EXPLORER FOR LINUX ADMINISTRATOR'S GUIDE

Websense® Web Filtering
Websense Web Security

v7

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published March 13, 2008
Printed in the United States of America and Ireland

Trademarks

Contents

CHAPTER 1

About Websense Explorer for Linux

Websense®, Inc., produces software that manages employee use of the Internet. Websense Web Filter gives an organization the ability to control, or simply monitor, network traffic to the Internet. Websense Web Security offers all these features, plus added security features.

Websense Explorer for Linux provides the ability to gather and keep information about Internet usage. It receives incoming data about Internet usage from Websense Web Security and Websense Web Filter, and stores it in a database.

What is Websense Explorer?

Websense Explorer creates a database that contains information about how your employees are actually using the Internet, and enables you to take a look inside that database.

Explorer is an interactive, browser-based application that provides thousands of reports as well as statistical analysis. It is easy to use and displays results quickly. It reports on current Internet usage, and has the capability to report on archived data as well.

How Explorer works

The Explorer for Linux Log Server receives Internet activity from Websense Web Filter and Websense Web Security, and inserts the data into your MySQL database.

Explorer creates an Intranet Web site on an Apache Web server. Explorer users access this Web site to run Internet usage reports on a Log Database.

Websense Web Security or Websense Web Filter must be installed and working in your network before Explorer can be installed or used.

How Explorer for Linux works with filtering software

Understanding Explorer requires an understanding of how Websense filtering software works with Explorer for Linux. Following is a simplified overview..

Note

Websense Explorer for Linux does not collect data from or report on threat-based filtering by the Websense Security Gateway real-time scanning and categorization features.

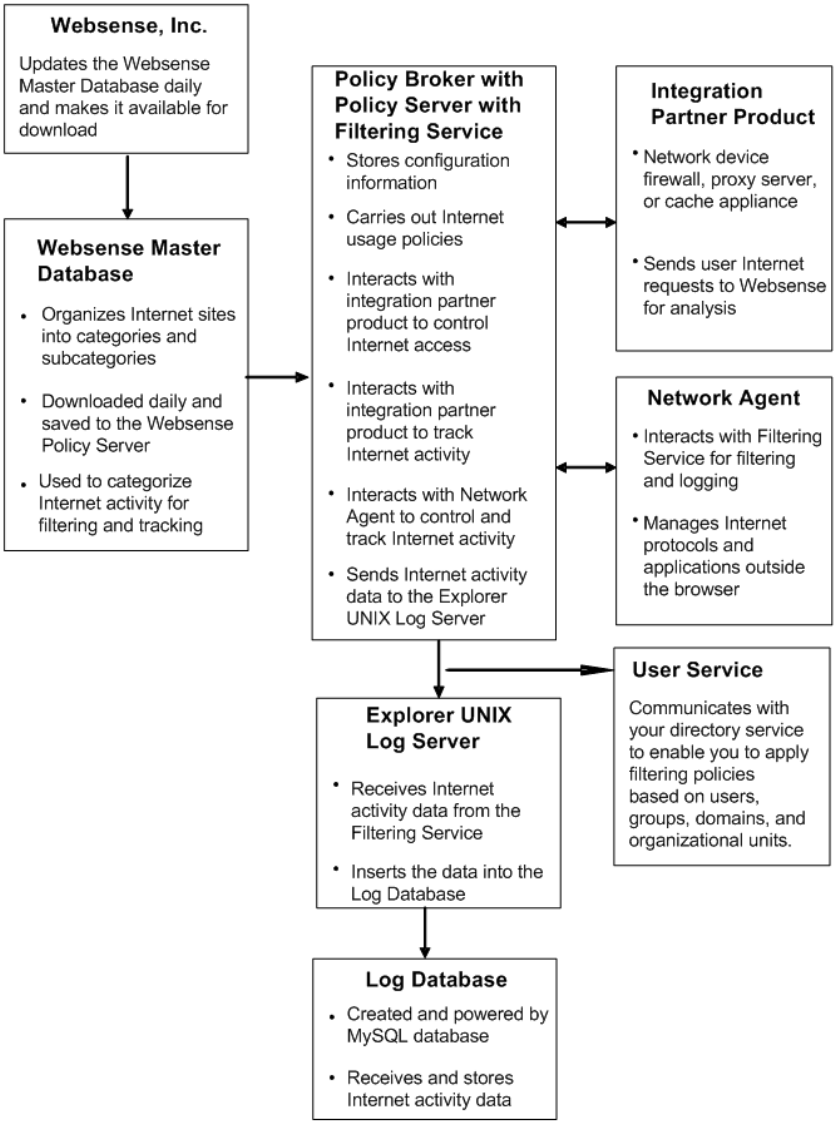
Components of Websense filtering software that affect Explorer include:

- Policy Broker
- Policy Server
- Filtering Service
- User Service
- Websense Master Database
- Integration partner product (firewall, proxy server or cache appliance)

Components of Explorer for Linux include:

- Explorer for Linux Log Server
- Log Database created by MySQL database
- Intranet Web site on an Apache Web server
- Microsoft® Internet Explorer Web browser

- Access to an existing MySQL Log Database



Policy Broker: Manages and stores information required by other Websense components to apply filtering policies.

Policy Server: Stores some Websense configuration information, and communicates with other Websense components.

User Service: Communicates with Directory Service to enable you to apply filtering policies based on users, groups, domains, and organizational units.

Filtering Service: Filtering Service also **i**nteracts with the firewall, proxy server or cache appliances (integration partner product) and Network Agent to implement Internet use policies and to track Internet activity. It sends activity data to the Explorer for Linux Log Server. (It does not send Log Server any data about threat-based filtering activities conducted by the Websense Security Gateway real-time scanning and categorization features.)

Websense Master Database: Organizes Internet sites (by IP addresses and their associated URLs) into one of approximately 90 major categories and subcategories. The updated version is downloaded daily from Websense, Inc., and saved to the Filtering Service machine. Filtering Service uses the Websense Master Database to categorize Internet activity for filtering and tracking.

Integration partner product: A network device that is either a firewall, proxy server or cache appliance. It sends users' Internet requests to the Websense server for analysis.

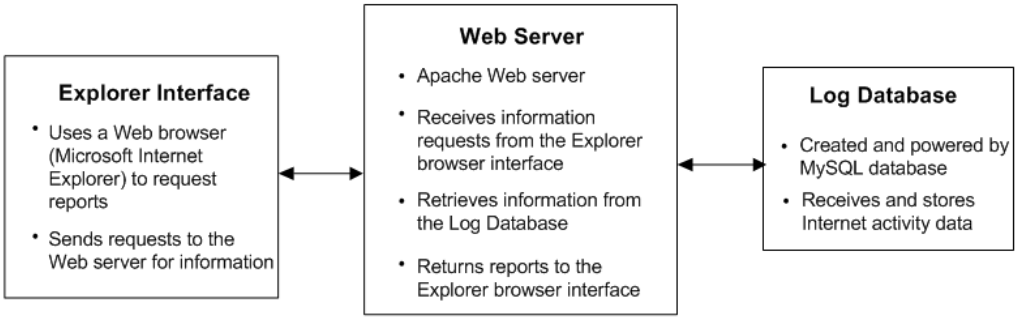
Network Agent: Manages Internet protocols and applications outside the Web browser. Depending on how it is configured for the organization, it can also filter and log Internet activity through the Web browser.

Explorer for Linux Log Server: Receives Internet activity data from Filtering Service and inserts the data into the Log Database.

Log Database: Created and powered by MySQL database. Log Database receives and stores Internet activity data.

How Explorer's Web server works

Explorer creates a Web server to access the Log Database. Microsoft Internet Explorer is used to view the Log Database via the Web server

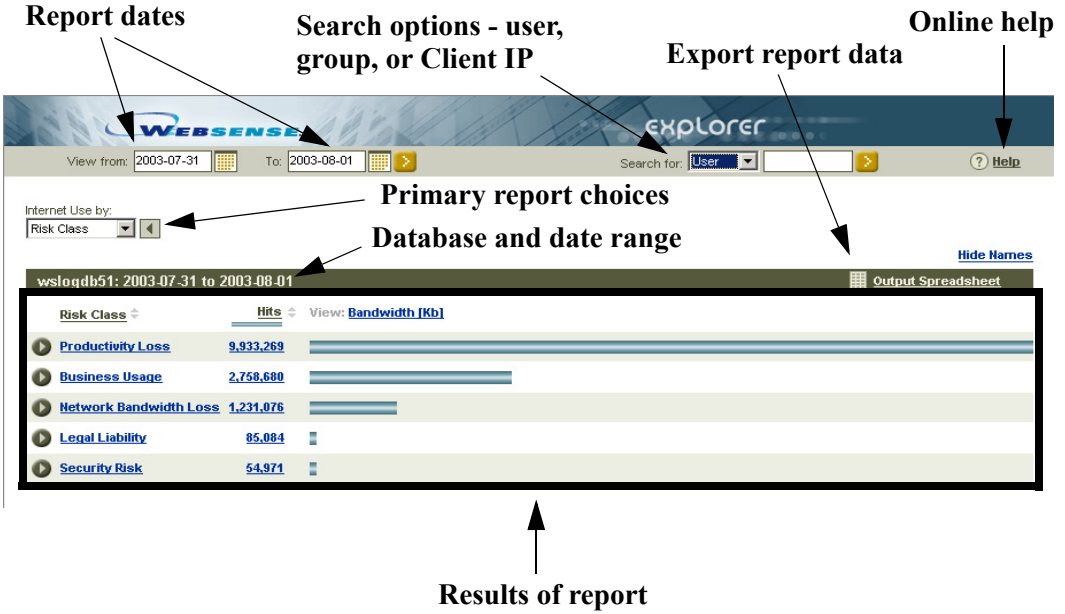


Explorer's Main Page

After Explorer has been installed and the Log Database contains data about Internet activity, use Explorer to view the Log Database from your Web browser.

For details of specific requirements and installation steps, see *Chapter 3: Launching Explorer*.

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. The following is a quick overview of Explorer's Main Page.



Primary report choices: Vary slightly, depending on whether there are multiple groups or domains in the database.

Groups: If there are no groups available, Group will not be available as a primary report choice or in the drop down options. If there is only one domain, Domain will not display as a primary report choice.

Report dates: Can be typed into the boxes or picked via a calendar.

Search for User, Group, or Client IP: Lets you quickly find Internet usage activity for a particular person, group or machine.

Help: Offers guidance on how to create the report you want.

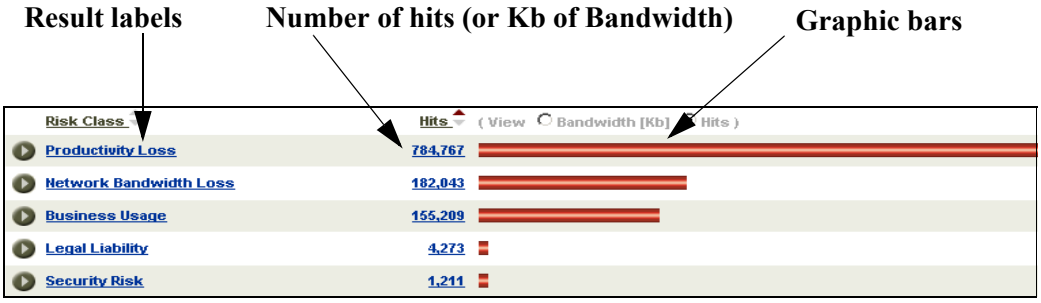
Hide Names: Allows you to show a report using only user IDs instead of user names. This button toggles back to **Show Names**.

