Configuration Guide

Transitioning from SurfControl Web Filter

v7

Contents

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

Published in 2008.
Printed in the United States of America and Ireland

Trademarks

Introduction

To help you make the transition to Websense Web Security or Websense Web Filter, this guide covers the basic steps involved in setting up Websense filtering software with reporting components in a small to medium Windows network (up to 2500 users).

Important

Please refer to the *Deployment Guide* for your Websense software version for detailed help in planning where and how to install Websense components.

This guide includes information about how to:

1. Install Websense filtering software on a Windows 2003 Server machine (*Install Websense filtering software*, page 6).
2. Install Websense reporting software on another Windows 2003 Server machine (*Install Websense reporting tools*, page 8).
3. Perform basic configuration tasks (*Initial configuration*, page 9).
4. Adapt the Default policy to the needs of your organization (*Install Websense filtering software*, page 6).
5. Add filtering clients to Websense Manager (*Add filtering clients to Websense Manager*, page 16).
6. Construct policies for filtering clients whose Internet access needs aren't met by the Default policy (*Design and implement custom policies*, page 17).
7. Assign custom policies to the appropriate clients (*Assign policies to clients*, page 20).
8. Use investigative reports to analyze Internet usage patterns (*Assess your implementation*, page 21).

Complete product documentation is available at www.websense.com/global/en/SupportAndKB/ProductDocumentation/.

Prepare to install

This guide provides instructions for installing the Websense filtering software, version 7, in a stand-alone configuration. This configuration is designed for small to medium networks (up to about 2500 users).

- Websense filtering components are installed on a single machine.
- Websense reporting components are installed on a different machine.
- Websense software is not integrated with any firewall, network appliance, or proxy server.

Note

A single machine may not have adequate processing power, memory, and disk space to handle your filtering needs. Websense software is designed to be modular, allowing you to deploy different components on different machines to make the most efficient use of your resources.

If you are installing Websense filtering in a larger network, or if you want to learn how to integrate Websense software with a firewall, network appliance, or proxy server, see the *Deployment Guide* for assistance.

Make sure that your installation machine meets or exceeds the following recommendations before starting the installation process.

Hardware recommendations

Filtering machine:

- Quad-Core Intel Xeon processor, 2.5 GHz or greater
- 2 GB RAM
- 10 GB free hard disk space

Reporting machine:

- Quad-Core Intel Xeon processor, 2.5 GHz or greater
- 4 GB RAM
- 100 GB free hard disk space

Software specifications

These are streamlined specifications for a small to medium Windows network. For a more complete list of supported configurations, or if you are deploying in a Linux or mixed environment, please refer to the *Deployment Guide*.

Operating system:

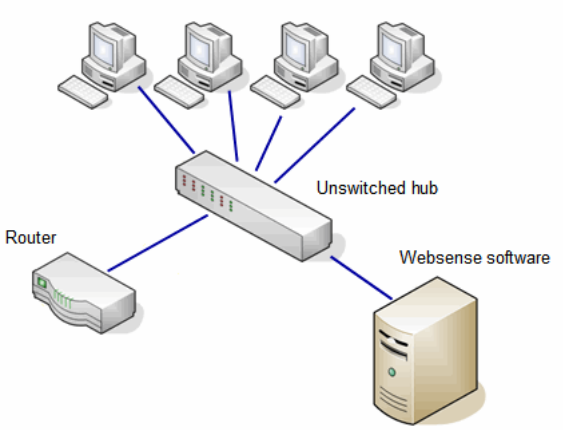
- Windows Server 2003 (Standard or Enterprise) SP1 or R2

Reporting tools used by Websense reporting tools:

- Microsoft SQL Server 2005 (recommended) or 2000, *or*
- MSDE 2000, *and*
- Internet Explorer v7

Configuration prerequisites

- **Deployment:** Connect the filtering machine to an unmanaged, unswitched hub that is located between an external router and your network. This allows the Websense Network Agent to monitor both outgoing Internet requests and replies sent to the requesting clients.



Important

Do not install Websense filtering software on a machine running a firewall. When Websense software is installed as a stand-alone product, the Websense Network Agent uses a packet-capturing utility that may not work properly when installed on a firewall machine.

- **Internet access:** For the database download to occur during installation, the Websense machine must have Internet access to the download servers at the following URLs:
  - download.websense.com
  - ddsdom.websense.com
  - ddsint.websense.com
  - portal.websense.com
  - my.websense.com

  Make sure that these addresses are permitted by all external firewalls, proxy servers, routers, or host files that control Internet access on the Websense filtering machine.

