model protocol filter until it is edited, and is not used in filtering until it is added to a policy.

Editing a protocol filter

You can only edit custom protocol filters. If you select a Websense-defined protocol filter, the filter is displayed, but the Edit function is not available.

1. If necessary, expand **Policy Tools** > **Protocol Filters** in the navigation tree and then select the protocol filter to be edited. Its settings appear in the content pane.

2. Click **Edit**. The Edit Protocol Filter dialog box appears.



3. Select a protocol and specify a policy action.

Policy Action	Function
Permit	Permits data transmitted by the selected protocol.
Block	Blocks data transmitted by selected protocol.
Log	Tells Websense software whether to show usage data for this protocol in report output. Reports include the number of attempted requests for the protocol, and bandwidth usage for that protocol.

By default, any new protocols created or downloaded after Websense Express was installed apply the **Permit** action, but not the **Log** action.

Note

If you set the **Block** and **Log** options for the Websense protocol **Gnutella**, you may see a very large number of log records for this protocol. To prevent excessive logging, disable the **Log** option for **Gnutella**.

4. To apply the selected policy action to the whole protocol group, click **Apply to Entire Group**.
5. Click **OK**.
6. Click **Save Changes** above the navigation tree.

If the protocol filter is already included in a policy, the new actions are enforced for the clients governed by the policy. If the protocol filter is not part of any policy, it must be added to a policy before its actions are enforced. See *Editing a policy*, page 40, and *Assigning a policy to clients*, page 42, for more information.

Working with policies

Custom policies let you apply more or less restrictive filtering for specific users or computers (clients) without affecting filtering for the entire organization.

1. Add a new policy (see *Adding a policy*, on this page).
2. Edit the policy to define its filtering restrictions (see *Editing a policy*, page 40).
3. Add a client (see *Working with clients*, page 41).
4. Assign the new policy to the client (see *Assigning a policy to clients*, page 42).

Adding a policy

When you create a new policy, you can either use an existing policy as a model or start from scratch.

1. Right-click in the navigation tree, and then select **Add Policy**. The Add Policy dialog box appears.
2. Enter a unique name (1-25 characters) for the new policy.
3. Click **OK**. The Policy Model dialog box appears.
4. Select a policy from the list to use as a template, or select **Create empty policy**.
5. Click **OK**. The new policy is added to the **Policies** node of the navigation tree and selected.

Edit your newly-created policy to specify filtering restrictions (see *Editing a policy*, page 40).

Editing a policy

A policy consists of specified time periods during which particular approved URL lists, URL category filters, and protocol filters are active.

Edit a policy to add, change, or delete time periods, and to change the active filters for each time period.

Note

When you edit the **Default** policy, the schedule must cover all time periods, 24 hours a day, 7 days a week. If there are any gaps in the policy, Websense Manager does not allow you to save the changes.

1. If necessary, in the navigation tree, expand the **Policies** node and select a policy.

   The content pane shows when the policy is active, and which URL category filters, approved URL lists, and protocol filters it enforces.
2. In the policy section of the content pane, click **Edit**. The Edit Policy dialog box appears.
3. Double-click under **Start Time** and **End Time** to define a time period during which to enforce these restrictions.

   Do not define a time period that spans midnight. To use the same URL category filter from 5:00 pm to 8:00 am, define 2 time periods for it: one with start time 17:00 (5:00 pm) and end time 24:00 (midnight) and another with start time 00:00 (midnight) and end time 08:00 (8:00 am).
4. Double-click in the **Days** column, and select each day of the week to enforce these restrictions. Click **Done**.
5. Double-click in the **URL Category Filter/Approved URL List** column and select the URL category filter or approved URL list to enforce during the days and times in the current row (see *Working with URL category filters*, page 26, and *Using an approved URL list*, page 34).
6. Double-click in the **Protocol Filter** column and select the protocol filter to enforce during the days and times in the current row. For more information, see *Working with protocol filters*, page 36.

7. Repeat steps 3 through 6 to edit other rows. Each time period is defined on a separate row.

   Add or delete a row by right-clicking on a row to access the shortcut menu, and then choosing **Add Row** or **Delete Row**.

8. Click outside the table to exit the table area.
9. Click **OK**.
10. Click **Save Changes** above the navigation tree.

Assign this policy to clients so Websense software can use it to filter Internet requests (see *Assigning a policy to clients*, page 42).

Working with clients

Assign policies to clients to determine how individuals and groups can access the Internet. Clients can be:

- **Users**:
  - **Users**: Specific users defined in a Windows directory service.
  - **Groups**: Specific groups established in a Windows directory service.
  - **Domains**: Groups of networked computers that share a common communications address.
  - **Organizational Units**: Custom, high-level definitions in a Windows directory service that associate related sub-groups.
- **Computers**: Individual computers in your network, defined by IP address.
- **Networks**: Groups of computers, defined collectively as a range of IP addresses.

To define users as clients, you must first configure Websense Express to communicate with your directory service. See *Clients* in the Websense Manager Help system for details.

Even if you do not establish communication between Websense Express and a directory service, you can add computers and networks as clients. See *Adding computer and network clients*, page 42.

Adding computer and network clients

Add an individual computer as a client, or add a network to manage filtering collectively for several computers.

A computer is identified by an IP address, and a network is a range of IP addresses. The IP address ranges for different network clients must not overlap.

1. Right-click in the navigation tree, and then select either **Add Computer** or **Add Network**.
2. Enter the **IP address** of the computer to add, or the **Starting IP address** and **Ending IP address** of the network.
3. Click **OK**.
   - Each computer IP address appears in the navigation tree under **Clients** > **Computers**.
   - Each IP address range appears under **Clients** > **Networks**.
4. Click **Save Changes** above the navigation tree.
5. Assign a policy to each new client (see *Assigning a policy to clients*).

Assigning a policy to clients

Assign a policy to one or more users, groups, computers, or networks, or change the policy assigned to one or more clients.

> **Note**
> When you select a single client, policy information for that client appears in the content pane. When you select multiple clients, no information appears in the content pane.

1. Expand the **Clients** node in the navigation tree.
2. Select 1 or more clients.

   Shift-click to select multiple, contiguous clients, or Ctrl-click to select non-contiguous clients.
3. Right-click any selected client, and then select **Assign Policy**. The Assign Policy dialog box appears.
4. Select the policy to assign, and then click **OK**.

5. Click **Save Changes** above the navigation tree.

When multiple policies affect a client

When multiple policies apply to a single client, such as when separate policies are assigned to the user and the machine, Websense Express determines which policy to enforce as follows:

1. Apply the policy assigned to the **user** making the request.
2. If no user-specific policy is found, or the policy has no URL category filter scheduled at the time of the request, apply the policy assigned to the **computer** or **network** from which the request was made.
3. If no computer or network-specific policy is found, or the policy has no active URL category filter at the time of the request, look for a policy assigned to any **group** to which the user belongs. If the user belongs to multiple groups, Websense software considers all group policies that apply.
4. If no group-specific policy is found, or the policy has no URL category filter assigned at the time of the request, look for a policy assigned to the **domain** to which the user belongs.
5. If no domain-specific policy is found, enforce the **Default** policy.

Working with custom URLs

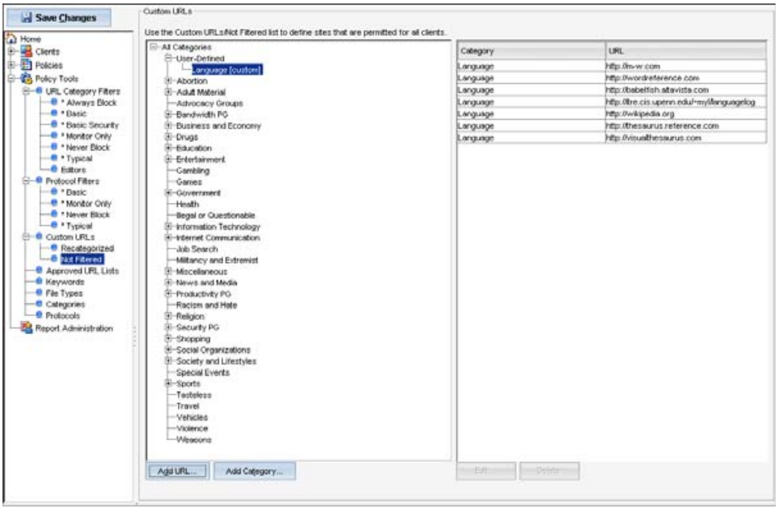
Custom URLs let you:

- Add sites to Websense Express that are not in the Websense Master Database.
- Filter sites differently than their Master Database categories.

Websense software considers custom URLs before URLs in the Master Database, and therefore filters the site according to the category assigned to the custom URL.

Websense Manager offers two custom URL lists:

- Custom URLs/Not Filtered lets you specify Internet sites to be permitted for all users, regardless of how the site's category is filtered. (The exception is the **Always Block** URL category filter, which blocks all Internet access.)



- Custom URLs/Recategorized lets you:
  - Classify sites that are not in the Master Database by adding them to a database category. Sites not in the Master Database are labeled **Miscellaneous Uncategorized** in Websense Explorer reports.

    When you recategorize a site, Websense software filters it according to the action applied to the selected category.
  - Reclassify sites that already exist in the Master Database. Single out sites to be filtered differently than their original categories. For example, block a specific site in an otherwise-permitted category.

You can also create new categories in which to store custom URLs (see *Adding a custom category*, page 45).

Defining custom URLs

1. Expand **Policy Tools** > **Custom URLs/Not Filtered** or **Custom URLs/ Recategorized** in the navigation tree. The custom URL editor is displayed in the content pane.
2. Select a URL category, and then click **Add**. The Add Custom URL dialog box appears.
3. Type the full URL for each site to filter under this category.

Each URL must be on a separate line.

Include the protocol for any non-HTTP site. If the protocol is omitted, Websense software filters the site as an HTTP site.

Note

Websense software recognizes approved URLs exactly as they are entered. This means that if you generally block search engines, but include **www.google.com** as an approved URL, users must type the full address to access the site. If a user types just google.com, the site is blocked. If you enter **google.com**, all sites with google.com in the address (such as maps.google.com) are permitted.

Websense software cannot match a custom URL with its equivalent IP address. To recategorize both the text URL and the IP address of a site, add both to the list:

63.212.171.196
www.websense.com

4. Click **OK**. Newly-added URLs appear at the end of the list.
5. Repeat steps 2 through 4 for each category to which to add custom URLs.
6. Click **Save Changes** above the navigation tree.

Defining custom categories and protocols

Define custom URL categories and protocols to provide more precise filtering and reporting for your organization. For example:

- Create a custom category called **Business Related** and populate it with sites used for daily business.
- Create a custom protocol called **Company Messaging** to make it easy to log use of a proprietary IM tool.

Custom URL categories and protocols are added to existing Master Database parent categories and protocols.

Adding a custom category

You can create up to 100 custom URL categories.

1. Go to **Policy Tools** > **Categories** in the navigation tree. A category list appears.
2. Select a category in the list, and then click **Add Category**. The Add Category dialog box appears.

   Note that you can use the **User-Defined** category to group your custom categories.
3. Enter a unique **Category Name**. Use only alphanumeric characters.
4. Select a policy action to apply to this category. This action applies only to custom URL category filters. You can later modify this action in individual filters (see *Editing a URL category filter*, page 28).

   Custom categories are set to **Permit** in all Websense-defined filters (see *Working with URL category filters*, page 26).
5. To apply keyword or file type filtering, check the appropriate settings.
6. Click **OK**. The custom category appears everywhere there is a category list.
7. Click **Save Changes** above the navigation tree.

Adding a custom protocol

Custom protocols must be defined by port number or IP address.

Warning

When you create a custom protocol that blocks a range of ports, ensure that you are not blocking ports used for communication between services in your network.

1. Expand **Policy Tools** > **Protocols** in the navigation tree. The existing protocol groups are displayed.
2. Select the protocol group to which to add the new protocol.
3. Click **Add Protocol**. The Add Protocol dialog box appears.
4. Enter a unique **Protocol Name**.
5. Under **Protocol Identifiers**, click **Add**.

6. Enter the ports or IP addresses used by this protocol, and select a **Transport Method** to associate with this protocol.

> **Note**
> If you create a custom protocol that uses the same port numbers as a Websense protocol, the custom protocol definition takes precedence in filtering and logging.

Follow these guidelines for creating protocol identifiers:

- At least one characteristic of the protocol definition—the port, the IP address, or the transport method—must be unique.
- If you select **All Ports** or **All external IP addresses**, that definition overlaps any specific ports or IP addresses entered in other protocol definitions.
- Port ranges or IP address ranges are not considered unique if they overlap. For example, the port range 80-6000 overlaps with the range 4000-9000.

7. Under **Protocol Filters**, select whether this protocol should be permitted or blocked, and whether requests for this protocol should be logged.