Information about the database being viewed is displayed above the report results. Database information is the database name and the machine name

(where the database is located). The report dates are also displayed above the report results.

Click the **Output Spreadsheet** icon to export the report data to a Microsoft Excel file.

The results of the report in Explorer's Main Page are shown by result labels, number of Hits (or Kb of Bandwidth), and graphic bars.



When Explorer for Linux Log Server logs Visits, Explorer will display log information as Hits.

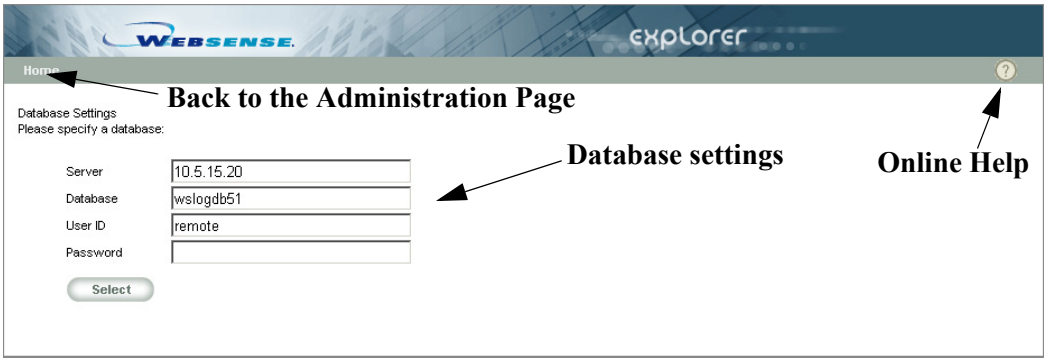
For further details on producing reports, see *Chapter 5: Explorer Reports*.

Explorer's Database Page

You can change the database that Explorer uses from Explorer's Database Page. Access this page from the Explorer Administration page.

For details on Explorer's Administration page, see *Chapter 3: Launching Explorer*.

The following is a quick overview of Explorer's Database Page.



From the Database Page, you can return to the Administration page by choosing **Home** in the upper left hand corner.

Help: Offers guidance on administrative tasks relating to the Explorer for Linux Log Server and changing the database.

Database Settings: Allow you to change the Log Database that Explorer is using to generate reports.

For more information on how to use the Explorer for Linux Log Server and how to change the database settings, see *Chapter 4: Explorer Administration*.

Online help

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

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

If corporate security standards permit, you can permanently disable the warning message in Internet Explorer. Go to **Tools > Internet Options > Advanced** tab **> Security**, and check **Allow active content to run in files on My Computer**.

Related documentation

For complete information on other components, see:

For information	See
Installation of Websense filtering software	Installation guide and integration-specific supplements, available at www.websense.com. Go to **Support**, and then navigate to Documentation:
Operation of Websense filtering software	Online help system within your Websense filtering software. The same information is available in PDF format at www.websense.com. Go to **Support**, and then navigate to Documentation.
Installation and operation of MySQL	MySQL documentation. http://www.mysql.com/documentation/index.html
Apache Web Server	Apache documentation. http://www.apache.org/

For further details on producing reports, see *Chapter 5: Explorer Reports*.

CHAPTER 2 | Installing Explorer

Before Websense Explorer for Linux is installed, Websense filtering software and MySQL must be installed and working.

Explorer adds an Apache Web server to an existing Websense filtering installation. The Web server connects to the Log Database running on MySQL.

Users use a standard Web browser to make report choices and view report results.

System requirements

Explorer runs over HTTPS.

The Web server portion can be installed on any machine that can connect to the Log Database on MySQL.

For system requirements, see the Websense *Deployment Guide*.

Installing MySQL

The instructions in this section are intended to assist in installing MySQL before installing Websense Explorer for Linux. For the most complete, accurate and up-to-date instructions, please see the MySQL documentation at:

http://www.mysql.com/documentation/index.html

MySQL and Explorer on the same machine

1. Download MySQL binaries from the following site:
   Version 5.0

http://dev.mysql.com/downloads/mysql/5.0.html

> **Note**
> Download the appropriate binaries for your operating system. Websense recommends that you use the standard, 32-bit version.

2. Run the following commands, replacing `mysql-binaries.tar.gz` with the filename of your binary download, and <password> with your root password:

```
groupadd mysql
useradd -g mysql mysql
cd /usr/local
gunzip < /path/to/mysql-binaries.tar.gz | tar xvf -
ln -s /full/path/to/mysql-binaries mysql
cd mysql
scripts/mysql_install_db
chown -R root  .
chown -R mysql data
chgrp -R mysql .
bin/mysqld_safe --user=mysql &
bin/mysqladmin –u root password <password>
```

3. Test whether everything has been set up correctly by running the following command, entering the password you set when previously prompted:

```
mysql –u root –p mysql
```

   If you receive a **mysql>** prompt after entering the password, then everything appears to be working.

4. Install Explorer, using the user name root and the password that you set previously.

MySQL and Explorer on different machines

1. Download MySQL binaries from the following site:

Version 5.0

http://dev.mysql.com/downloads/mysql/5.0.html

> **Note**
> Download the appropriate binaries for your operating system. Websense recommends that you use the standard, 32-bit version.

2. Run the following commands, replacing `mysql-binaries.tar.gz` with the filename of your binary download, and <password> with your root password:

```
groupadd mysql
useradd -g mysql mysql
cd /usr/local
gunzip < /path/to/mysql-binaries.tar.gz | tar xvf -
ln -s /full/path/to/mysql-binaries mysql
cd mysql
scripts/mysql_install_db
chown -R root  .
chown -R mysql data
chgrp -R mysql .
bin/mysqld_safe --user=mysql &
bin/mysqladmin –u root password <password>
```

3. Test whether everything has been set up correctly by running the following command, entering the password you set when previously prompted:

```
mysql –u root –p mysql
```

If you receive a **mysql>** prompt after entering the password, then everything appears to be working.

4. At the MySQL prompt, enter the following command, being sure to replace <ip> with the IP address of the server that Explorer will be installed on and <password> with the password you would like to use:

```
GRANT ALL PRIVILEGES ON *.* to root@<ip> IDENTIFIED by
'<password>' with GRANT OPTION;
```

5. Run the following command, entering your password when prompted:

   ```
   mysqladmin -u root -p reload
   ```

6. Install Explorer, using the user name root and the password that you set previously.

Installing Websense Explorer for Linux

The Websense Explorer for Linux installation package is self-extracting. It will:

- Install an Apache Web server
- Delete the current Log Database (if applicable)
- Create a Log database in MySQL (`wslogdb70`)

  For information on creating a new database, go to the Explorer Administration tasks and see *Creating a new database*, page 28.
- Install the Explorer for Linux Log Server

  - In Linux the default installation location is:

    `/usr/local/websense/UNIXExplorer`
  - In Solaris, the default installation is:

    `/opt/websense/UNIXExplorer`
  - The default location for the binary wrapper scripts is:

    `UNIXExplorer/bin`

What you need to know

To complete the installation, you need to know the following:

- The path to the MySQL binaries.
- MySQL user name.
- MySQL password.
- Websense Policy Server address.
- IP address (preferred) or name of machine running MySQL.
- If you choose short logging, short logging only writes the hostname of the URL to the database. This decreases the size of the database and slightly

increases logging performance, at the expense of losing the full URL path information.

- You do not need to install Websense Explorer and the Explorer for Linux Log Server on the same machine; you can install them on separate machines. Websense Log Server does not need Websense Explorer functionality to log data.
- Choose Visits or Hits logging - Visits logging is a compression (roll-up) mode that reduces the number of log records written to the database by aggregating accesses within a Web page from the same user. In this mode, fully granular access information is not saved, but it can be significantly faster in a large environment.
- Whether you choose to use WebCatcher - This cron procedure allows you to send all uncategorized sites found in the logs to Websense for classification, so they can be analyzed for inclusion in an upcoming Websense URL database.
- Information to complete the OpenSSL Certificate - country code, state/province, city, company name, group, and email address.
- Whether you choose to use the default HTTPS server port of 443.
- If Explorer should launch when the machine starts up.
- Websense recommends that you run logserverd as nobody.

Setting user name and password for roles

Explorer supports three roles when running on Apache: Administrator, HR User, and Restricted User.

- An Administrator can make changes to the database settings, and may run any report.
- An HR User can run any report, but does not have access to the database settings.
- A Restricted User can run reports, only with user IDs instead of user names (and has no access to the database settings).

More than one person may assume each role, and the user name and password for a role applies to that role, not a specific user.

During installation you are required to provide a password for each of the roles.

After installation

After installation, you can launch Explorer from Explorer's Administration page. For details on Explorer's Administration page, see *Chapter 3: Launching Explorer*.

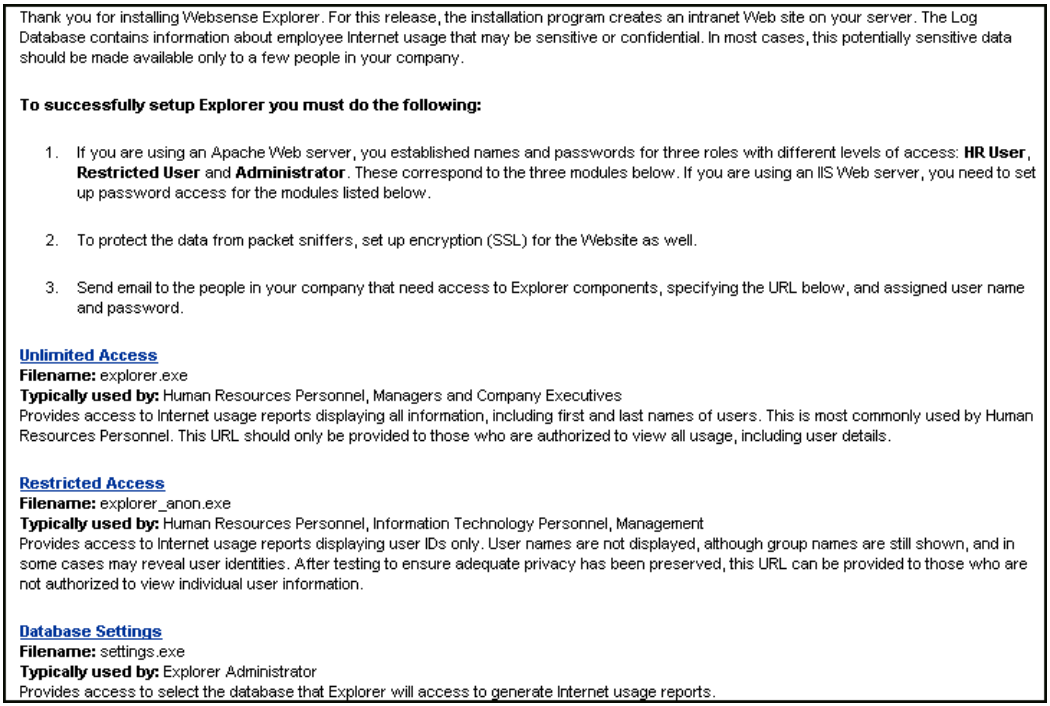
CHAPTER 3 | Launching Explorer

The Explorer Administration page allows access to Websense Explorer for Linux. The Administration page opens in your Web browser.

To access the Explorer Administration page, type in the address:

```
https://<machine name or IP address where the Explorer
Web server has been installed>
```

The Administration page appears. It provides links to executable files for the different levels of access.



Thank you for installing Websense Explorer. For this release, the installation program creates an intranet Web site on your server. The Log Database contains information about employee Internet usage that may be sensitive or confidential. In most cases, this potentially sensitive data should be made available only to a few people in your company.

To successfully setup Explorer you must do the following:

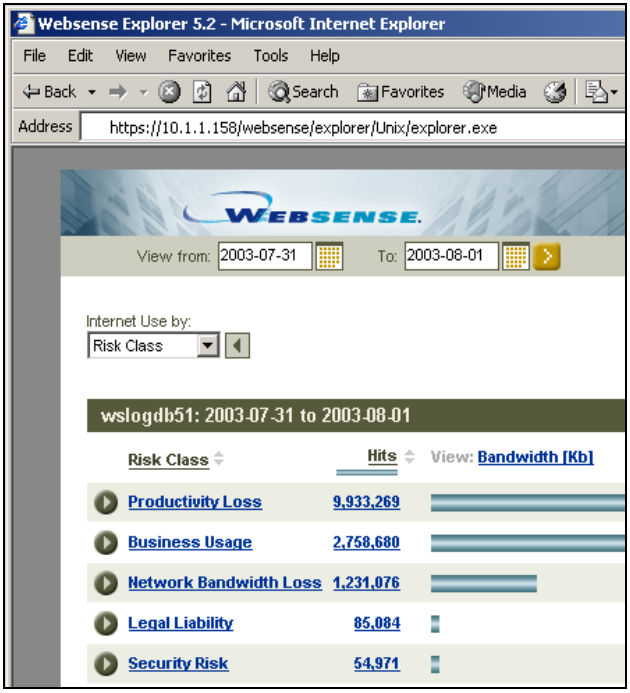
1. If you are using an Apache Web server, you established names and passwords for three roles with different levels of access: **HR User**, **Restricted User** and **Administrator**. These correspond to the three modules below. If you are using an IIS Web server, you need to set up password access for the modules listed below.
2. To protect the data from packet sniffers, set up encryption (SSL) for the Website as well.
3. Send email to the people in your company that need access to Explorer components, specifying the URL below, and assigned user name and password.

Unlimited Access
Filename: explorer.exe
Typically used by: Human Resources Personnel, Managers and Company Executives
Provides access to Internet usage reports displaying all information, including first and last names of users. This is most commonly used by Human Resources Personnel. This URL should only be provided to those who are authorized to view all usage, including user details.

Restricted Access
Filename: explorer_anon.exe
Typically used by: Human Resources Personnel, Information Technology Personnel, Management
Provides access to Internet usage reports displaying user IDs only. User names are not displayed, although group names are still shown, and in some cases may reveal user identities. After testing to ensure adequate privacy has been preserved, this URL can be provided to those who are not authorized to view individual user information.

Database Settings
Filename: settings.exe
Typically used by: Explorer Administrator
Provides access to select the database that Explorer will access to generate Internet usage reports.

To test the Explorer installation, click **Unlimited Access**, and then enter a user name and password. You should see a report similar to the following:



If you cannot get an opening report similar to this from Explorer's Administration page, see *Appendix A: Maintenance and Troubleshooting*.

Levels of access

There are 3 links from Explorer's Administration page, which provide different levels of access to Explorer.

- **Unlimited**: Provides access to Internet usage reports displaying all information, including first and last names of users. This is most commonly used by Human Resources personnel.
- **Restricted**: Provides access to Internet usage reports displaying user IDs only. User names are not displayed, although group names are still shown and in some cases could reveal user identities. Testing should be done to ensure adequate privacy has been preserved by anonymizing users.

A way to test for privacy is to run several different reports with this type of access, and consider the following:

- Are there groups or domains with only one user?
- Does the group name or domain name identify such a small group that a reasonable guess can be made as to individual users?
- Do some of the full URLs include user names?

- **Database Settings**: Provides a way to select the Log Database that Explorer will use to generate reports. Also allows access to perform diagnostics on the Log Database. This should only be used by the Explorer Administrator.

Each of the links from Explorer's Administration page results in viewing a different URL in your Web browser.

Here is an example of a URL providing unlimited access.

```
https:localhost/websense/explorer/UNIX/explorer.exe
```

When providing the link to others, replace localhost with the IP address of the machine where the Explorer Web server is installed.

Provide the user ID, password, and URL to allow the appropriate level of access to authorized individuals.

Security

By installing Explorer, you have created an Intranet Web site to access a Log Database.

The Log Database contains potentially sensitive information about employee Internet use. In most cases, this information should only be available to a few people in your company.

CHAPTER 4 | Explorer Administration

Websense Explorer administrative tasks include

- *Using Explorer for Linux Log Server*
- *Creating a new database*
- *Setting up Auto-Archive*
- *Changing the database*
- *Changing the configuration settings via the .INI file*

Using Explorer for Linux Log Server

Use the following options to control the Linux Log Server.

- *Linux Log Server database management tools main menu*
- *logserverd*
- *logserverdctl*

Linux Log Server database management tools main menu

Usage: /UNIXExplorer/bin/logserverd-dbtools

1. **Database Archive**: Save the current database and create a new one for logging.
2. **Database Auto-Archive Setup**: Save the current database when it reaches a certain size or a certain time and create a new one for logging.
3. **Database Purge**: Delete some portion of the current database.
4. **Database Information**: Version information.
5. **Create a New Database**
6. **Uninstall**
7. **Help**
8. **Quit**

logserverd

Usage: /UNIXExplorer/bin/logserverd [options...]

Performance tuning

Parameter		Value
tune-db-pool-size	PIII / Sparc II	Leave as is
	P4 / Xeon / Sparc III	Set to **10** **Note:** Increase this number only if commit files are building up and there is still reasonable idle CPUI.

Service control

-se	-edit	Edit and reload local default config file
-sk	-killclient	Kill specific client
-sl	-logswitch	Switch (rollover) logfile now
-sm	-monitor	Ala -status, but poll every second
-sr	-rehash	Rehash/reload config file
-s	-service	Service host[:port] (default localhost)
-ss	-status	Service status

Main options

-cf	-config	Use alternate config file
-d	-debug	Debug mode
-dc	-diag-cdump	Category description table (diag)

-df	-diag-fdump	Record field description table (diag)
-ds	-diag-sdump	Status description table (diag)
-h	-help	This help
	-log-dsn	ODBC data source name
-lF	-log-fields	Record fields to show (default all)
-lf	-log-file	Output log file
-ld	-log-file-disable	No file logging with database logging
-lR	-log-filter	Regex filter for log fields
-lm	-log-maxsize	Max logfile size (bytes), triggers auto-logswitch
-lD	-logswitch-dir	Logswitch destination directory
-lp	-logswitch-in-place	Auto logswitch log over itself
-p	-port	Use alternate listen port
-tp	-tune-db-pool-size	Size of database write pool (tune)
-v	-version	Program version
-wm	-wbsn-master	Set Websense Version X.X Update Version Variable policy server master

logserverdctl

Used to start, stop, kill, and get status of the Explorer for Linux Log Server.

Usage: logserverdctl [start|stop|kill|status|server-log|monitor]

start	-start logger (with defaults)
stop	-stop logger gracefully
kill	-kill logger forcefully (use if stop doesn't work)
status	-status (pid) of running logger

server-log	-monitor server log /usr/local/websense/tools/logserverd/logs/server.log
monitor	statistics monitor

Creating a new database

To minimize the loss of data and run reports in a timely manner, create a new Log Database (rather than archive). You can quickly create a new Log Database without stopping the Explorer for Linux Log Server. Once the new Log Database is created, you can:

- Change the Explorer for Linux Log Server to log to the newly-created Log Database during a period of low activity.
- Run reports against the old Log Database or the new Log Database.

This minimizes the potential loss of data.

Changing the Directory Service settings in Websense Manager may cause duplicate user entries in Websense Explorer. Avoid this problem by creating a new database before updating the Directory Service settings.

This process is automated to allow you to follow the on-screen prompts while stepping through the procedure. In this example, we will create a new Log Database, **test21**.

1. Go to the `Logserverd-dbtools` utility in the following directory.

   /usr/local/websense/UNIXExplorer/utils

2. The Explorer for Linux Log Server Tools Main Menu appears.

```
Websense Log Server Tools Main Menu
-----------------------------------------------------
1. Database Archive
2. Database Auto-Archive Setup
3. Database Purge
4. Database Information
5. Create New Database
6. Check Database Version
7. Help
```

3. Enter **5** to run the Create New Database program.
4. Enter the name of the new database. For this example, enter **test21**. If the information cannot be obtained, a message displays, stating that the database could not pull the information from the logserverd-dbsetup and that you should enter the information manually.

   Enter the correct information for:

   - Location of the local host for MySQL Server
   - MySQL User name
   - MySQL Password

   A message displays, asking you to verify that this information is correct for these settings.

```
Server:    localhost

User:      root

Database: test21
```

5. Enter **Y** (yes) to confirm that the information you entered for these settings is correct.

   A message displays, stating that you have successfully created the new database.

6. The process creates the necessary Domain Service Name (DSN) connection and updates the `logserverd.conf` file with the new DSN information. Users can log to the new database simply by restarting the Log Server, because the process assumes the Log Server will be writing to the new database.

> **Note**
> Use the logserverd-dbsetup utility to point the Log Server to write to a different database.

```
Now creating DSN for database test21 and setting LogServerd to log to it.

Websense Logserverd 5.x DBSetup (Build 43-20050201-Tritium)

Platform    :i686-pc-linux-release

Build Date: Tue Feb 1 13:35:30 PST 2006
```

7. You are prompted to edit the default configuration Logging settings:
   - **Enable short logging?**: Answer **Y** (yes) to write only the hostname of the URL to the database and decrease the size of the database while slightly increasing logging performance. (Does not log the full URL path.) The default is no.
   - **Enable visits logging?**: Answer **Y** (yes) for a compression (roll-up) mode that reduces the number of log records written to the database by aggregating accesses within a Web page from the same user. The default is yes.