   When you add a custom protocol, this action is applied in all custom protocol filters. You can later modify this action in individual protocol filters (see *Editing a protocol filter*, page 37). In Websense-defined filters, all custom protocols are set to **Permit**.

8. Click **OK**, and then click **Save Changes**.

CHAPTER 3

Websense Explorer Reporting

Websense Explorer is installed at the same time as Websense Express. Use Explorer to view the database from your Web browser.

Explorer creates an intranet Web site on your Web server, and then users access this Web site to run Internet usage reports on the data stored in the database. Reports are based on the employee Internet activity information contained in the database that Explorer is currently using.

Overview

There are many components that work together in Websense Express and Websense Explorer for Windows.

The Reporting components consist of:

- Log Database - Center of Reporting
- Explorer Web server
- Web browser
- Explorer
- Log Server
- Microsoft® MSDE server database
- Microsoft Internet Explorer

> **Note**
>
> Your reports may vary from the samples shown in this guide. Follow the documentation to learn how to create or modify your reports.

Log Database - the center of Reporting

Created and powered by Microsoft® MSDE, the Log Database encompasses the Catalog Database (created at installation) and database partitions for reporting.

All log records are stored in database partitions. Data older than 30 days will automatically be deleted.

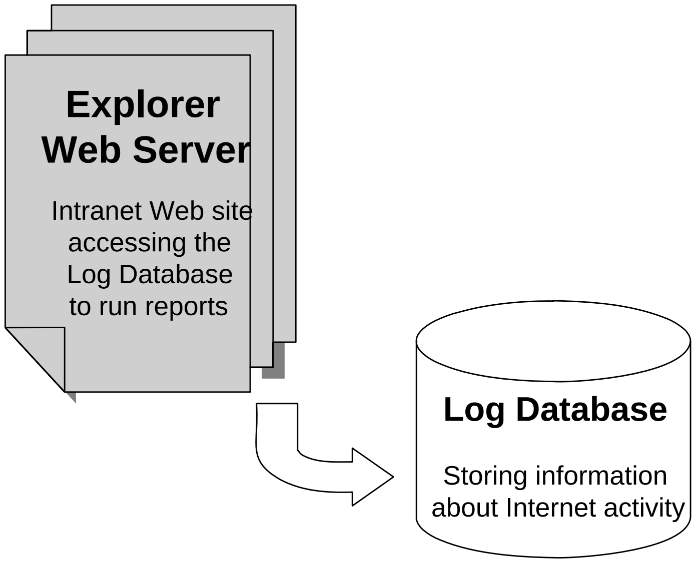
The Log Database receives and stores Internet activity data. Websense Express sends information to Websense Explorer about Internet activity. This activity is stored in the Log Database.

Information in the Log Database answers questions like:

- Who accessed the Internet?
- Who was blocked from accessing the Internet?
- At what time?
- What URL was accessed?
- How is that site categorized?
- How much time was spent online?
- What protocol was used?

Explorer Web server

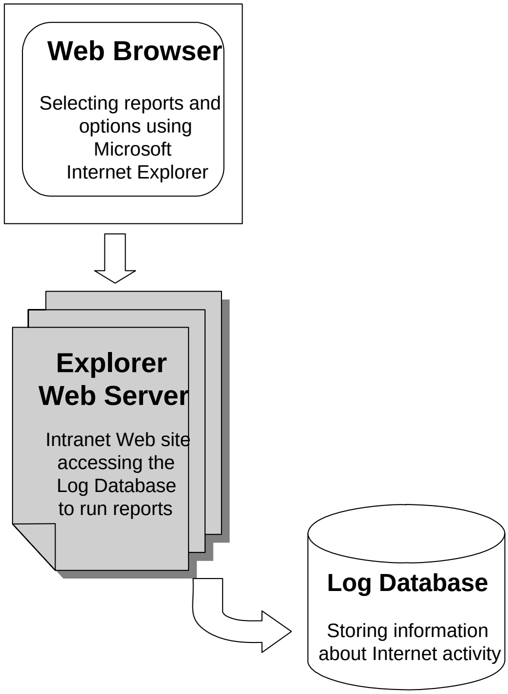
The Websense installer sets up the Explorer virtual directory.



Explorer Web server accessing the Log Database

Web browser

Access the Explorer Web server from your Web browser (Microsoft Internet Explorer).



Accessing the Explorer Web site from your Web browser

Explorer

Explorer is a viewer into the Log Database from your Web browser and it runs flexible detail reports on the logged activity.

Permissions

Permissions are granted by the administrator when creating a role. Permissions include:

- **Hide user names in reports**: Makes report entries anonymous in reports the administrator runs.

- **Save Favorite reports**: Allows the administrator to create and save report criteria for repeated use.
- **Schedule Favorite reports**: Allows the administrator to set Favorite reports to run in Explorer.
- **Database Administration**: Allows the administrator to use Database Administration to configure Internet Browse Time reporting and maintain the database partitions.

Set up with access permissions to all web-based Reporting tools, and set up with administrators attached to them.

Features

Explorer offers the following features:

- **Role-based Reporting**: Gives access to all web-based reporting tools based on a role.
- **Reporting Tools Portal**: Provides access to all web-based Reporting tools.
- **Favorite Reports in Explorer**: Includes saving report definitions as Favorite Reports (favorites). Favorites can be scheduled to run on a regular basis.
- **Flexible Detail View for Reports in Explorer**: Can be designed by drilling down into the filtering choices on Explorer's Summary view, and then clicking on the measurement bar for the detail view.
- **Multi-Level Reporting**: Allows you to display more than 1 dimension. Also limit the number of entries that are shown in the top reports, such as, Top URLs, Top Categories, and Top Users, with a starting value of 5. Select multiple rows for comparison or detail.
- **Summary View**: Launches when Explorer opens. View current activity in the database for all users. From there, you can drill down to see specific information and look at the activity in a variety of ways. Reports are line-item summaries or details of the report filters that you have selected.

Log Server

Receives Internet activity data from Filtering Service and inserts data into the Log Database.

Microsoft® MSDE Server Database

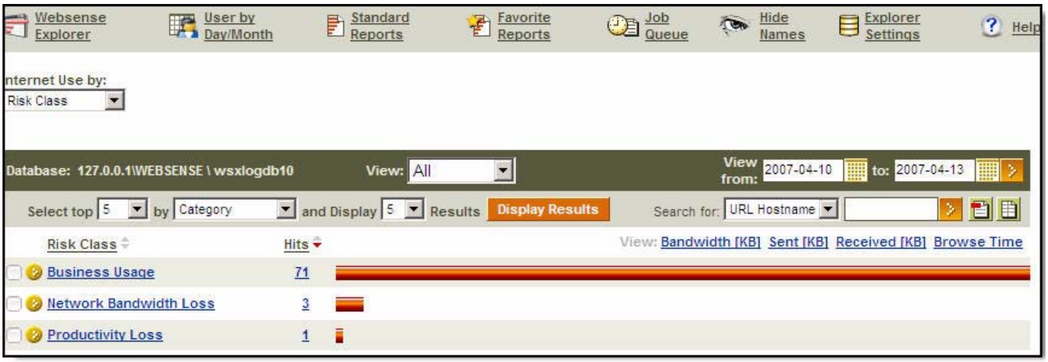
Log Database is created and powered by Microsoft Desktop Engine (MSDE).

Microsoft Internet Explorer

Standard Web browser used by Explorer to request reports.

Analyze Internet access trends

When you open Explorer, the main page is displayed. You can define any further reports from this page, or simply browse data in a real-time manner. For example, use the **Search** function to view activity for a particular user or client.



Explorer main page

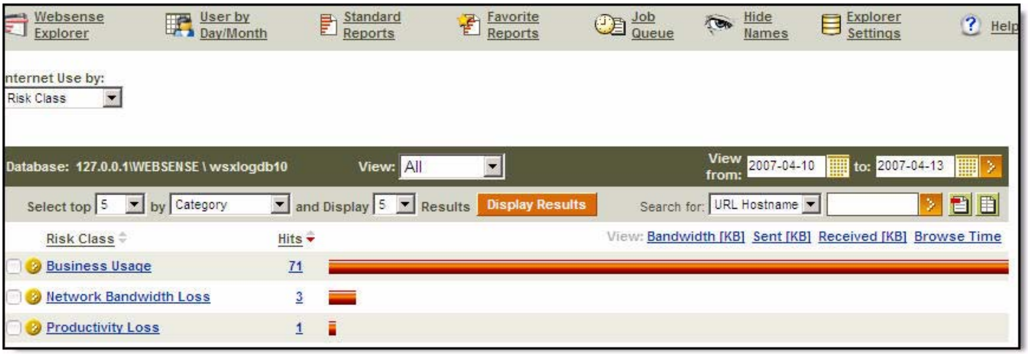
You can customize your report view using Explorer’s Flexible Detail Reports feature.

In Flexible Detail View, you can design your own reports, choosing or reordering up to seven columns and sorting through the detailed information.

NOTE

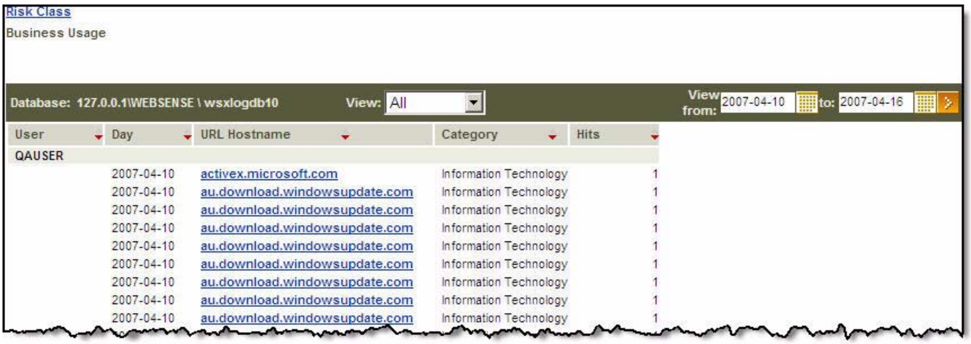
Although you can request a Detail View on any row, it is recommended that you drill down to less that 100,000 rows before requesting a detail report.

1. Run a Summary View or multi-level report. Your summarized results display.



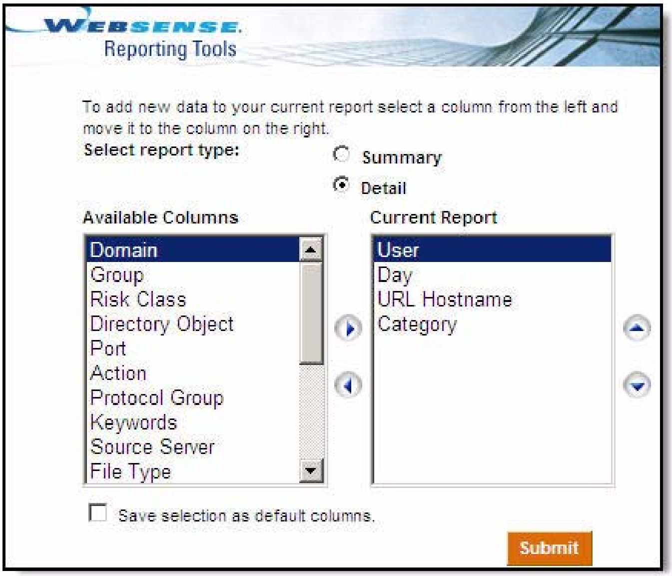
Summary View report

2. Drill into the results to create a Flexible Detail View. For this example, click the number value under **Hits**. You can also use the horizontal bar to drill down in a report. Explorer loads the detailed report area and displays a Detail View report.



Detail View report

3. Click **Modify Report** at the top of the page to begin designing a Detail View report.



Selecting report columns

The columns included in your Summary View report are already displayed in the **Current Report** Field.

4. Under **Available Columns**, select: **User**, **Day**, **Time**, **URL Hostname**. Highlight each selection and click the appropriate arrow button (< or >). These criteria display:
   - **User**: Name of the user who made the request.
   - **Day**: The day the request was made.
   - **Time**: The amount of time spent browsing the requested site.
   - **URL Hostname**: The domain name of the requested site.
5. Click the up and down arrow buttons to sort how the information should be displayed in your Flexible Detail View report. The first entry represents the first column in your report.
6. Click **Submit**. Your Detail View report loads and displays.
7. Click **Next** to page through the results. To look at the Web site visited, click the URL. The Web site opens in a new window.

NOTE
You can also save this report as a Favorite Report to schedule it to run on a recurring basis.

Accessing Websense Explorer and Reporting tools

Access Explorer and other Web-based Reporting tools through the Reporting Tools Portal. Log on at this page with your network User Name and password. The page will open in your browser (Microsoft Internet Explorer).