These options can be customized and updated any time to meet reporting needs.

```
Editing default configuration...

Logging Features

Short Logging
   Short logging writes only the hostname of the URL to the
   database. This decreases the size of the database and
   slightly increases logging performance, at the expense of
   full url path information.
Enable short logging [y/n]? [n]:

Visits Logging
   Visits logging is a compression (roll-up) mode that
   reduces the number of log records written to the database
   by aggregating accesses within a web page from the same
   user. In this mode, fully granular access information is
```

8. When the configuration is complete, the files are populated with default category information, risk class mapping, protocols, and dispositions.

```
Using defaults in /usr/local/websense/UnixExplorer/logserverd/etc/logserverd.conf
Using dsn 'DSN=test21' as default
Connected to Websense server at 10.201.1.219 (NTX/WNA/5.5.0)
Populated categories (100)
Populated dispositions (26)
Populated protocols (48)
Populated keywords (0)
Populated value classes (5)
Populated filetypes (60)
Schema init done. 6 sections(s) populated.
```

9. If you are using MySQL 5.0, change the password of the user with access to the Log Server database, so that it is compatible with older MySQL clients.

10. Restart the Log Server with the following command:

    `[UNIXExpDir]/bin/logserverdctl restart`

    Where `[UNIXExpDir]` is the directory in which you installed Websense Explorer for Linux, typically /usr/local/websense/UNIXExplorer.

Setting up Auto-Archive

Set up Auto-Archive so that the Websense Log Database can roll over automatically on a regular basis. The rollover of the old database occurs when the Log Database reaches a predetermined size or on the first of each month. A new database is created and the Log Server begins to write information to the new database.

When the unattended archive session takes over, it does the following:

- Gets connection information from the Log Server, thus validating the Log Server installation.
- Looks at the Auto-Archive parameter passed (either size or monthly).
  - If the current database is less than the parameter, the job exits.
  - If the current database meets the parameter setting (either the predetermined size setting has been met or one month has passed), it goes on to create a new Log Database.
- Writes information from the Log Server to the new Log Database.
- Updates Explorer settings to reflect the new Log Database.

  This process is automated to allow you to follow the on-screen prompts while stepping through the procedure.
  - If for some reason the cron job cannot get the Log Server information (cannot pull information from logserverd-dbsetup) or if permissions are insufficient, an email is sent to the root user stating that there has been no valid logserverd installation found and that it is terminating. The automatic archiving process stops.
  - Verify cron job is running as root, in case it cannot get the information for some other reason, such as insufficient permissions.

To configure Auto-Archive:

1. Log on as root user.
2. Go to the `logserverd-dbtools` utility in the following directory.

```
/usr/local/websense/UNIXExplorer/bin
```

The Websense Log Server Tools Main Menu appears.

```
Websense Log Server Tools Main Menu
-----------------------------------------------------------
1. Database Archive
2. Database Auto-Archive Setup
3. Database Purge
4. Database Information
5. Create New Database
6. Check Database Version
7. Help
```

3. Enter **2** to run the Database Auto-Archive Setup program. The following menu appears.

```
Websense Log Server Auto-Archiving Setup
-----------------------------------------------------------
1. Archive monthly
2. Archive based on size
```

4. The Database Auto-Archive Setup menu options are:

Menu Option	Description
1. Archive monthly	Selecting this option displays a prompt asking if you want to schedule an archive to be run at 12:15 am local time on the first of each month. Select: N = No. Exits this option and returns to the menu. Y = Yes. Confirms the auto-archive should be run at the specified time each month.
2. Archive based on size	Selecting this option schedules an archive to be run nightly whenever your Websense Log Database exceeds a given size. N = No. Exits this option and returns to the menu. Y = Yes. Confirms the auto-archive should be run nightly when the Websense Log Database exceeds the given size. When prompted, enter the number of gigabytes, in whole numbers, that represents the maximum size when the auto-archive should occur. For example, for auto-archive to occur when the database grows to 4 GB, enter 4. When the Log Database exceeds 4 GB, the auto-archive will begin that evening. Enter a whole number only (for example, do not enter 4.5. Instead, enter 4). This number must be greater than zero and less than 1000 (which is equal to 1 TB).
3. Return to main menu	Selecting this option returns you to the Websense Log Server Tools Main Menu.

5. Enter **crontab -l** to list and verify the new setup.
6. Database Auto-Archive unattended will take over, so there must be a connection to the current Log Server. If for some reason the Auto-Archive cannot get the Log Server information (cannot pull information from logserverd-dbsetup) or if permissions are insufficient, an email is sent to the root user stating that no valid logserverd installation was found, and that it is terminating. The automatic archiving process stops.

Changing the database

During Explorer installation, the database was created in MySQL.

You can change the database that Explorer uses to run reports.

1. Open the Explorer Administration page by typing in the address in your Web browser:

   ```
   https://<machine name or IP address where the Explorer
   Web server has been installed>
   ```

2. Click **Database Settings** to access the Database Page.
3. Make the appropriate choices to connect to the database where you would like to run Explorer reports.

Server	Enter the machine name (or IP address) where the Log Database is stored.
Database	Enter the name of the Log Database.
User ID	Enter User ID to make changes to the database.
Password	Enter the password to access the database.

4. Click **Select** to complete the database connection change.
   - If you have entered valid information, you will receive a confirmation message.
   - If you have entered invalid information, you will receive an error message.

   Make sure you entered a valid user ID and password and the correct machine and database names. You may also check for a typing error.
5. Click **Home** at the top left corner of the Database Page to go back to the Administration page to begin viewing Explorer reports on the newly-connected database.

Changing the configuration settings via the .INI file

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

`/usr/local/websense/UNIXExplorer/apache2/htdocs/websense/explorer`

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

Parameter	Default value	What it controls
maxUsersMenu	5000	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.
maxGroupsMenu	3000	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:** There must be more than one group for Group to show as a primary report choice. There must be more than one domain for Domain to show as a primary report choice. There is no maximum value on the number of domains.
maxUsersDrilldown	5000	User displays in red during drill down if there are more users than this number in the proposed report.
maxGroupsDrilldown	2000	Group displays in red during drill down, if there are more groups than this number in the proposed report.
warnTooManyHits	10000	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.
maxHitsGroup	3000	If there are more hits than this value, they will not be grouped by URL. Instead, they will be shown in time sequence.

Parameter	Default value	What it controls
maxHitsList	30000	If there are more hits than this value, they will not be grouped by URL or shown by time sequence. Instead, the hits will be displayed in random order. The number of hits displayed per page will be no greater than the value of hitsPerPage.
maxHitsGroupOverride	1000000	If there are more hits than maxHitsGroup, you can try to override the constraint against requesting a report grouped by URL. If there are more hits than this value, you will not be able to override the constraint.
hitsPerPage	100	The number of items displayed per page will be no greater than this value.
maxOutputBufferSize	4000000	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, the message "some results not shown" will display in gray.

System configuration files

The following configuration files store system information.

- **`odbc.ini` file**: Stores DSN information (database connection)
- **`logserverd.conf`**: Stores the configuration information for the Explorer for Linux Log Server, along with the IP address of the Policy Server

CHAPTER 5 | Explorer Reports

Websense Explorer offers the following main types of reports on Internet usage:

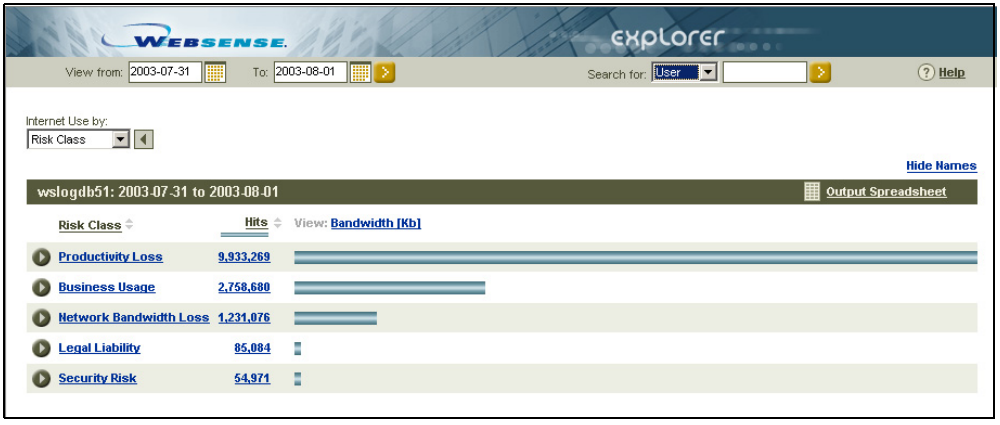
- *Hits (or Bandwidth) Summary table*
- *Lists grouped by URL*

All Explorer reports will be based on the employee Internet activity information contained in the Log Database that Explorer is currently viewing.

For details on how to connect Explorer to a different database, see *Explorer Administration*, page 25.

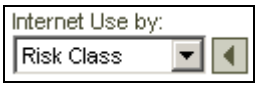
Hits (or Bandwidth) Summary table

When Explorer's Main Page opens, a report is run based on usage by risk class, for all users and for all available dates in the database.



At the top of the report, the chosen date range is displayed for the current report.

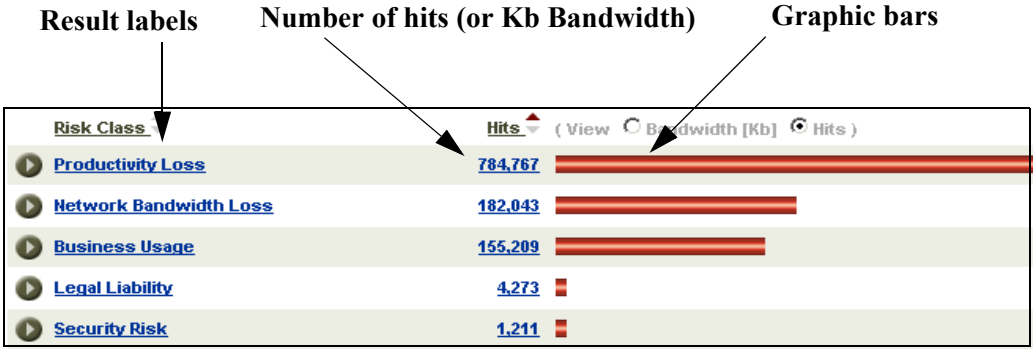
You can see that the primary report choice is Risk Class.



You can also see the following:

- the name of the database
- date range chosen for the report
- table headings for the report results
- whether Hits or Bandwidth has been chosen for the view

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



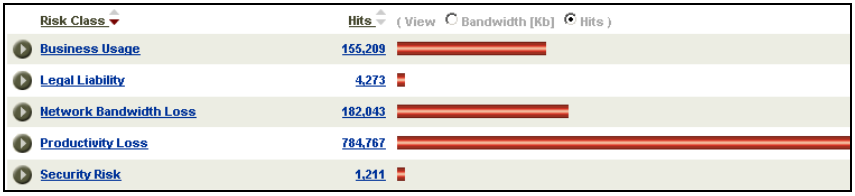
The result labels identify the name of the risk class in that row.

The number of hits displays how many hits or visits were made in that risk class (or how much Bandwidth was used by that activity).

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

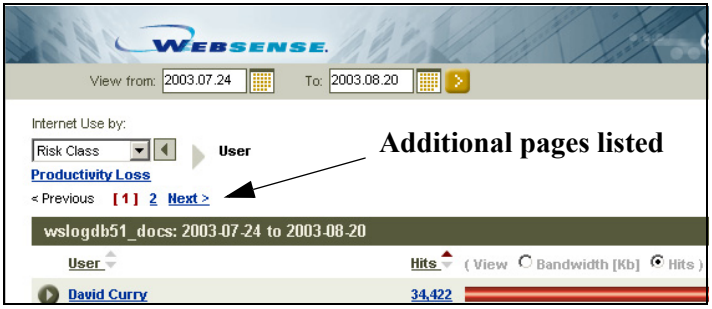
The order of the rows in the table is generally based on highest amount of activity to the lowest.

You can reorder the rows alphabetically ascending or descending by choosing **Risk Class** at the top of the rows.

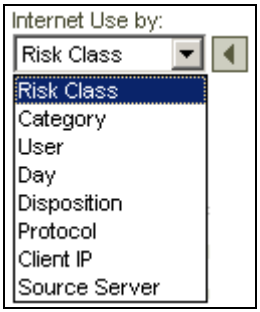


You can also reorder the rows by value ascending or descending, by choosing Hits or Bandwidth at the top of the rows.

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 will extend over additional pages, so you can view additional pages by choosing the page number at the top of the report.



Primary report choices



To display the primary report choices, display the drop-down list under **Internet Use by**.

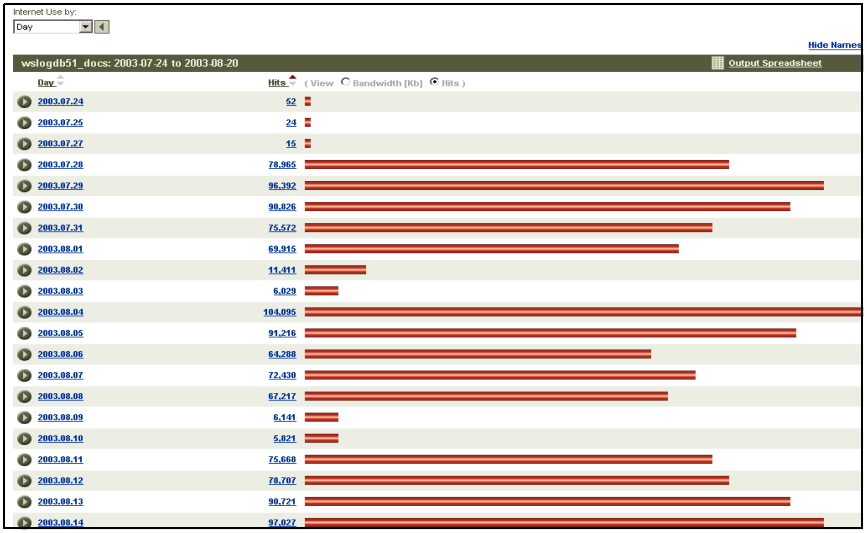
These choices will vary, depending on the database and Explorer's configuration settings.

- 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 is only one Domain, **Domain** will not display as a primary report choice.

For details on running user and group reports by drilling down into report results, see *Primary report choices*, page 42.

Every Hits (or Bandwidth) Summary Table report starts with a primary report choice.

Select **Day** from the **Internet Use by** drop down list to see a report by day, for all users and for all available dates in the database.



For the other primary report choices, the original order of the rows in the table is based on highest amount of activity to the lowest. For Day, the order of the rows is based on date order, with the oldest date on the first row. You can

reorder the rows by the highest activity by choosing Hits (or Bandwidth) at the top of the rows.

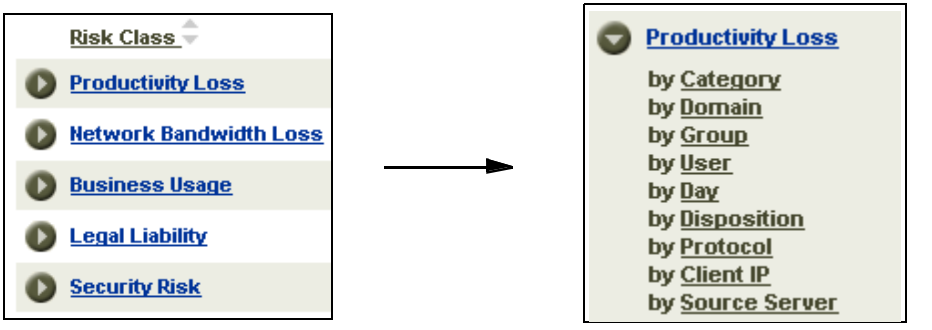
Drill down into results

Use the following procedure to drill down into the data you want to see.

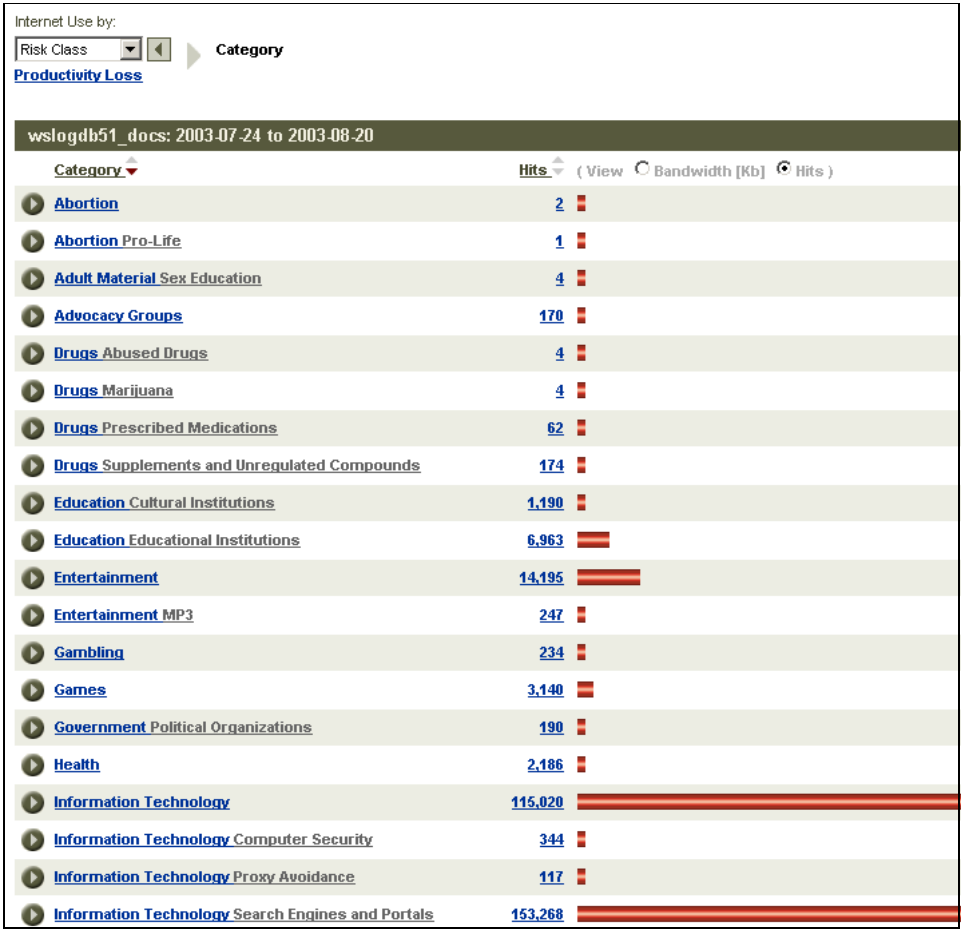
1. To obtain specific information about the data in a row, select > (drill-down arrow to the left of the row).

2. For example, to get more information about Productivity Loss, click > (drill-down arrow) to the left of **Productivity Loss**.

   Detail about the usage in this risk class is available from the drop-down list.

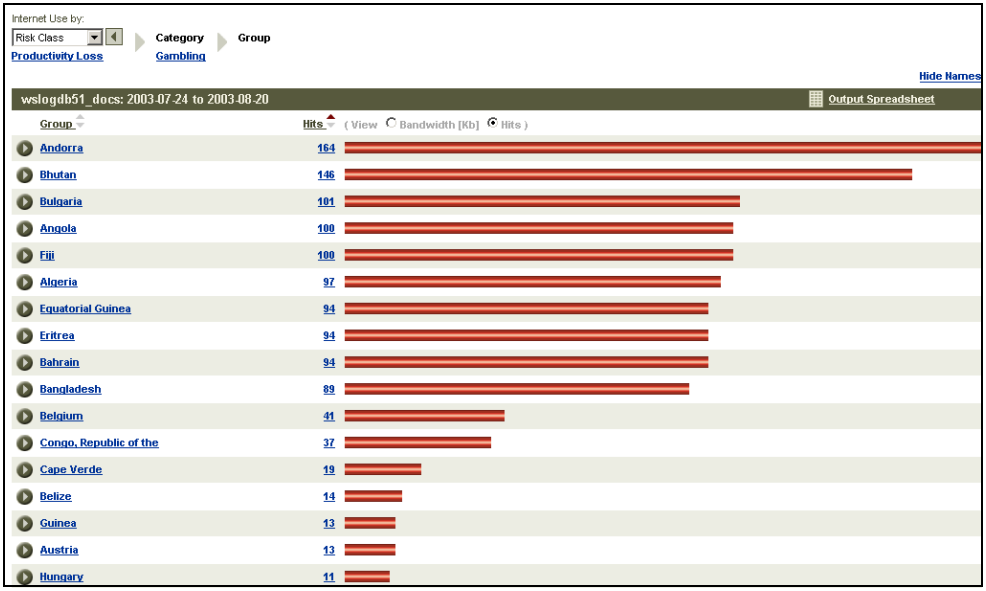


3. In this example, to see what categories have Internet activity considered to be a risk of Productivity Loss, select **by Category**.



4. For more detail about usage in the gambling category, click > (drill-down arrow) to the left of Gambling.

5. To see which groups have Internet activity in the Gambling category, select **Group**.



6. To see which users in a group have Internet activity in the Gambling category, select **User** in the drop-down list under that Group.

Changing report dates

You can see the date range available in the database by moving the mouse slowly over the calendar icons, or by clicking on a calendar icon.

1. Limit the report by changing the date range.

   Enter the new start or end date in the window by typing over the previous date, or select the dates from the date calendar. 