The logon is validated through the directory service. If no directory service is available, you will have to use the default Administrator logon of **WebsenseAdministrator** and the password that was set up to access the Policy Server in Websense Manager.

- Access to the Reporting Tools Portal is based on the Reporting roles created in Websense Manager.
- After roles have been defined in Websense Manager, enter your network User Name and Password to access the Reporting Tools Portal.

Note
The most recent versions of Microsoft Internet Explorer (v.6.x) have the highest default security settings. This causes users with this Web browser to be blocked from the Explorer pages, even though they are retrieved from an intranet server.

Reduce the Microsoft security level via the Microsoft Internet Explorer Web browser, or contact your System Administrator for assistance.

Ways to access Explorer reports

- Go to the **Current Status** or **Usage Summary** tab in Websense Manager, and then click the **Reporting Tools** link at the bottom of the page. Once logged on to the Reporting Tools Portal, click **Websense Explorer** to launch Explorer's main page.

- Double-click any graph in the **Current Status** and **Usage Summary** tabs in Websense Manager to launch Websense Explorer for more information. You are prompted to log on to the Reporting Tools Portal.
- Access Websense Explorer from a remote machine.

IMPORTANT

It is recommended that you click on the **Secure Log On** link to access Explorer. This ensures that your data, including the user name and password, will be protected.

Websense Express installs self-signed certificates for use with HTTPS. This will cause the browser to display a warning about the security certificate, since the certificate has not been issued by a certificate authority. If you wish to install a certificate that has been signed by a certificate authority like Verisign, you can replace the self-signed certificates with your own certificates. You can find more information on creating real Secure Sockets Layer (SSL) certificates on the Apache Web site at: http://httpd.apache.org/docs/2.2/ssl/ssl_faq.html#aboutcerts

Enter the URL path to Explorer in your Web browser. Depending on your Web server setup, use one of the following addresses.

Note

If you access Explorer through HTTPS, SSL uses a secure logon for port 8443. (If that port is in use, it increments to the next available port that is not being used.)

- https://<*machine name*>:<*port number*>/Websense

  Example: https://crobinson:8443/Websense
- https://<*IP address*>:<*port number*>/Websense

  Example: https://10.201.10.102:8443/Websense
- https://server.domain.com/Websense

Summary view of hits, bandwidth, or browse time

When you open Explorer, a Summary View report is run based on usage by Risk Class for all users, and for the most recent day's activity in the database.

When in summary view or multi-level view, click the number value in the table (hits, bandwidth, or browse time) or on the horizontal bar to see a *flexible detail view.*

At the top of the report, the date range is displayed with the most recent day's activity.

> **Note**
> When you link to Explorer from the Websense Manager Home Console, the date range from the console is inserted into the report. However, if your Log Database contains no data for the last date in the range (for example, no data logged on a weekend), you will receive a message telling you that the "to" date in the range is past the last date in the database.
>
> Change the date range to match your database before trying to run any reports.

Also see:

- Primary report choice
- Machine name where the database is located and name of the database (or the Data Source Name)
- 1 day, 1 week, 1 month, or All
- How much of the database is being used by the data in the selected date range
- Date range chosen for the report
- Display results
- Results of your search
- Output to Portable Document Format (PDF) or Microsoft Excel spreadsheet
- Table headings for the report results

- Whether hits, bandwidth, or browse time has been chosen for the view

The results of the report are shown by result labels, number of hits, and horizontal bars.

The result labels identify the name of the Risk Class in that row. Check the boxes to the left of the report to refine your search and obtain information on those entries only.

The Hits column displays how many hits or visits were made in that Risk Class (or how much bandwidth or browse time was used by that activity).

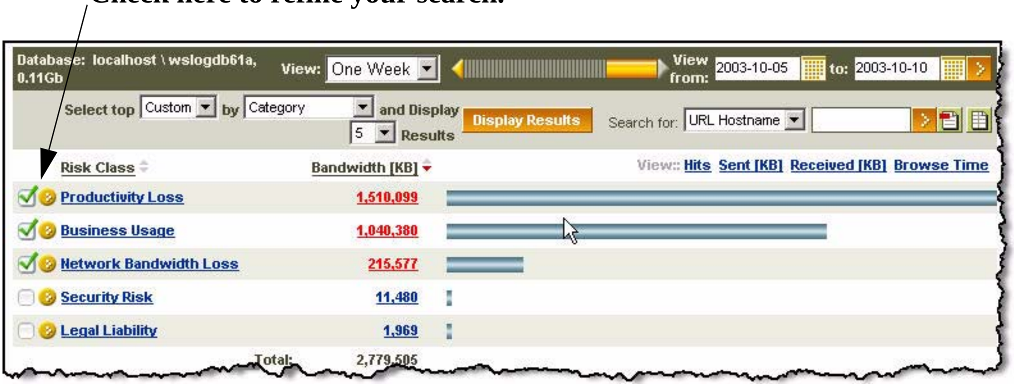
The horizontal bars provide a visual comparison among the rows. When the cursor rests over a horizontal bar, a small pop-up gives you the percentage of that row relative to the total.

The default order of the rows in the table is generally based on highest amount of activity to the lowest (descending).

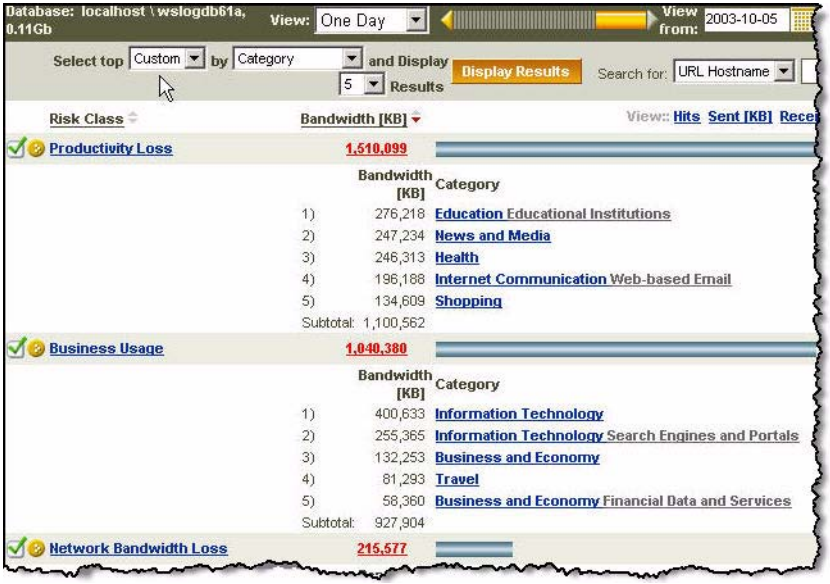
Drill-down for more information on a specific entry

Check the box next to the > (drill-down arrow) to select 1 or more entries, and to see more information about the categories for these entries. The information for the selected entries is listed in the report.

Check here to refine your search.



The information for the selected entries is listed in the report.



There is a limit to the amount of information that can be displayed in Explorer's main page. When this limit is reached, the report extends over additional pages. To view additional pages, select the page number at the top of the report or click **Next**.

Primary report choices

Primary report choices are in the upper left corner of the main page in the **Internet Use by** field, just under the calendar.

These choices vary, depending on the database and Explorer's configuration settings.

- If there are no groups defined in the database, Group will not be a primary report choice or in the drop-down options.
- If there are more than 3,000 groups, Group will not be a primary report choice.
- If there is only 1 domain, Domain will not display as a primary report choice.
- If there are more than 5,000 users, User will not be a primary report choice.

To obtain more information about the data in a row, drill down into the *flexible detail view.*

Changing report dates

See the date range available in the database listed at the bottom of the Calendar dialog box. Also see the earliest and latest available database dates by hovering over the calendar icons in their respective **View from** and **To** fields.

1. Limit the report by changing the date range.

   Enter the new start or end date by typing over the previous date, or click the calendar icon.

   Navigate inside the calendar to find the year and month for the start or end date of the report.

2. After the correct dates are chosen, close the calendar.
3. When you have adjusted the dates, click > (**Go** arrow) to produce the new report.

   If a date is outside the available range, you will receive an error message.

Searching for information

- Since you are viewing Explorer reports through a Web browser, use the Web browser's search feature. Select **Find (on this Page)** from the the **Edit** menu to access the Web browser's search tool.
- Use the **Search** fields:
  a. Select 1 of the following: **User**, **URL Hostname**, **Destination IP**, or **Source IP** in the left **Search** field to focus your search.
  b. Enter part or all the identifying details, such as last **user** name, **URL**, or **IP**, into the next **Search** field. Enter the exact spelling.

     Note: When entering only a portion of an IP, the subnet of that entry is searched. For example, if you enter 10.5., subnets 10.5.0.0 through 10.5.255.255 are searched.

  c. Click > (**Go** arrow).

Search for a user

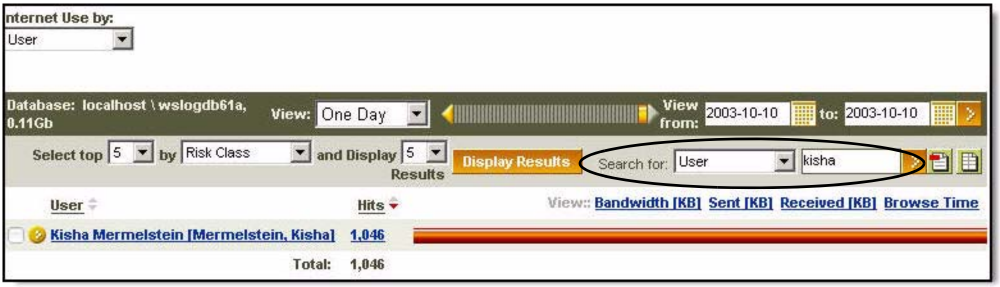
Find Internet usage for a particular person or group.

1. Select 1 of the following: **User**, **URL Hostname**, **Destination IP**, or **Source IP** in the left **Search** field to focus your search.
2. Enter part or all the identifying information into the second (right) **Search** field.
   - Enter all or part of the first or last **user** name or **URL**, and make sure whatever you enter is the exact spelling.

- Enter the whole **IP**, or a portion thereof.
  Note: When you enter only a portion of the IP, the subnet of that entry is searched. For example, if you enter **10.5.**, subnets 10.5.0.0 through 10.5.255.255 are searched.

3. Click **>** (**Go** arrow).

In the following example, **kisha** was entered in the **Search for User** field.



Once you have located the user, click > (drill-down arrow) or User Name link for more choices.

Click the drill-down arrow or User Name link for more choices.

Hide names

It may be useful to show a person or group in a report without showing user information.

Use the Hide Names link to display User IDs instead of User Names.

The Hide Names link toggles back and forth with Show Names.

Note:
When you choose to set up anonymous logging in Websense Manager, Explorer reporting will omit user information in the reports that are run.

If you choose to not log user names, user names are omitted from the report output to preserve anonymity in Internet usage reporting.

If you choose to not log IP addresses, IP addresses are omitted from the report output.

Self-Reporting

Allows users to see Explorer reports only on their own Web browsing, showing what information is being gathered and monitored. This, then, gives users the opportunity to alter their Internet browsing habits and accommodates government regulations that require companies to allow users to see the type of information that is being collected.

Roles do not need to be set in Websense Manager to initiate self-reporting. Instead, check **Self Reporting** in *User Settings* on the Reporting Tools Portal to allow users to self report in Explorer. See information on editing these settings in the topic titled *User Settings*.

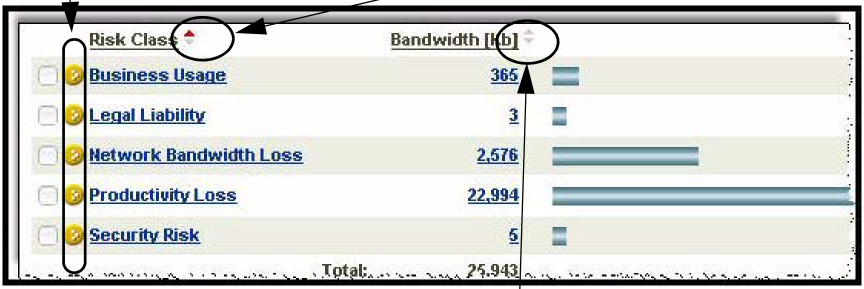
Sorting information in Explorer reports

Reorder the Explorer rows alphabetically by choosing the table heading at the top of the rows. In the following example, the small arrows to the right of

Risk Class indicates that the column has been sorted alphabetically in ascending order.

Drilling down to select 1 or more entries.

Sorting the column alphabetically.