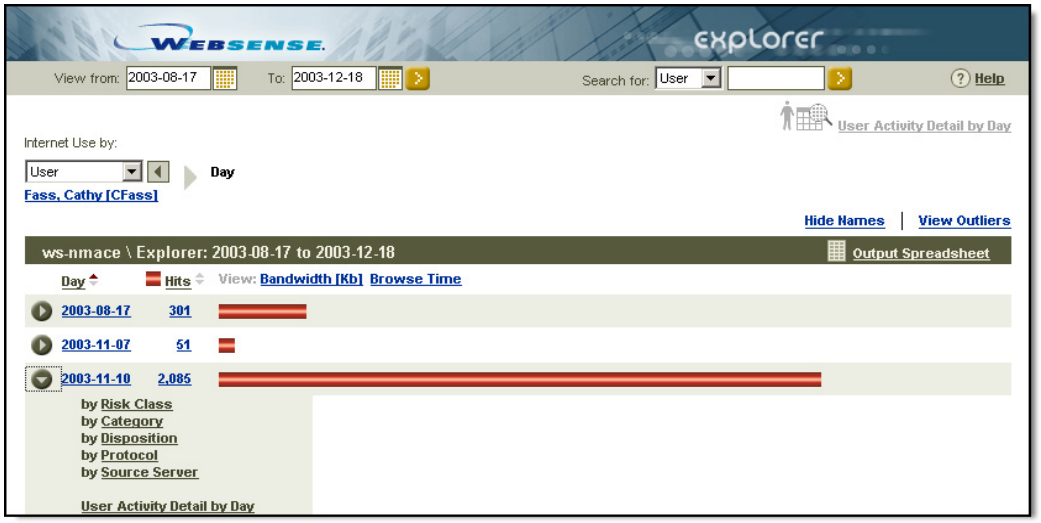
   Navigate inside the calendar to select year and month for the start or end date of the report.
2. Select the correct day for the Start or End date, and then click **x** in the upper right hand corner to close the calendar window. If you select dates that are outside the available range, they are corrected to available dates when you click > (**Go** arrow). You also get a message, notifying you that the date was reset.
3. When you have adjusted both the start and end dates, click > (**Go** arrow) to produce the new report. 

Timeline/Calendar View

This report shows activity for only one user at a time. If you have drilled down into other areas (such as category, risk class, or disposition), the Timeline and Calendar View only reflects the date and user.

- To get to the Timeline and Calendar View option:
  1. Drill down into an Explorer report.
  2. Select both a **User** and a **Day**.

3. Drill down to **Day** and **User**.

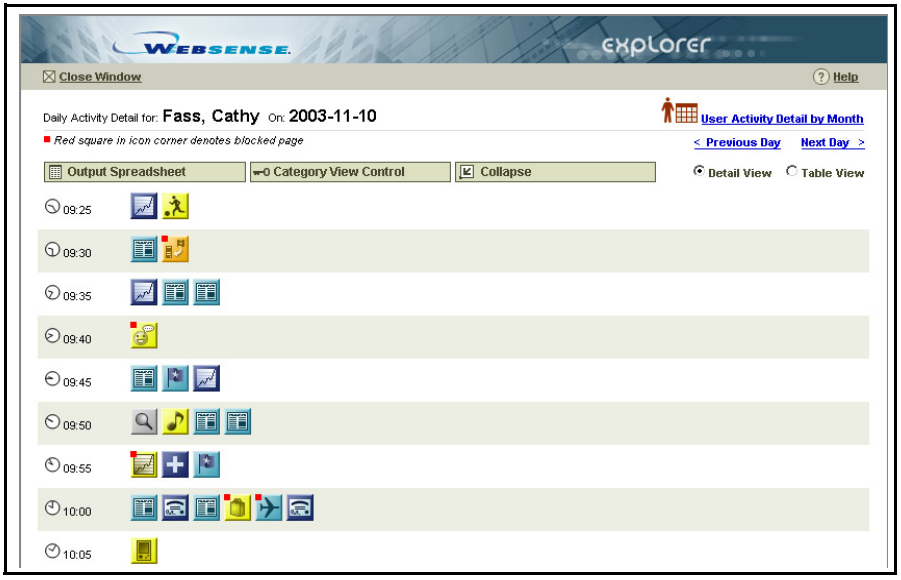


Either use the link that is available in the drill-down options or the link in the upper right hand corner of the page to run a Timeline/Calendar report.

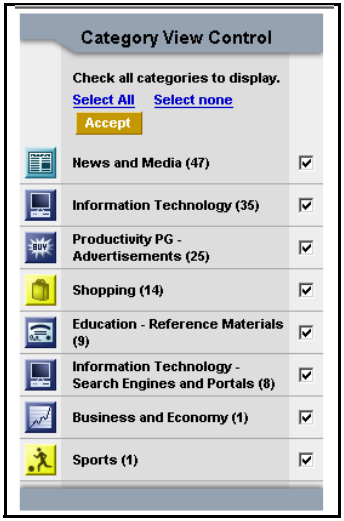
The link in the upper right hand corner is available only when a **User** and **Day** are displayed as bold and underlined in the report choices across the top of the report

In the example above, you would need to drill down further into any area in order to display the Day.

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



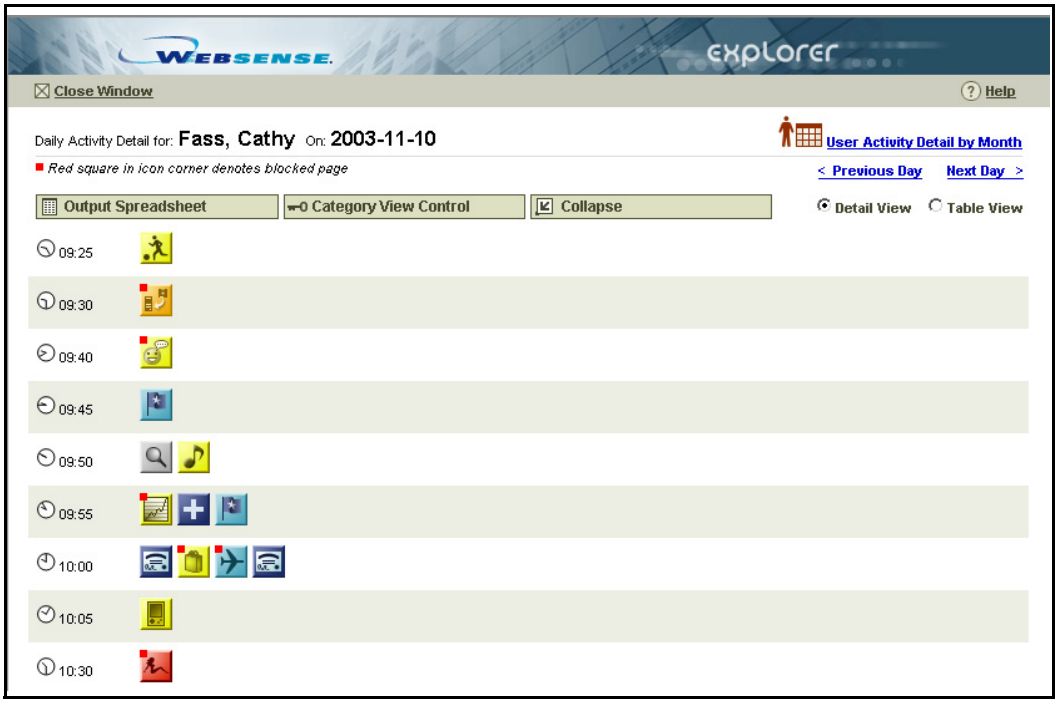
- To see which categories are represented by which icon, click **Category View Control**.



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

- To hide a category, uncheck the box, and then click **Accept**.

  In the following example report, the categories News and Media and Business and Economy have been hidden.

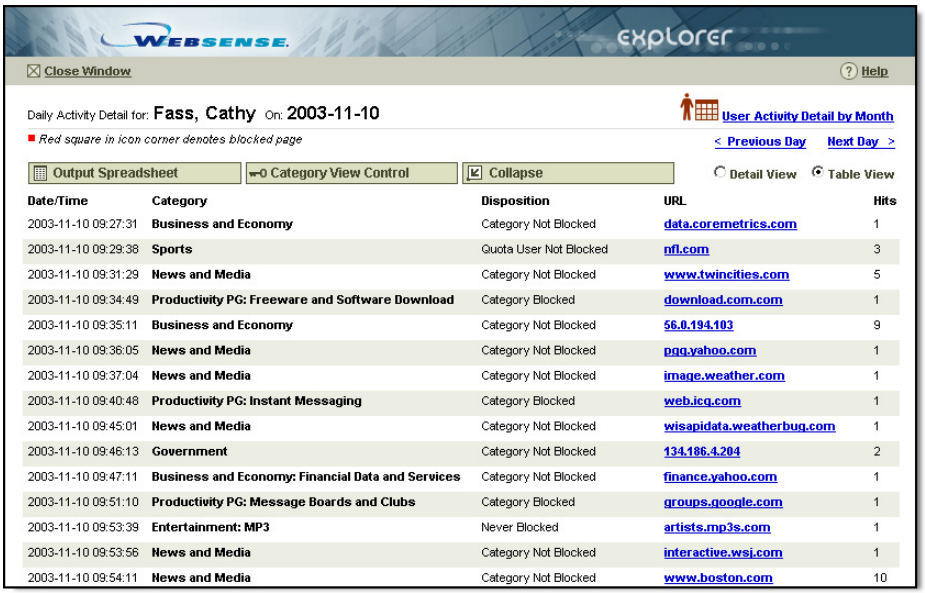


- Click **Collapse** to hide hits that are similar. This algorithm hides hits that have occurred within a particular time threshold (default is 10 seconds), with the same base URL, category and disposition. For procedures on how to change the time threshold, see the online help for your Websense filtering software.

  Collapse toggles back and forth with **Expand**.

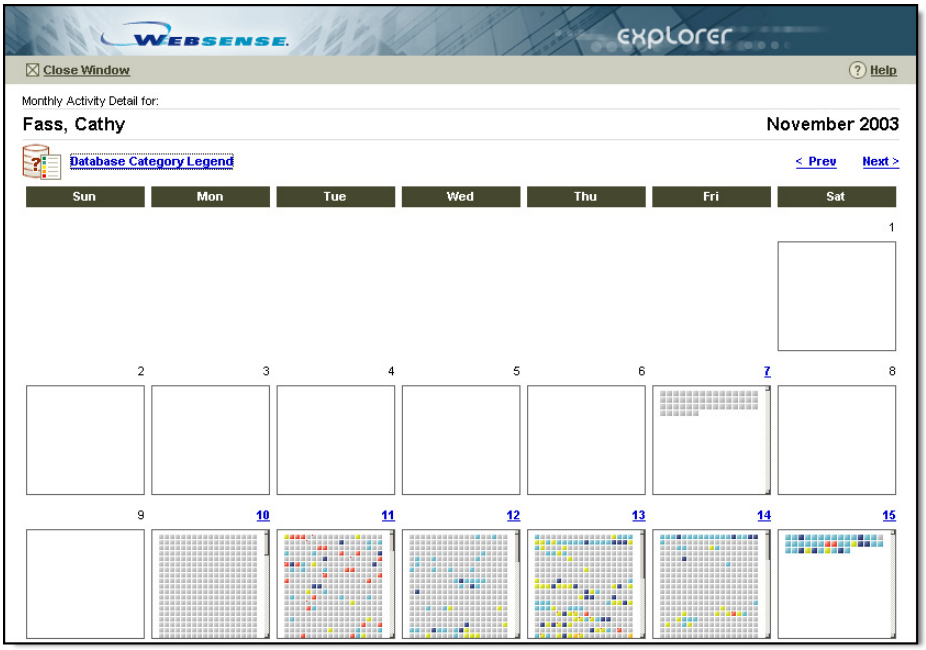
- Click **Expand** to see all hits not restricted by the Category View Control.