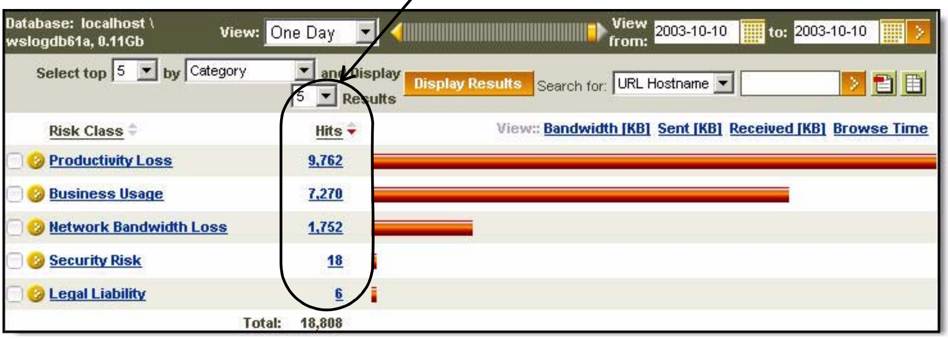


You can also reorder the rows by value by choosing the column heading at the top of the measure values in ascending or descending order.

Also reorder the rows in ascending or descending order (value).

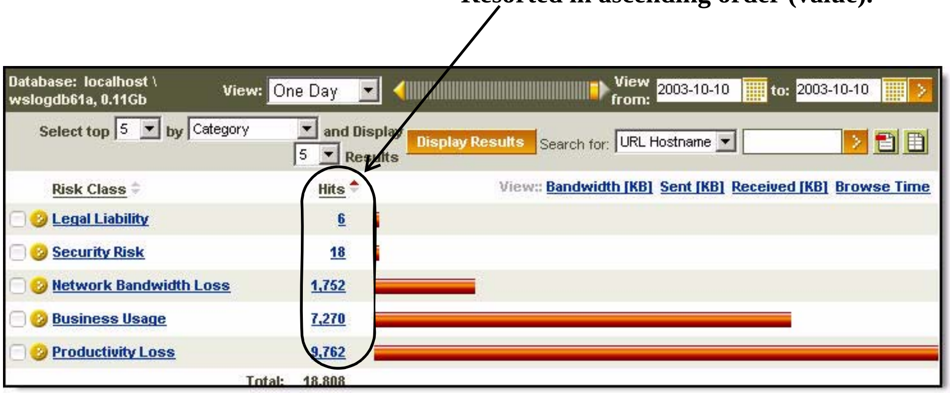
Click the arrows next to the current measure heading (Hits, Bandwidth, or Browse Time) at the top of the rows. In the following example, Risk Class has been sorted by value in descending order.

Sorted in descending order (value).



The following has been resorted in ascending order (value).

Resorted in ascending order (value).



Types of Explorer reports

The following types of Explorer reports are discussed:

- Flexible Detail View
- Standard Reports
- Multi-level Reporting
- Favorite Reports
- User activity by day or month

Flexible detail view

In the flexible detail view, design your own reports on Web sites that have been visited by choosing or reordering columns and sorting through the detailed information.

There is a limit of 7 columns to view information in each report.

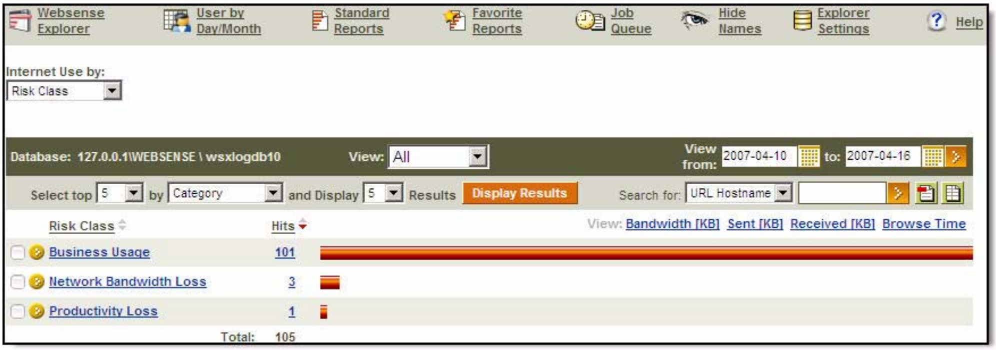
Although you can request a detail view on any row, you should probably drill down to less than 100,000 rows before requesting a detail report.

Also, Explorer is limited by your processor, available memory and network resources, and may time out on requests for large reports.

IMPORTANT

In any drop-down or values list, information may display in red. The red lettering is to warn that this option may result in a very large report. It will likely be more useful to drill down further into results before making this choice.

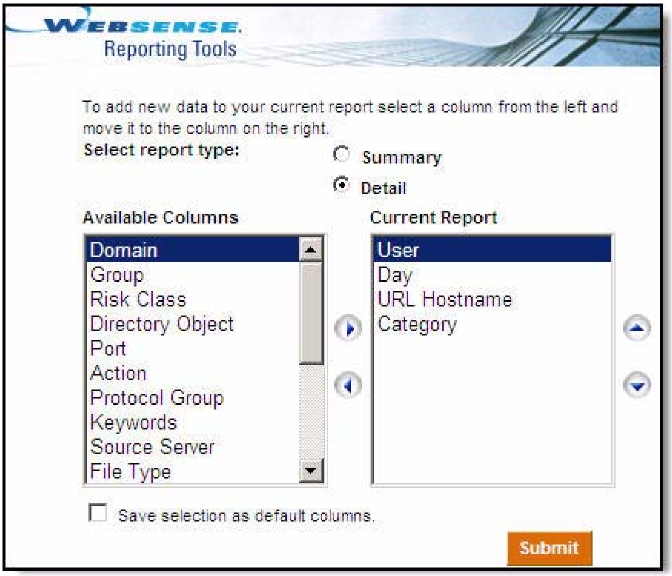
1. Run a Summary View or Multi-Level report for a summarized list of results.



2. Drill down into the results to create a flexible detail view. Click the number value of **Hits**, **Bandwidth**, or **Browse Time**. Or, click the measurement bar. Explorer loads the detailed report area.

   Note: If the report is taking a long time to generate, save it as a Favorite Report and schedule it to run later. Explorer is limited by your processor, available memory, and network resources and will time out on requests for large URL reports.

3. Click **Modify Report** at the top of the page to begin designing a Detail View report specific to your needs. For example, reorder the columns, choose to include or exclude information, and include up to 7 columns of information in your report. The dialog box displays the flexible design selections.

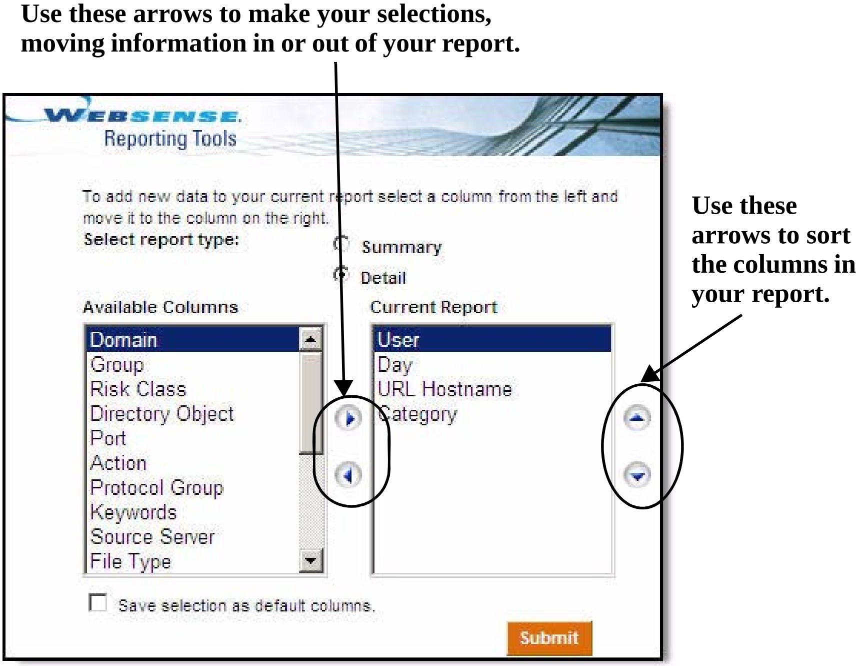


The information columns included in your Summary View report are already displayed in the **Current Report** Field.

4. Design your Detail View report, choosing from the **Available Columns** field. Highlight each selection and click the appropriate arrow button (< and >) to make your choices and move selections into or out of the Detail View report.

> **Note**
>
> You can have a maximum of 7 columns of information in your report.

5. When you have made your selections and added them to the **Current Report** field, click the appropriate up and down arrow buttons to sort the order of the information to be displayed in your report. The first entry represents the first column in your report.



This selection process allows you to report on the information you want to see, in the order you want it displayed.

6. Click **Submit** to load and display your report. The Detail View report is based on time. If there is more than 1 page of results, click **Next**. To look at the actual Web site visited, click the URL. The Web site will open in a new window.

   Save this report as a Favorite Report to schedule it to run on a recurring basis.

Example of drilling down into results

To obtain information about the data in a row, click > (drill-down arrow) on the left hand side.

- To get more information about any of the Risk Classes, click > (drill-down arrow).

Information about the usage in this Risk Class is available from the drop-down list.

IMPORTANT

In any drop-down or values list, information may display in red. The red lettering is to warn that this option may result in a very large report. It will likely be more useful to drill down further into results before making this choice.

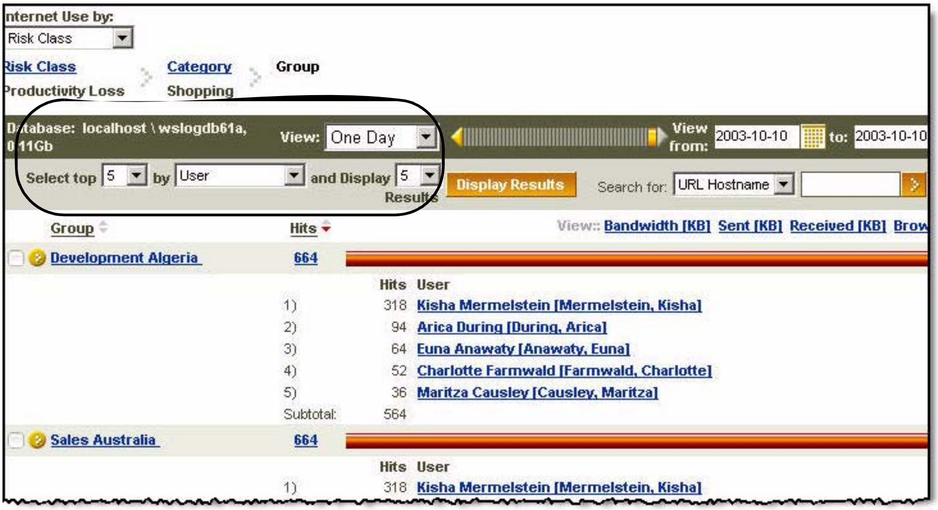
- To see which categories have Internet activity that is considered to be a risk from Productivity Loss, select by **Category**.

For more information, drill down further.

- Select Top N where N represents the number of objects to compare by another filter. For example, you could limit your entries in the Top By

Hits report. To limit your entries by user in the Shopping category, select **Top 5** by **User** to display **Top 5**. Click **Display Results** to get the report.

Selected the top 5 Users within the top 5 Groups.



- You can drill down and see the information for a specific group.

List of URLs

To see specific addresses of Web sites that have been visited, run a URL report.

- Select the number of hits, or measurement bar, to get a URL report on a row.
- Although you can request a URL report on any row, it is not practical or useful to generate a report with millions or even a hundred thousand URLs.
- Explorer is limited by your processor, available memory, and network resources. Explorer will time out on requests for large URL reports.
- The following list explains Explorer's default guidelines for displaying URL reports. These configuration settings can be changed in the `wse.INI` file.
  - Explorer displays URL reports with consolidated URLs, unless the number of hits is more than 3,000.

- If the number of hits is more than 3,000, then the URLs display in time sequence, unless the number of hits is more than 30,000.
- If the number of hits is more than 30,000, the URLs are not grouped by URL or shown by time sequence. Instead, the hits are displayed in random order.
- If there are more than 3,000 hits, you can try to override the constraint against requesting a report grouped by URL.
- If there are more than 1,000,000 hits, you will not be able to override the constraint.
- If there are more than 500 hits displayed in time sequence, they will be presented in the pages of the report.

◆ To look at the actual Web site visited, select the URL.

Standard reports

Standard reports are provided as part of Explorer. Generate any of these reports and schedule them to run on a recurring basis. To learn about scheduling reports, see *Scheduling Explorer Reports*.

Run Standard Reports to get information about the potential security risks your company faces. Also see details about how users are accessing the Internet, consuming bandwidth, and causing loss of productivity.