- To see the view in a column format, click **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	pqq.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

- To see a monthly view of thumbnails of each day's activity, select **User Activity Detail by Month**.



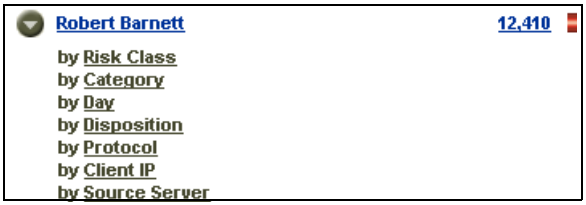
- The Database Category Legend link provides a key to the visual cues about the risk levels of the category icons displayed.

Search for user, group, or client IP

- To find Internet usage for a particular person or group, enter part or all of the first, last, or group name in the Search for User box. Make sure whatever you enter is the exact spelling.
- To find Internet usage for a particular machine, enter the Client IP in the Search for Client IP box.

In the following example, **robert** was entered for the search.

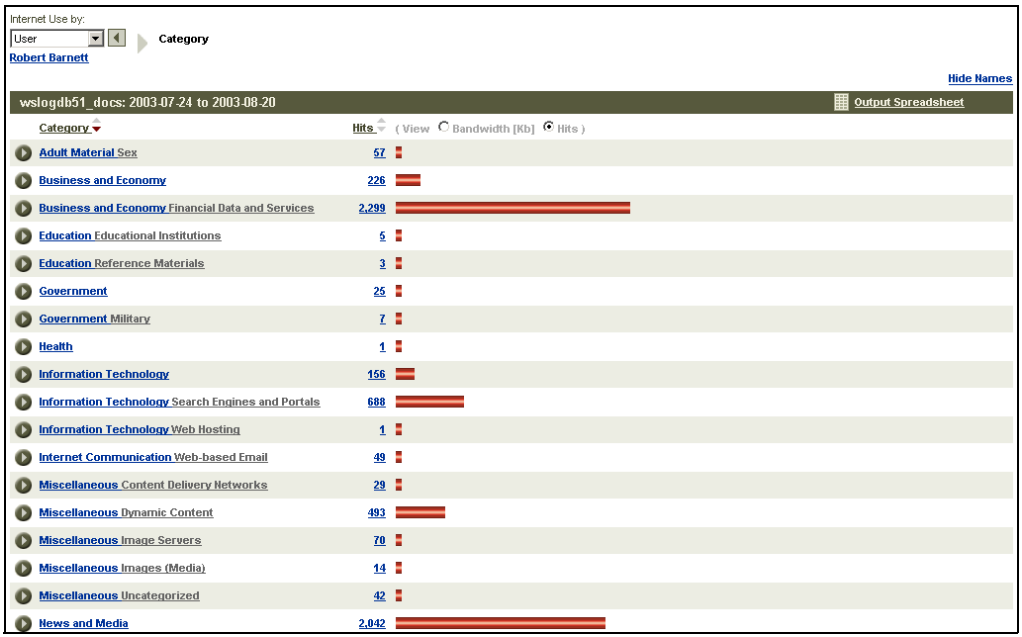
Once you have located a specific user, click > (drill-down arrow) to the left of the user name for a drop-down list to make further choices.



Output to spreadsheet

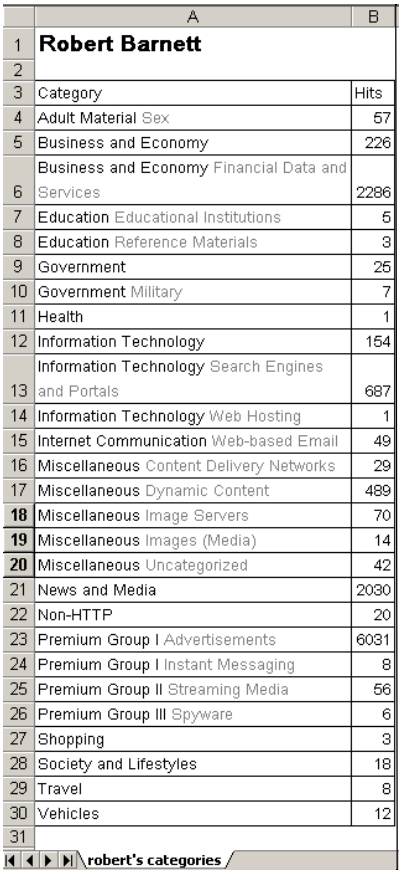
Any report results can be exported to a Microsoft Excel spreadsheet by choosing the Output Spreadsheet icon on the far right side of the page.

1. Define the report. For example, the following report shows the categories of Internet usage by Robert Barnett.



2. To produce an Excel file, click the **Output Spreadsheet** icon.
3. Select whether to Open the file, or Save it to the hard drive.

You need to have Microsoft Excel installed on your system in order to view Excel files. Your Excel file should look something like this.



	A	B
1	**Robert Barnett**	
2		
3	Category	Hits
4	Adult Material Sex	57
5	Business and Economy	226
6	Business and Economy Financial Data and Services	2286
7	Education Educational Institutions	5
8	Education Reference Materials	3
9	Government	25
10	Government Military	7
11	Health	1
12	Information Technology	154
13	Information Technology Search Engines and Portals	687
14	Information Technology Web Hosting	1
15	Internet Communication Web-based Email	49
16	Miscellaneous Content Delivery Networks	29
17	Miscellaneous Dynamic Content	489
18	Miscellaneous Image Servers	70
19	Miscellaneous Images (Media)	14
20	Miscellaneous Uncategorized	42
21	News and Media	2030
22	Non-HTTP	20
23	Premium Group I Advertisements	6031
24	Premium Group I Instant Messaging	8
25	Premium Group II Streaming Media	56
26	Premium Group III Spyware	6
27	Shopping	3
28	Society and Lifestyles	18
29	Travel	8
30	Vehicles	12
31		

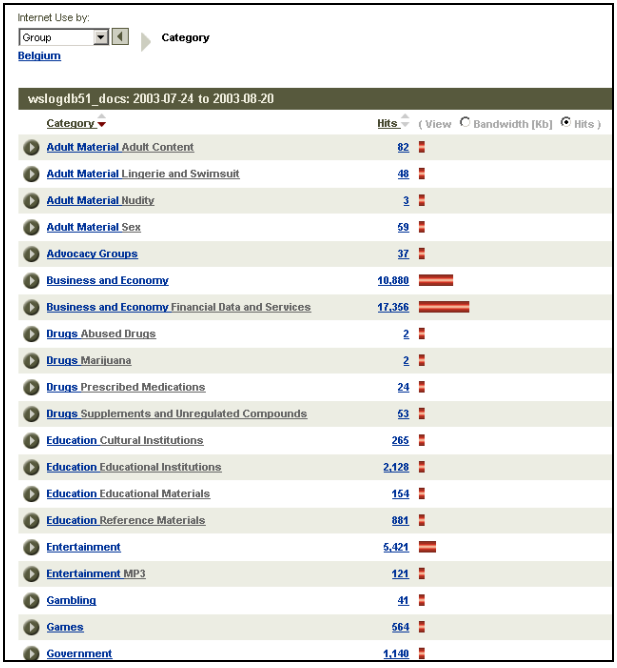
robert's categories

Lists grouped by URL

- To see specific addresses of Web sites that have been visited, run a URL report.
- Choose the number of hits, or graphic bar, to get a URL report on a row.
- Although you can request a URL report on any row, it is probably not very practical or even useful to generate a report with millions or even a hundred thousand URLs.

- Also, Explorer is limited by the processor, available memory and network resources, and it may time out on requests for large URL reports.
- Websense recommends that you drill down to get smaller and more specific summary report results before choosing a URL report.

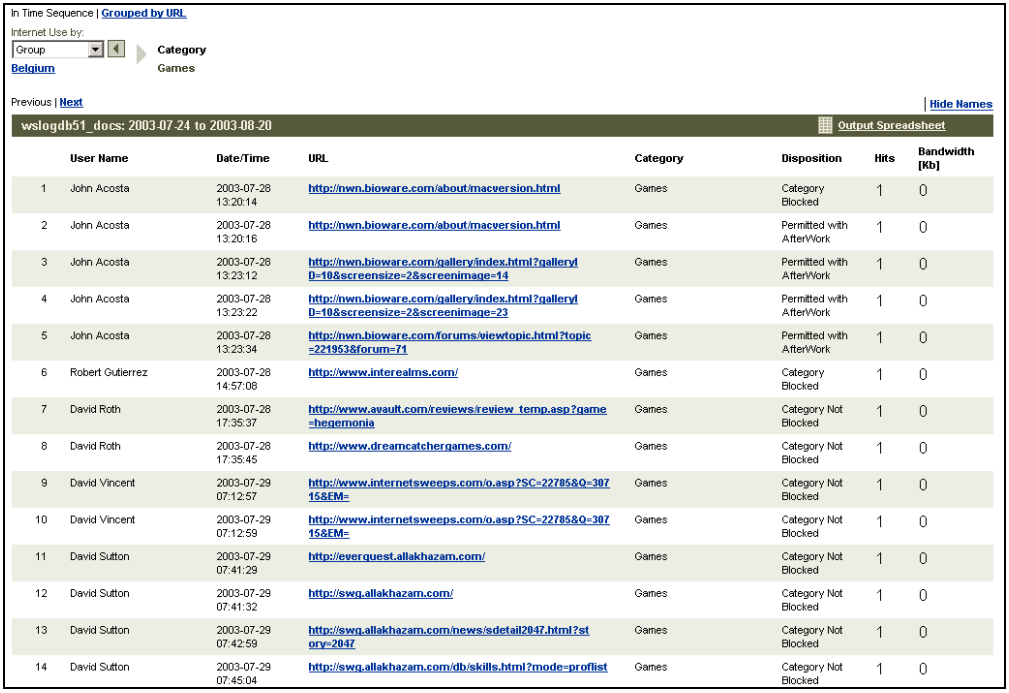
  In the following example, the URL report was defined by choosing **Group** from the **Internet Use by** drop down list, then the specific group **Belgium**, then **Category**. The results were then sorted alphabetically.



- To see the URLs in the Games category visited by this group, click 564 (the number of hits) or the graphic bar beside the number. URLs will be

shown by Hits or Bandwidth, depending on what has been chosen on the Main Page.

- To select this usage in chronological order, along with user names, select **In Time Sequence** at the top of the URL report.



In Time Sequence | Grouped by URL

Internet Use by:

Group | Category

Belgium | Games

Previous | Next | Hide Names

wslogdb51_docs: 2003-07-24 to 2003-08-20 | Output Spreadsheet

	User Name	Date/Time	URL	Category	Disposition	Hits	Bandwidth [Kb]
1	John Acosta	2003-07-28 13:20:14	http://nwn.bioware.com/about/macversion.html	Games	Category Blocked	1	0
2	John Acosta	2003-07-28 13:20:16	http://nwn.bioware.com/about/macversion.html	Games	Permitted with AfterWork	1	0
3	John Acosta	2003-07-28 13:23:12	http://nwn.bioware.com/gallery/index.html?galleryID=10&screensize=2&screenimage=14	Games	Permitted with AfterWork	1	0
4	John Acosta	2003-07-28 13:23:22	http://nwn.bioware.com/gallery/index.html?galleryID=10&screensize=2&screenimage=23	Games	Permitted with AfterWork	1	0
5	John Acosta	2003-07-28 13:23:34	http://nwn.bioware.com/forums/viewtopic.html?topic=221953&forum=71	Games	Permitted with AfterWork	1	0
6	Robert Gutierrez	2003-07-28 14:57:08	http://www.interealms.com/	Games	Category Blocked	1	0
7	David Roth	2003-07-28 17:35:37	http://www.avault.com/reviews/review_temp.asp?game=hegemonia	Games	Category Not Blocked	1	0
8	David Roth	2003-07-28 17:35:45	http://www.dreamcatchergames.com/	Games	Category Not Blocked	1	0
9	David Vincent	2003-07-29 07:12:57	http://www.internetsweeps.com/o.asp?SC=22785&Q=30715&EM=	Games	Category Not Blocked	1	0
10	David Vincent	2003-07-29 07:12:59	http://www.internetsweeps.com/o.asp?SC=22785&Q=30715&EM=	Games	Category Not Blocked	1	0
11	David Sutton	2003-07-29 07:41:29	http://everquest.allakhazam.com/	Games	Category Not Blocked	1	0
12	David Sutton	2003-07-29 07:41:32	http://swg.allakhazam.com/	Games	Category Not Blocked	1	0
13	David Sutton	2003-07-29 07:42:59	http://swg.allakhazam.com/news/sdetail2047.html?story=2047	Games	Category Not Blocked	1	0
14	David Sutton	2003-07-29 07:45:04	http://swg.allakhazam.com/db/skills.html?mode=proflist	Games	Category Not Blocked	1	0

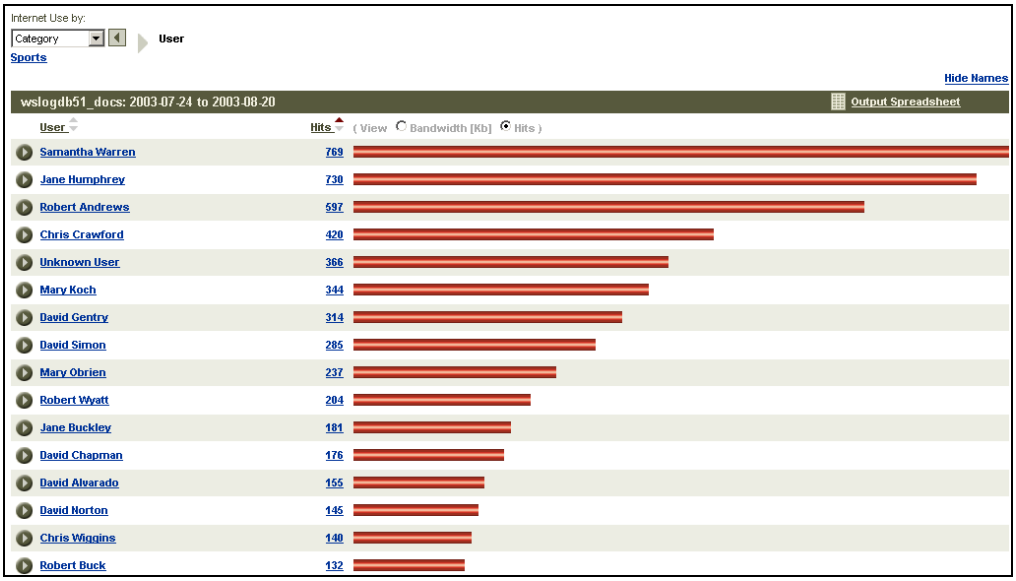
In the example, the first 14 result rows are shown. You can page through the results by choosing **Next**. To look at the actual Web site visited, click the URL to go to that site.

Hide names in reports

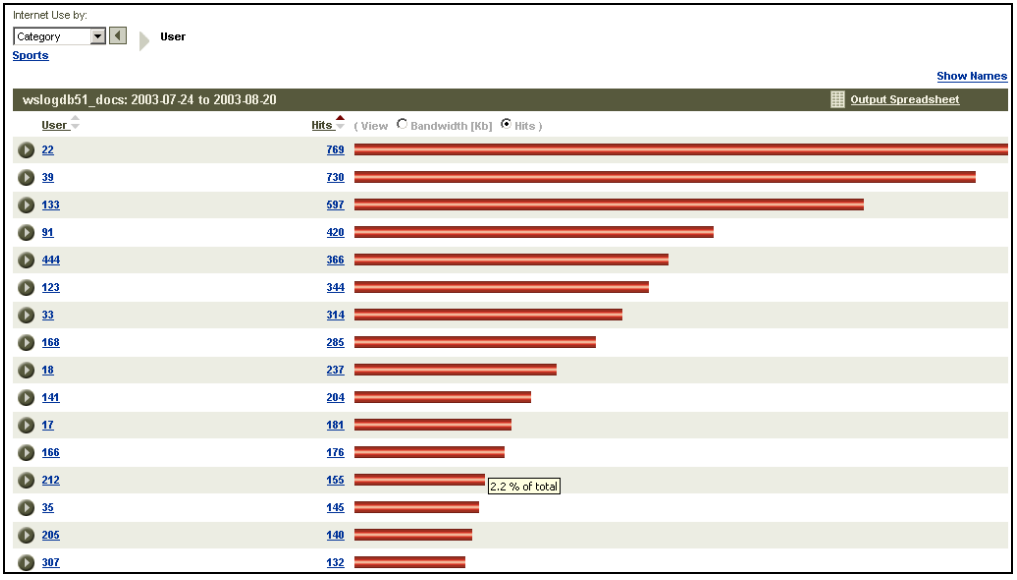
It may be useful to show a person or group a report without showing individual user names.

Use the **Hide Names** link to display user IDs instead of user names.

As an example, the report below shows a Sports category report for all users.



Using this example report above for the Sports category, the new report with hidden user names would look like this.



The only change to the report is that the names are replaced by ID numbers. **Hide Names** toggles back and forth with **Show Names**.

Tips on running URL reports

- **How practical is it to run URL reports on large number of hits?** Although you can request a URL report on any row, it is probably not very practical or even useful to generate a report with millions or even a hundred thousand URLs.

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

  Websense recommends that you drill down to get specific summary report results, before choosing a URL report.

- **Is it a good idea to run a URL report as the first Explorer report?** Although you have immediate access to running URL reports, your request will be less likely to time out if other reports are run first. Drill down into some other reports before you try running a URL report.

APPENDIX A | Maintenance and Troubleshooting

Maintenance and troubleshooting issues include:

Frequently Asked Questions (FAQs)

Question	Answer
Is there performance monitoring built in?	Some basic performance statistics can be found by going to the UNIXExplorer/bin directory and running ./ logserverdctl monitor. The different output columns are described here: • Client: The address(es) of the machine(s) which is sending log data to this server • V: The version of the log protocol. Always **3** for Websense 5.x. • RProc: The number of records processed • RCache: The number of records deferred to disk by the writer cache. The **0** means reader/writer threads are all caught up. • RFilt: The number of records filtered out by the -log-filter option • RIn/Route: # of log records in/# of log records out, in records/sec. • Age: The time since client connected to this server, in HH:MM:SS.

Question	Answer
Is there an installation log?	Yes, this file is created in the same directory as the installer package as: UNIXExplorer-6.1_install.log
How can I tell where the product is installed?	This can be found by checking the line in /etc/logserverd file that starts with ExplorerInstallPath
How can I purge records?	This can be done using the Database Purge function in the logserverd-dbtools utility.
How can I back up the database?	This can be done using the Database Archive function in the logserverd-dbtools utility.
How do I know WebCatcher is installed and running? How can I change the schedule?	To verify that WebCatcher is installed, check the UNIXExplorer/bin directory for a file called webcatcher. Changing the WebCatcher schedule is done by changing the appropriate cron job.
Is there an uninstaller?	You may uninstall by running the downloaded install package and selecting the Uninstall option from the main menu.
How do I start the logserver?	This can be done by going to the UNIXExplorer/bin directory and running ./logserverdctl start
Where are the access logs to the Explorer interface?	These logs can be found in the file UNIXExplorer/ apache2/logs/access_log
How can I create a new database?	This can be done using the Create New Database function in the logserverd-dbtools utility.
How can I view the last X records in the database?	This can be done using the Database Information function in the logserverd-dbtools utility.
How can I tell log records are coming in?	This can be done by going to the UNIXExplorer/bin directory and running ./logserverdctl monitor and verifying whether there are any clients connected.

Question	Answer
How do I change the password for the hr, admin, and anonymous logons?	This can be done by going to the /websense/UNIXExplorer/apache2/bin directory and running the following command: bash: LD_LIBRARY_PATH=../../ssl/lib ./htpasswd ../conf/.htauthpasswds username csh/tcsh: setenv LD_LIBRARY_PATH ../../ssl/lib ./htpasswd ../conf/.htauthpasswds username Be sure to replace user name with the user name you want to change the password for.

Database size

If you have been using Websense Explorer successfully and notice that reports are taking longer to display, or you begin receiving timeout messages from your Web browser, consider archiving the current Log Database and creating a new one.

Changing passwords

If you need to change Explorer passwords, it must be done at the Web server.

You can use the htpasswd command to change the password for any of the three user roles you defined during Explorer installation. For details on using this command, go to http://httpd.apache.org/docs/programs/htpasswd.html. If this link becomes outdated, you should be able to find help for the command by doing a Google search.

Special characters in domain names

When special characters are included in domain names, you may not be able to obtain a URL list for that particular domain name. Special characters include items, such as, a degree sign (°) and some country-specific characters, such as an accent (Á).

Potential issues when generating reports

Some of the potential issues when generating reports are:

Some queries take a long time.

You may see a blank screen or get a message saying that your query has timed out. This can happen for the following reasons:

- Apache Web server times out.

  If the standard timeout value is not long enough for a larger organization, try manually increasing the Timeout value in the **httpd.conf** from 300 seconds to 600 seconds.

- MySQL times out.

  You may need to manually increase the timeout limit.

- Proxy and Caching Server times out.

  You may need to manually increase the timeout limit.

When I choose Hits to look at URLs, Explorer results vary.

When you choose Hits to look at individual URLs, Explorer may decide that there is a risk of timing out during the database search if the number of Hits is too large.

Normally, if there are fewer than 3,000 Hits, Explorer groups them according to URL. If there are more than 3,000 but fewer than 30,000, Explorer will display Hits in chronological order. If there are more than 30,000, it will display the first 500 Hits found in the database (no sorting), which will usually be the first 500 in chronological order.

Users do not show up in a domain.

If users are not in any group, they will not show up in a domain either. Both Group and Domain choices will be inactive.

Explorer reports number of hits.

When the Explorer for Linux Log Server logs Visits, Explorer displays log information as *Hits*.

Index