The categories and Standard Reports are:

Highest activity levels

- **Which users have the most hits**: View the users on your network, sorted by day, time, URL Hostname, and Bandwidth within the Risk Class, Network Bandwidth Loss, to find the highest amount of hits to the lowest.

  A hit is a request for one URL. A Web page contains many elements, each having its own URL. Requesting the URL for the overall page automatically generates requests for each component (including images) that make up the Web page.
- **Top 10 users for top 10 visited URLs**: View the top 10 users with the top 10 URLs visited. Shows the top Web sites that people in your organization are browsing.
- **Top 5 users activity in Shopping, Entertainment and Sports**: View the top 10 users visiting the shopping, entertainment, and sports Web sites more than occasionally.

- **Top 5 URLs for top 5 visited categories**: The top five URLs for the top five visited categories are shown. For example, you can check to see if there are hits that have been logged to Adult Material: Adult Content sites. If that is the case, these sites may contain adult material and may increase your organization's risk of legal liability in a sexual harassment-related situation.

Most blocked

- **Which users were blocked most**: Look at users who may be looking for a way around the system. Look at the URLs in the Miscellaneous category for these users.
- **Which sites were blocked most**: See which sites were blocked most. You have implemented a policy to block certain categories from being viewed by employees, and would like to know how valuable this policy has been to the organization.
- **Detail URL report on users who were blocked**: See which sites were blocked for all users. Details are shown by user, day, time, URL Hostname, and number of hits.
- **Top 10 blocked categories**: View the top 10 visited categories that have blocked access.

Highest bandwidth consumption

- **Which groups are consuming the most bandwidth**: Use this report to find groups who are downloading audio, video, and other large files. View Risk Class and Network Bandwidth Loss, along with the details about users, day, time, and URL hostname.
- **Groups consuming most bandwidth in Streaming Media**: View the groups using the most bandwidth. For example, when reviewing data related to instant messaging, you can view bandwidth used by MSN Messenger, Yahoo! Messenger, and AOL Instant Messenger.
- **Detail URL report on users by network bandwidth loss**: See the top URLs (sites) users have visited that are consuming the most Network Bandwidth.
- **Top groups for Bandwidth Premium Groups**: View the top 10 groups by Premium Group to see how much bandwidth is being consumed and in which categories.

Highest security risk

- **Top categories posing a security risk**: View what high security risk categories are the most heavily trafficked on your network. Some of the security risk categories are Hacking, Peer-to-Peer (P2P), and File Sharing.
- **Top users of P2P protocol**: View the top users with heavy traffic in Peer-to-Peer (P2P) activity that can pose a possible security risk to your company.
- **Top users of Security Premium Group sites**: Websense Premium Groups are Master Database categories with associated subcategories that enhance your ability to manage and report on Internet use. View the top users of the Security Premium Group (Security PG) for all categories.
- **URLs for top 10 machines with spyware activity**: You may find it useful to see if there is any activity in the Spyware category. View the sites users have visited that contain spyware activity.

Most time online

- **Which users spent the most time online**: This report calculates the time users spend accessing the Internet and can include details about the time spent at each site. Internet Browse Time is an approximate measurement of the cumulative time a user has spent browsing.
- **Users that spent the most time on Productivity PG sites**: View users that have spent the most time visiting personal sites (sites listed in the Productivity Premium Group (PG) that are not business-related), causing productivity loss.

Legal liability

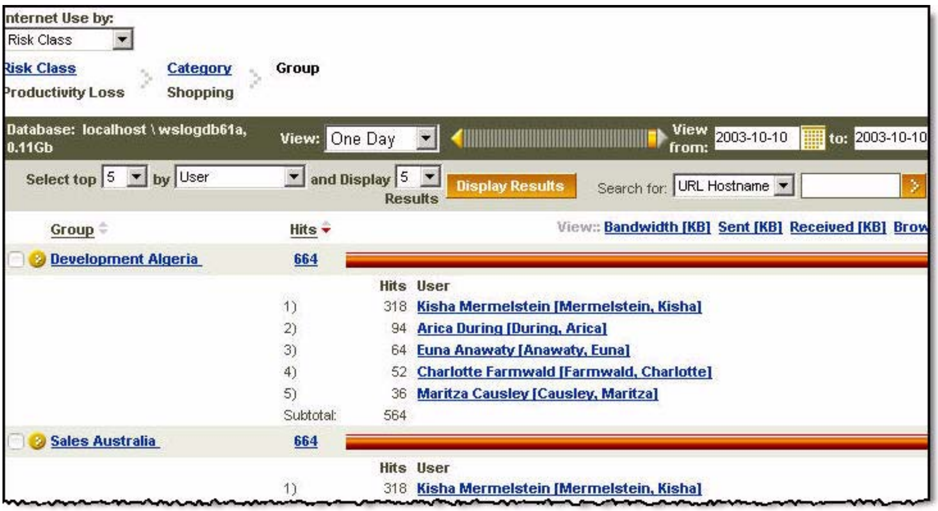
- **Legal Liability Risk by Category**: Use this report to find activity in Internet sites, including gambling, adult material, and other categories, who could potentially make your company liable for legal action.
- **Top users in Adult categories**: This report let you see users who have the most activity visiting sites with adult material and who could potentially make your company liable for legal action.

The logon is validated through the directory service. If no directory service is available, you will have to use the default Administrator logon of **WebsenseAdministrator** and the password that was set up to access the Policy Server in Websense Manager.

1. Go to the Reporting Tools Portal from the **Current Status** tab in Websense Manager.
   - Access to the Reporting Tools Portal is based on the Reporting roles created in Websense Manager.
   - After roles have been defined in Websense Manager, enter your network User Name and Password to access the Reporting Tools Portal. The Reporting Tools Portal provides access to:
2. Click **Websense Explorer** to launch Explorer's main page.
3. Click **Standard Reports** at the top of the page.

Multi-level Reporting

Run multiple levels of Reporting, comparing dimensions by using the top dimension (for example, users, categories, and URL hostname) and another dimension. This displays the top N where N represents another filter with a value starting at 5. Also select multiple rows for comparison or detail.



Favorite reports

When you have defined a report in Explorer that you would like to generate again, save it as a Favorite report. Click **Favorite Reports** at the top of the page. Your report heading is displayed in the field directly above other favorite reports already saved.

- Click **Add** to add this report to your Favorite Reports list.
- Schedule up to 5 favorite reports in 1 job when scheduling favorites.
- Reports have to be saved as Favorites before they can be scheduled.

Creating Favorite reports

When you have created a user-defined report in Explorer, you have the option to save the report as a Favorite report.

1. While in the flexible detail view for reports in Explorer, design your report by drilling down into various filtering choices on Explorer's Summary view. Click **Modify Report** to add or delete columns.

   When you have finished choosing the criteria, reordering the columns, and sorting through the details to get the report you need, you are ready to save (create) a Favorite report.
2. Click **Favorite Reports** in the Explorer tool bar.
3. Name the new Favorite report by using the name that Explorer has assigned, or enter a different name unique to your reporting needs.

   If you enter a name that already exists in the list of favorites, you will receive a message stating that the name already exists.
4. Click **Add to Favorite Reports**. Your new Favorite report is saved in the list of Favorite Reports.

   Once your Favorite report is created, you can schedule it, delete it, or run it on demand. You can also go into the flexible detail view and modify the report to create a new Favorite report.
5. Click **Close**.

Generating Favorite reports

1. Click **Favorite Reports** in the Explorer tool bar.
2. Select a Favorite report from the list of Favorite Reports, and then:
   - Click **Run Now** to run the report immediately.
   - Click **Schedule** to schedule the report to run later or on a recurring basis.
3. Click **Close**.

Modifying Favorite reports

Rather than modify Favorite reports within Explorer, create a new Favorite report from an existing Favorite, and then save it as a new Favorite report.

1. Click **Favorite Reports** in the Explorer tool bar.
2. Run an existing Favorite report, make changes, and then save it as a Favorite report.
3. Click **Close**.

Deleting Favorite reports

1. Click **Favorite Reports** in the Explorer tool bar.
2. Select a Favorite Report from the list of saved Favorite Reports, and then click **Delete**.
3. Click **Close**.

Scheduling Favorite reports

- Schedule up to 5 Favorite Reports in 1 scheduled job.
- Schedule selected reports to run at a specific time on a repeated basis with the Scheduled Jobs feature. These reports can be emailed to selected recipients.

User activity by day or month

This report shows activity for only 1 user at a time. Even if you have drilled down into other areas (such as category, risk class, or action), the User Activity by Day or Month only reflects the date and user.

User activity by day

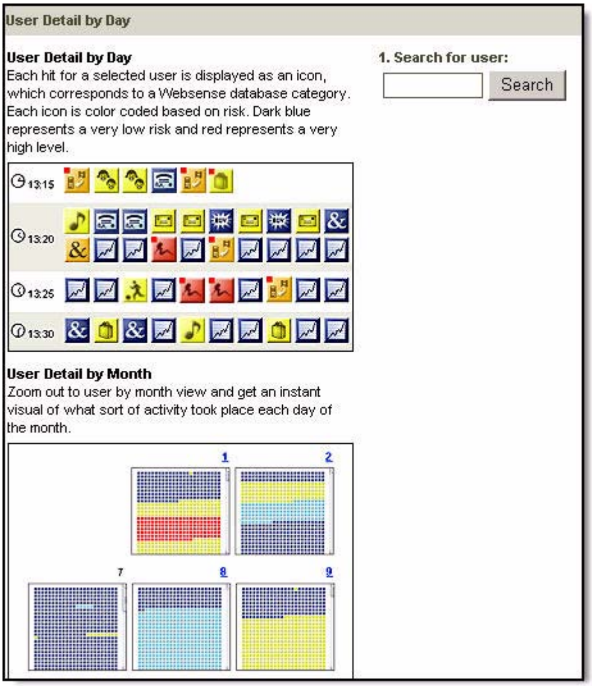
See a more in-depth view of a specific user's activity.

The logon is validated through the directory service. If no directory service is available, you will have to use the default Administrator logon of **WebsenseAdministrator** and the password that was set up to access the Policy Server in Websense Manager.

Go to the Reporting Tools Portal from the Current Status tab in Websense Manager.

- Access to the Reporting Tools Portal is based on the Reporting roles created in Websense Manager.
- After roles have been defined in Websense Manager, enter your network User Name and Password to access the Reporting Tools Portal.

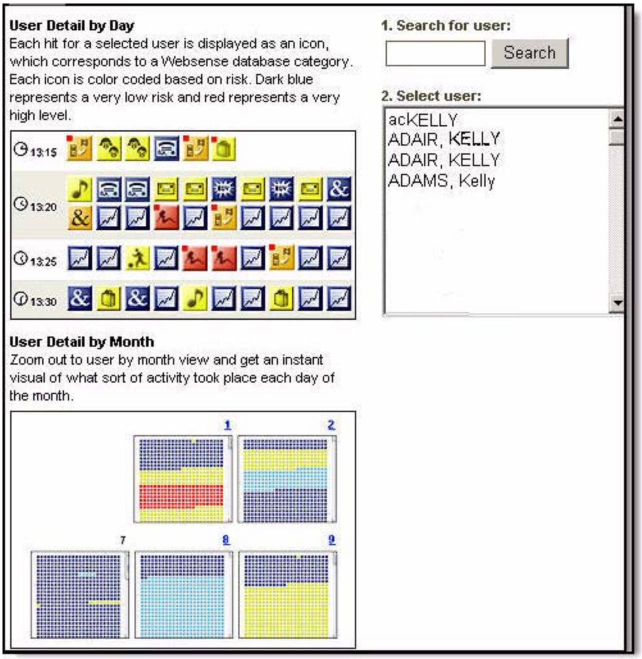
1. Click **Websense Explorer** to access the Websense Explorer page.
2. Select **User by Day/Month** at the top of the page. The User Detail by Day box appears.



3. Enter a user's name, or a portion of the name, in the **Search for a user** field, and then click **Search**. For example, enter **kelly**.

   If the user is not found in the database in the `user_name` table, an error message is displayed, stating that there are no names found containing xxx.

Otherwise, a list of up to 100 matching user names is displayed with a maximum of 10 entries listed in alphabetical order in the **Select desired user below** field.

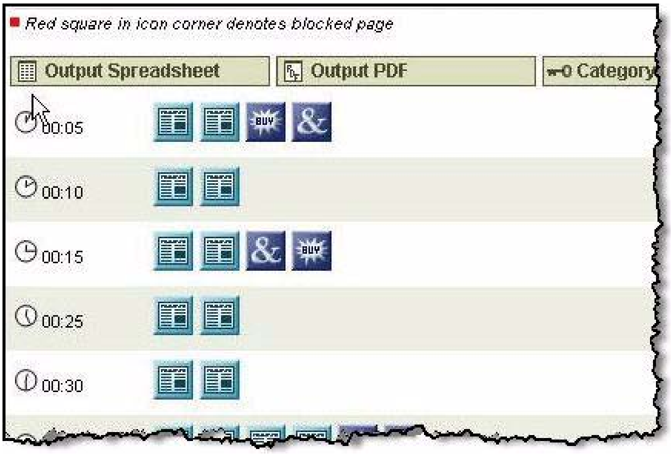


4. Select a user from the list of matching entries found in field 2. When you select a user, the last date of that user's activity is displayed, by default, in the **Select day you would like to view** field.
5. Leave the date as is, or enter a new date. Either type over the previous date or click the calendar icon to make a new date selection.

   A calendar window displays, giving you the option to scroll through months and years to select a specific date for this user.

   A list of available dates for this user is noted at the bottom of the calendar.
6. Make your date selection, and then close the calendar.

7. Click **Go to User by Day**. If there is no user activity for that day, a blank report is displayed with only a top banner. Otherwise, the detail activity for that user is displayed. See *Database Category* and *Category view* for information on the detail activity icons.

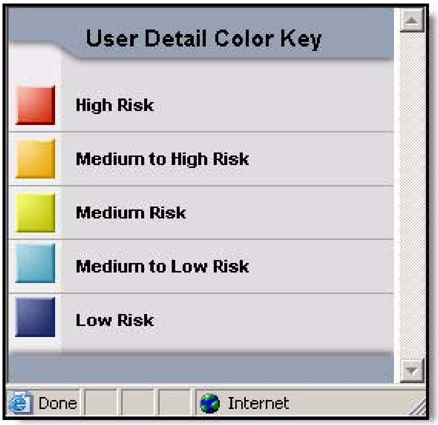


The timeline view shows the user's activity in 5-minute increments and the categories are represented by icons.

Each hit for a selected user is displayed as an icon, which corresponds to a Websense Master Database category. Each icon is color coded, based on risk. See *Database category* for the User Detail Color Key information and *Category view* for an example list of categories.

Database category

The Database Category legend provides a key to the visual cues about the risk levels displayed. The risk levels range from high risk to low risk.



Category view

At the Category View Control, select which categories to display and which categories to hide. The categories with a check mark in the check box will be displayed.

To see which categories are represented by which icon, click **Category View Control**.

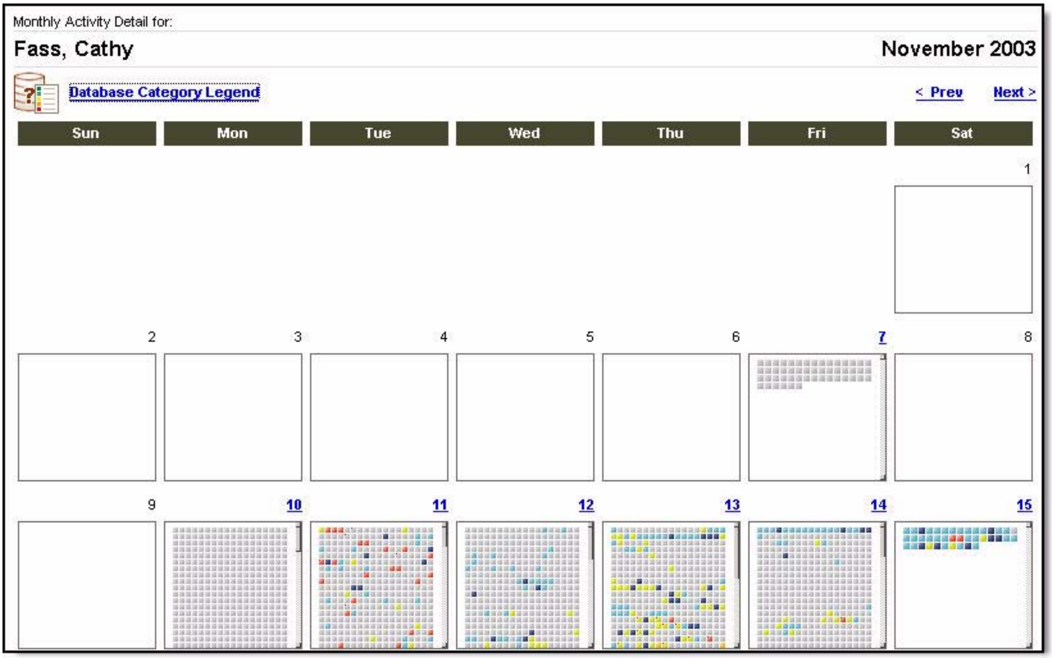
To hide a category, click inside the checkbox to remove the check mark, then click **Accept**.

User activity by month

While in the User Activity Detail report, see the monthly activity for that user. The following example looks at the monthly activity for Cathy Fass.

Click **User Activity Detail by Month** at the top of the Daily Activity Detail report.

The report is displayed in calendar format with the daily activity displayed in thumbnail categories.

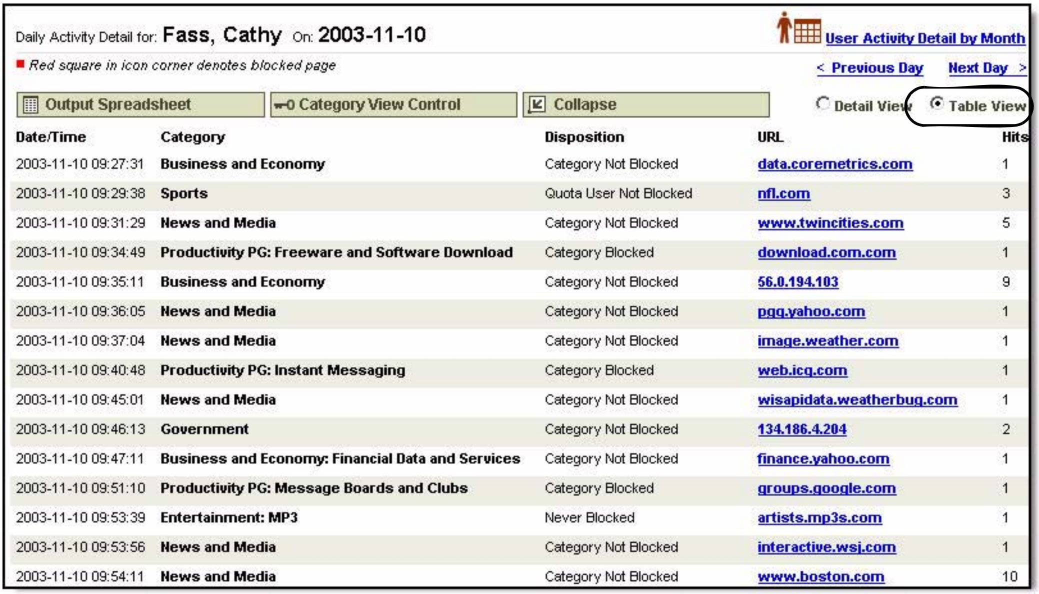


Collapse the view

Click **Collapse** to hide hits that are similar. This algorithm hides hits that have occurred within a particular time threshold (default is 10 seconds) with the same base URL, category, and action.

Collapse toggles back and forth with Expand. Click **Expand** see all the hits not restricted by the Category View Control.

To see the view in a column format, select **Table View**.



Daily Activity Detail for: **Fass, Cathy** On: **2003-11-10**

User Activity Detail by Month

Red square in icon corner denotes blocked page

< Previous Day   Next Day >

Output Spreadsheet | Category View Control | Collapse | Detail View | Table View

Date/Time	Category	Disposition	URL	Hits
2003-11-10 09:27:31	Business and Economy	Category Not Blocked	data.coremetrics.com	1
2003-11-10 09:29:38	Sports	Quota User Not Blocked	nfl.com	3
2003-11-10 09:31:29	News and Media	Category Not Blocked	www.twincities.com	5
2003-11-10 09:34:49	Productivity PG: Freeware and Software Download	Category Blocked	download.com.com	1
2003-11-10 09:35:11	Business and Economy	Category Not Blocked	56.0.194.103	9
2003-11-10 09:36:05	News and Media	Category Not Blocked	pgq.yahoo.com	1
2003-11-10 09:37:04	News and Media	Category Not Blocked	image.weather.com	1
2003-11-10 09:40:48	Productivity PG: Instant Messaging	Category Blocked	web.icq.com	1
2003-11-10 09:45:01	News and Media	Category Not Blocked	wisapidata.weatherbug.com	1
2003-11-10 09:46:13	Government	Category Not Blocked	134.186.4.204	2
2003-11-10 09:47:11	Business and Economy: Financial Data and Services	Category Not Blocked	finance.yahoo.com	1
2003-11-10 09:51:10	Productivity PG: Message Boards and Clubs	Category Blocked	groups.google.com	1
2003-11-10 09:53:39	Entertainment: MP3	Never Blocked	artists.mp3s.com	1
2003-11-10 09:53:56	News and Media	Category Not Blocked	interactive.wsj.com	1
2003-11-10 09:54:11	News and Media	Category Not Blocked	www.boston.com	10

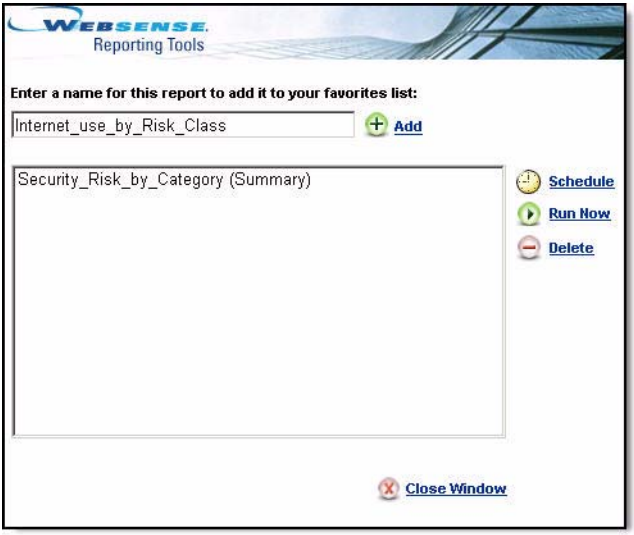
Scheduling Explorer reports

Schedule up to 5 Favorite Reports in 1 scheduled job. Reports can be generated at regular intervals and emailed to others.

First create the Favorite Report, and then schedule the report to run later.

1. Create a Favorite Report in Explorer.

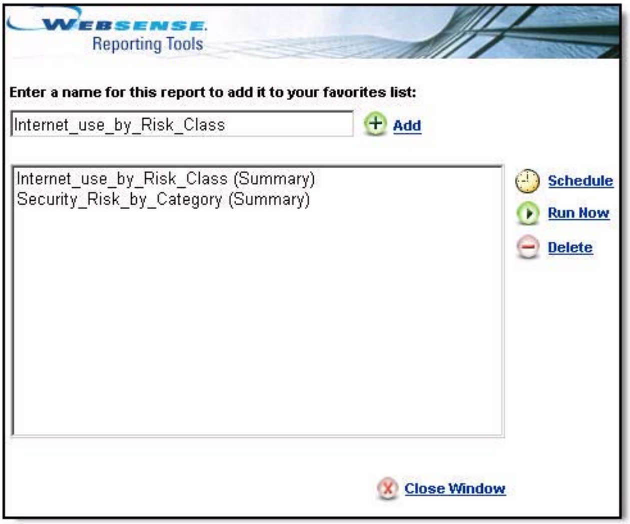
a. Click **Favorite Reports** in the Explorer tool bar. The Favorite Reports dialog box appears.



b. Name the new Favorite Report by using the name that Explorer has assigned, or enter a different name unique to your reporting needs.

If you enter a name that already exists in the list of Favorite Reports, you will receive a message stating that the name already exists. Enter a different name, or use the assigned name.

c. Click **Add**. Your new Favorite Report is saved in the list of Favorite Reports.



Once your Favorite Report is created, you can schedule it, delete it, or run it on demand.

2. Schedule the Favorite Report in Explorer.
   a. Click **Favorite Reports** in the Explorer tool bar.
   b. Select a favorite from the list of Favorites.

   --Click **Schedule** to schedule the report to run later or on a recurring basis.

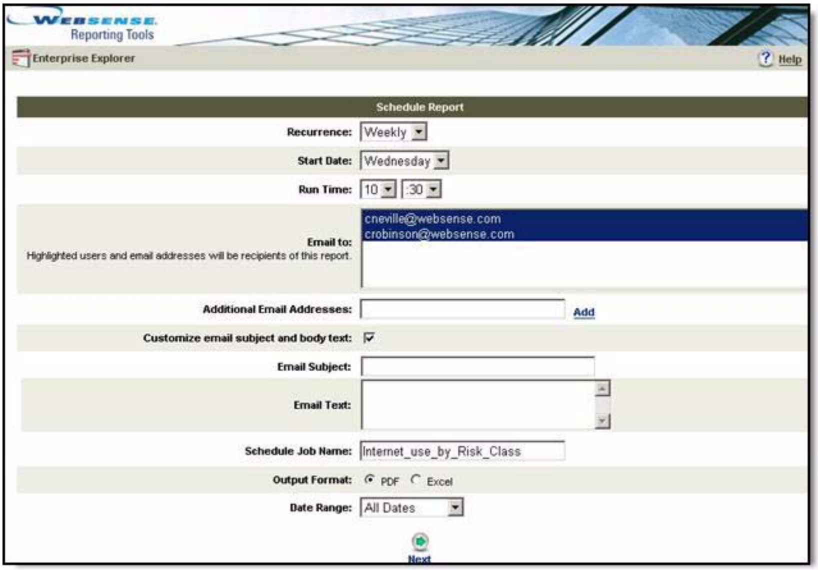
Note

You can schedule up to 5 *Favorite Reports* in 1 scheduled job.

--Click **Run Now** to run the report immediately.

--Click **Close Window** to exit.

c. Click **Schedule** to schedule the report. The Schedule Report dialog box appears.



d. Click **Next**. The Schedule Confirmation dialog box appears, confirming your scheduling choices.

e. Click **Save** to save your selections or **Previous** to go back and update your selections.

Exporting Explorer reports

Explorer report results can be exported to a Microsoft Excel spreadsheet or Portable Document Format (PDF) (either A4 or 8 1/2 X 11inches in size).

Regardless of the output format, there is no formal page sequence, which does not affect page numbers within the report. Every 1,000 rows of results are processed, inserting a new page break with banner, title, and column headers.

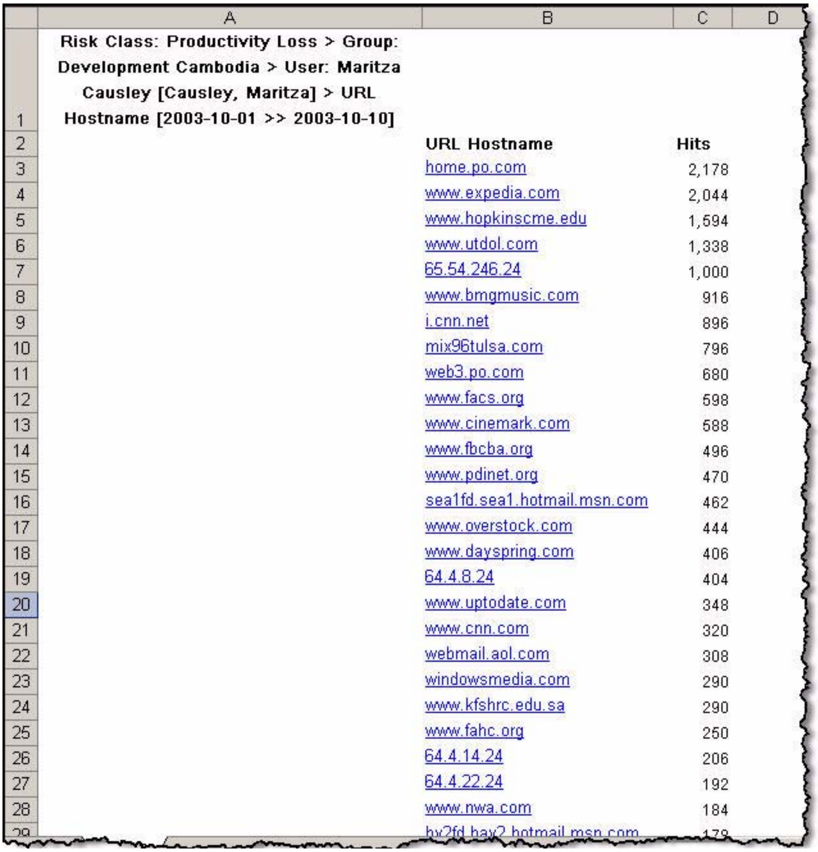
Output to spreadsheet

Export Explorer report results to a Microsoft Excel spreadsheet by choosing the **Output Spreadsheet** icon on the far right side of the page.

1. Define the report.
2. To produce an Excel file, click the **Output Spreadsheet** icon
3. Choose whether to Open the file, or Save it to your hard drive.

   Note: You need to have Microsoft Excel installed on your system in order to view the Excel files.

   Your Excel file should look similar to the following.



	A	B	C	D
1	Risk Class: Productivity Loss > Group: Development Cambodia > User: Maritza Causley [Causley, Maritza] > URL Hostname [2003-10-01 >> 2003-10-10]			
2		URL Hostname	Hits	
3		home.po.com	2,178	
4		www.expedia.com	2,044	
5		www.hopkinscme.edu	1,594	
6		www.utdol.com	1,338	
7		65.54.246.24	1,000	
8		www.bmgmusic.com	916	
9		i.cnn.net	896	
10		mix96tulsa.com	796	
11		web3.po.com	680	
12		www.facs.org	598	
13		www.cinemark.com	588	
14		www.fbcba.org	496	
15		www.pdinet.org	470	
16		sea1fd.sea1.hotmail.msn.com	462	
17		www.overstock.com	444	
18		www.dayspring.com	406	
19		64.4.8.24	404	
20		www.uptodate.com	348	
21		www.cnn.com	320	
22		webmail.aol.com	308	
23		windowsmedia.com	290	
24		www.kfshrc.edu.sa	290	
25		www.fahc.org	250	
26		64.4.14.24	206	
27		64.4.22.24	192	
28		www.nwa.com	184	
29		by2fd.bay2.hotmail.msn.com	[illegible]	

Output to Portable Document Format (PDF)

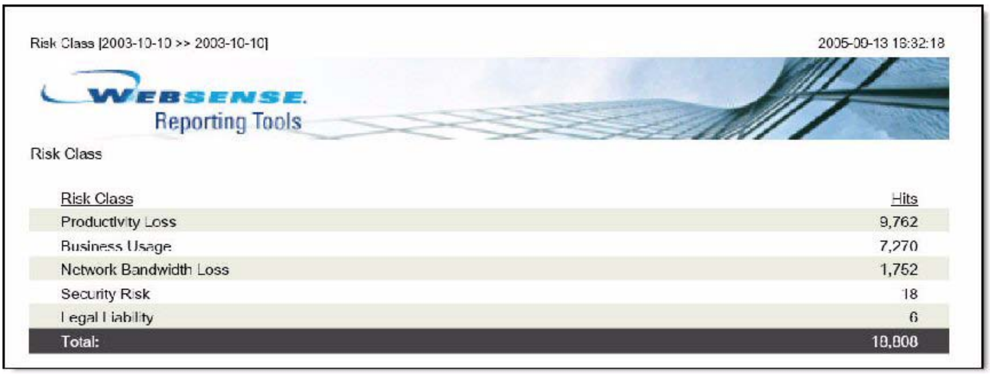
Export Explorer report results to Portable Document Format (PDF) by choosing the **PDF Output** icon on the far right side of the page.

1. To produce a PDF of this report, click the **PDF Output** icon.

> **Note**
>
> If you are using Adobe Acrobat Reader and it requires updates, you will receive a prompt to download updates in a separate window that usually opens behind other open windows. Go to that window and either download your updates, or click **Cancel** to continue.

2. Choose whether to Open the file, Save As to your hard drive, or Print. For information on printing, see *Printing Explorer reports*.

   Your PDF file should look similar to the following.



Risk Class [2003-10-10 >> 2003-10-10] 2005-09-13 18:32:18

Risk Class

Risk Class	Hits
Productivity Loss	9,762
Business Usage	7,270
Network Bandwidth Loss	1,752
Security Risk	18
Legal Liability	6
Total:	18,808

The default page size is Letter (8 1/2 X 11 inches in size), but can be modified in the `wse.ini` file settings. To modify the page size, see the *Reporting Administrator's Guide* or contact your Websense Administrator for help.

Printing Explorer reports

Print Explorer reports via the:

- Web browser print function by choosing **Print** from the File menu

- Output to Portable Document Format (PDF) option

Although Explorer reports have been set up to print more successfully than most Web pages, you may want to test printing to check the result. You will find that as you design your own report, the column widths differ according to the detailed information included in the report. The page defaults to A4 if the report is wider than the 8 1/2 X 11 inches Letter size. Page width is determined by:

- regular - portrait
- top N - portrait
- timeline - landscape

The content of the pages is either 7 1/2 inches or 10 inches wide. In the case of A4, the margins are slightly narrower but still within print range.

Column widths are specified in the `detail.xml` file and are associated with each dimension.

CHAPTER 4 Managing Log Server

Log Server is a separate service that reporting uses to receive Internet access information from Websense. Log Server saves this information to a log cache file (`logx.tmp`, where x is a number). Log cache files (also called log files) act as temporary storage for data accumulated by Log Server. Log Server stores information in a log file until the file reaches the specified capacity, or a certain amount of time has passed. After reaching either limit, Log Server saves the file and creates a new one. You can select a capacity and time interval on the Settings tab in the Log Server Configuration window.

Log Server will cache log records until CPU time becomes available. Log Server then reads the oldest log file and sends its information to the Log Database.

Log Server configuration

During installation of Log Server, establish settings that define how Log Server should interact with Websense Express and the Log Database. The Log Server Configuration window allows you to modify those settings.

IMPORTANT

After making changes on 1 or more of the Log Server Configuration tabs:

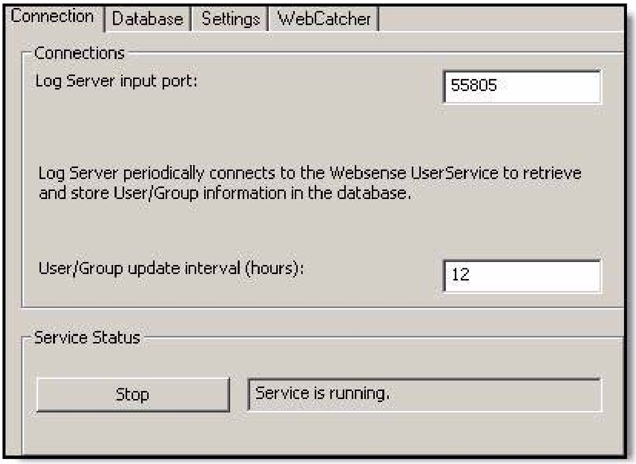
- Click **Apply**.
- Stop and restart Log Server for the changes to take effect.

1. Go to **Launch Log Server Config** in the **Actions** menu in Websense Manager. The Log Server Configuration window opens and contains tabs with options.
2. Select a tab to display its options and make any changes. See online Help for details about the settings in each tab.

3. Click **Apply** to save the changes.
4. Stop and restart Log Server for the changes to take effect.

Connection tab

The **Connection** tab contains options for creating and maintaining a connection between the Log Server and Websense.



Stopping and starting Log Server

Log Server receives information from Websense and saves it in the Log Database for use by Explorer.

Stop and restart Log Server any time you make changes through the **Connection** tab in the Log Server Configuration window.

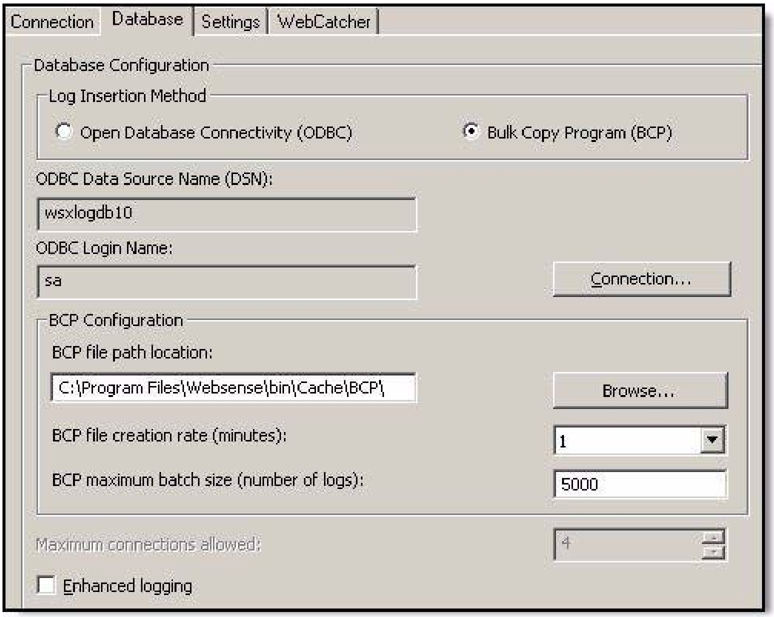
Log Server restarts each time you restart the machine, but you can also stop and start Log Server manually through the Connection tab in the Log Server Configuration window.

Note

Websense cannot log Internet access that occurs while Log Server is inactive.

Database tab

Open the **Database** tab to select a database engine and configure the Log Database.



Settings tab

On the **Settings** tab, use the Cache section to establish how often the Log Server should create a new `logx.tmp` file for saving information. The Log

Server creates a new log cache file when either the time limit is reached, or the size of the current log file reaches the size indicated on this tab.

WebCatcher tab

Use WebCatcher to analyze unrecognized URLs and Security URLs for categorization and the potential for security and liability risks. Storing full URLs is not necessary to use WebCatcher. Subsequent downloads of the Websense Master Database will include category revisions reflected in the improved filtering.

> **Note**
> Currently, intranet sites are not sent with WebCatcher. This includes all sites in the 10.xxx.xxx.xxx, 172.16.xxx.xxx, and 192.168.xxx.xxx ranges.

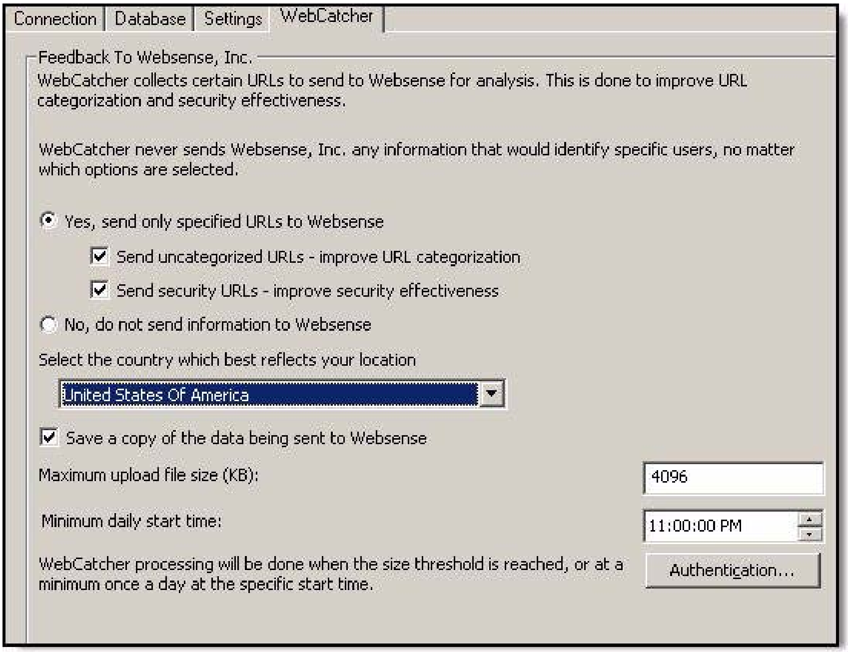
Note that the information sent to Websense, Inc., contains only URLs and does not reflect individual user information.

The following example illustrates the information that would be sent to Websense, Inc., if you activated 1 or both of the send options. The IP address in this entry reflects the address of the machine hosting the URL, not the requestor's IP address.

```
<URL HREF="http://www.ack.com/uncategorized/"
CATEGORY="153" IP_ADDR="200.102.53.105" NUM_HITS="1" />
```

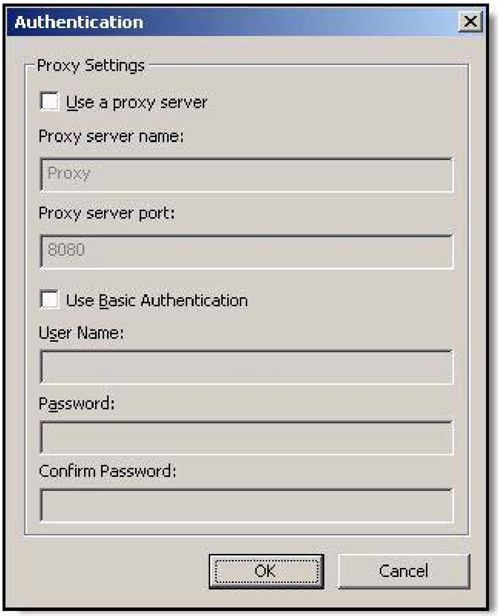
You may need to make changes on your proxy server or firewall to permit this information to be sent via HTTP post. For information on the types of changes that could be needed, see the documentation located at www.websense.com. Go to Support and Knowledge Base, and then navigate to Product Documentation.

WebCatcher runs when the maximum file size has been reached or at the daily start time.



Authentication dialog box

The Authentication dialog box appears after you click **Authentication** on the WebCatcher tab.

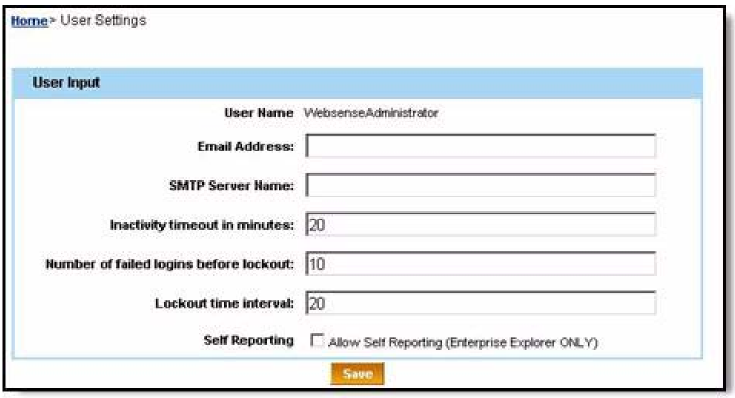


APPENDIX A User Settings

The administrator designates user settings in Settings on the Reporting Tools Portal, including the SMTP server (email server), to be used by users to email reports and job notifications.

> **Note**
> Make sure your email system administrator has set a large enough email size limit. Otherwise, some large reports may not be delivered properly via email.

1. Go to the **Reporting Tools** portal, and then click **User Settings**. The User Settings dialog box appears.



2. The **User Name** is displayed.
3. Enter the **Email Address** from which email notifications are to be sent.
4. Enter the **SMTP Server Name** that will be used to email reports and job notifications.
5. The **Inactivity timeout in minutes** field has a default time out of 20 minutes for an inactive session and can be edited as needed.

6. The **Number of failed logins before lockout** field has a default of 10 failed login attempts before an unauthorized user is locked out of the login screen and can be edited as needed.
7. The **Lockout time interval** field has been set to 20 minutes and can be edited as needed.
8. Check **Self Reporting** to allow users to self report in Websense Explorer.
9. Click **Save** to update the User Settings.

APPENDIX B

Administering the Database

All log records are stored in database partitions. Data older than 30 days will automatically be deleted.

The Database Administration tool allows you to:

- Refresh the Database Administration screen
- Configure Internet Browse Time and maintenance
- See error log activity

Accessing Database Administration

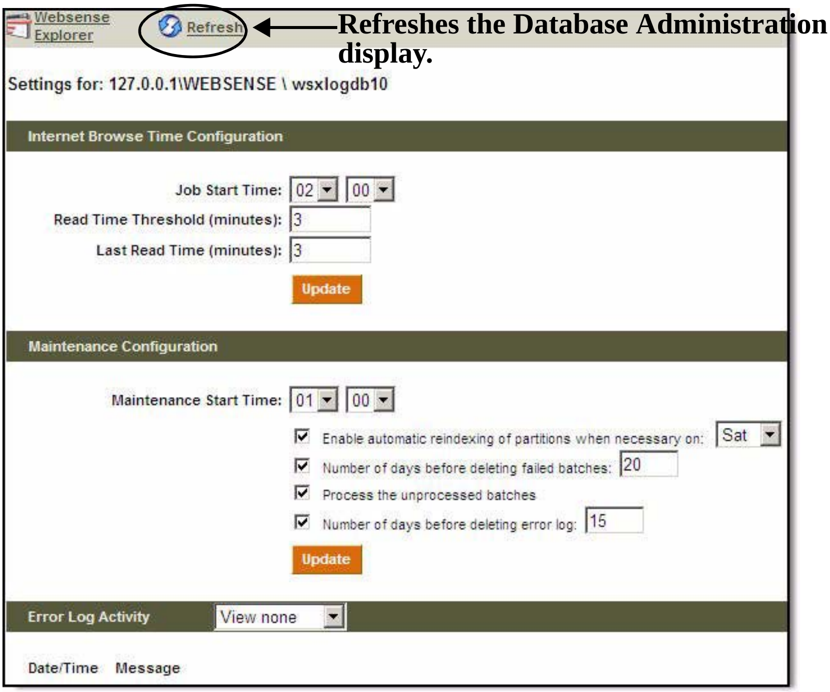
1. Go to the Reporting tools link in the **Current Status** tab in Websense Manager.
   - Access to the Reporting Tools Portal is based on the Reporting roles created in Websense Manager.
   - After roles have been defined in Websense Manager, enter your network User Name and Password to access the Reporting Tools Portal.

     The logon is validated through the directory service. If no directory service is available, you will have to use the default Administrator logon of **WebsenseAdministrator** and the password that was set up to access the Policy Server in Websense Manager.
2. Click **Database Administration**. The Database Administration tool appears with the name of the Log Database.

> **Note**
> Generally, only 1 person should have the responsibility for administering the database.

Database Administration tool

Detailed database administration options can be updated to suit your database and reporting needs. See online Help for details about configuration and maintenance settings.



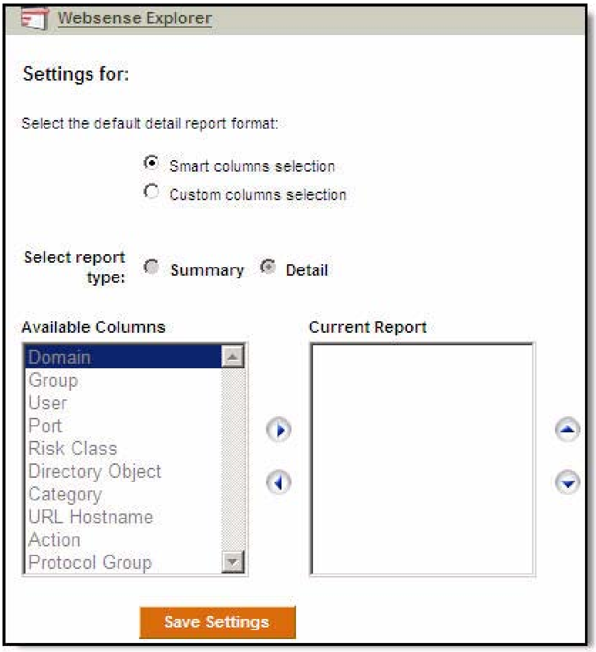
APPENDIX C

Explorer Settings, Display, and Print Options

- Modify Explorer Settings via the *Explorer Settings page*.
- Modify Explorer Display and Print options via the `wse.ini` file.

Explorer Settings page

You can edit Explorer settings by clicking the **Explorer Settings** link at the top of the Websense Explorer main page. The following Settings page is displayed.



1. When you have finished making your selections, click **Save Settings** to complete the changes.
2. Click **Websense Explorer** at the top left of the page to go back to the Explorer main page.

Changing configuration settings via the wse.ini file

Make adjustments to the way Explorer displays report choices and report results by making parameter changes to the `wse.ini` file. If you selected the default location during installation, this file is located at:

```
C:\Program Files\Websense\webroot\Explorer\wse.ini
```

The following table explains the parameter, what it controls, and the default value.

Default value	Parameter	What it controls
5000	maxUsersMenu	The database must have fewer users than this value to show User as a primary report choice at the top of Explorer's Main Page.
3000	maxGroupsMenu	The database must have fewer groups than this value to show Group as a primary report choice at the top of Explorer's Main Page. **Note:** You need more than 1 group for Group to show as a primary report choice. You need more than 1 domain for Domain to show as a primary report choice. There is no maximum value on the number of domains.
5000	maxUsersDrilldown	User displays in red during drill down, if there are more users than this number in the proposed report.
2000	maxGroupsDrilldown	Group displays in red during drill down, if there are more groups than this number in the proposed report.
10000	warnTooManyHits	If there are more users than the maxUsersDrilldown value, but fewer hits than this value, user will not display in red. If there are more users than the maxUsersDrilldown value and more hits than this value, user will display in red.

Default value	Parameter	What it controls
100	hitsPerPage	The number of items displayed per page will be no greater than this value.
4000000	maxOutputBufferSize	This is the limit (in bytes) on the total size of a page that can be displayed in Explorer's Main Page. When this limit is reached, a message stating that some results are not shown will display in gray.
10	timelineCompression Threshold	In the User Activity by Day or Month, when the Expand/Collapse button is available: This is the time threshold to collapse hits that occur within this time with the same base URL. For example, everything up to the third slash, Websense category, and action.
Letter	PageSize	Explorer report results can be output to Portable Document Format (PDF). The page size can be modified to A4 or Letter (8.5 X 11 inches).

Index

R

S