Install Websense filtering software

1. Log on to the machine that you want to use for filtering with **local** and **domain** administrator privileges.

   Install with domain administrator privileges to ensure that User Service can retrieve user logon information from the domain controller.
2. Stop any antivirus software and close all unnecessary applications.
3. Download the Windows installer package from www.mywebsense.com/download. Select the Websense Web Security / Web Filter installer.
4. Extract the installer files.

   Important

   Do not extract the installer files to a folder on your desktop. Accept the default location (**C:\Temp**), or select another appropriate directory.

   After the files are decompressed, **setup.exe** runs automatically.
5. When the welcome screen appears, click **Next**, and then follow the onscreen instructions to accept the subscription agreement.
6. Select **Websense Web Security / Web Filter** as the product to install, and then click **Next**.
7. Enter and confirm the **Password** for the **WebsenseAdministrator** account. This is the default account used to access Websense Manager.

   Important

   Make note of the WebsenseAdministrator password. Unless you create other administrative accounts, you must enter this password each time you access Websense Manager.

   Because WebsenseAdministrator has full, unconditional access to all Websense Manager features and functions, creating a strong password is highly recommended. A strong password contains a combination of lower and upper case letters, plus numbers and special characters.
8. Proceed through the installer, following the onscreen instructions and making the selections described here:

- **Multiple IPs Detected**: If the installation machine is multihomed, all enabled network interface cards (NICs) with IP addresses are listed. Select the IP address of the card to use for Websense component communication.
- **Integration Option**: Select **Stand-alone**.
- **Network Card Selection**: Specify which network interface card (NIC) to use for monitoring traffic. If the machine includes multiple NICs, select the one (connected to an unswitched hub, span port, or mirror port) that is able to monitor all Internet requests.
- **Websense Filtering Feedback**: Indicate whether Websense software should send information about access to Websense-defined categories and protocols to Websense, Inc. This data does not include information about users or machines in your network, and is used to continually improve filtering accuracy.
- **Transparent User Identification**: This guide does not include instructions for configuring Websense software to identify users or objects in a directory service without prompting them for logon information. Select **None**. You can install a transparent identification agent later.
- **RADIUS Agent**: Select **Do not install RADIUS Agent**. The agent can be installed later, if desired.
- **Installation Directory**: Accept the default path.
- **System Requirements Check**: The installer checks the resources of the installation machine. If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
- **Installation**: A summary list appears, showing the installation path and size, and the selected components. Click **Next** to begin installation.

A status bar shows the progress of the installation process.

9. After installing the filtering software, the installer displays an installation complete message. Click **Next** to exit the installer.
10. An HTML page opens, giving instructions for starting Websense Manager. Close the page. You do not need to launch Websense Manager at this time.

With the installation complete, start your antivirus software again, and then move to the reporting machine to install Websense reporting components.

Install Websense reporting tools

1. Log on to the machine that you want to use for reporting with **local** and **domain** administrator privileges.
2. Stop any antivirus software and close unnecessary applications.
3. Copy the Websense installer package from the filtering machine, or download it again from www.mywebsense.com/download.

   The same installer is used for both filtering and reporting components.
4. Extract the installer files.

   Important

   Do not extract the installer files to a folder on your desktop. Accept the default location (**C:\Temp**), or select another appropriate directory.

   After the files are decompressed, **setup.exe** runs automatically.
5. Click **Next** on the welcome screen, and then accept the subscription agreement.
6. When prompted to select a product to install, select **Custom**, and then click **Next**.
7. To choose which reporting components to install, select **Custom**, and then click **Next**.
8. Mark the **Log Server** check box, and then click **Next**.

   Log Server is the Websense reporting component that collects Internet activity information for reporting. When you install Log Server on a Windows machine, you activate the reporting features of your Websense software.
9. In the **Policy Server IP Address** field, enter the IP address of the machine on which you installed Websense filtering components, and then click **Next**.
10. When prompted, provide the following information about the database engine you want to use to store filtering log records:
    - **Database Information**: Specify the location (IP address or machine name) of the database engine (Microsoft SQL Server or MSDE) machine. If the database resides on the local machine, the host name is entered automatically. Select **SQL database account** as the method for Log Server to access the database. Do not use a Trusted Connection.
    - **Database Access Account**: Enter the user name (for example, **sa**) and password for a SQL Server account with administrator rights.
    - **Database Location**: Accept the default location for the Log Database (**wslogdb70**), or click **Browse** to select another location. Depending on the number of users filtered, the database may grow rapidly.
    - **Minimizing Database Management**: Accept the default database management selections (site visits are logged; log records are not consolidated).
11. Select an installation location for the Websense reporting components, and then click **Next**.
12. The installer checks the resources of the installation machine, and then provides a summary of the components to be installed. Click **Next** on each screen to continue the installation.

    A status bar shows the progress of the installation. When the Installation Complete message appears, click **Next** to exit the installer.

Once the reporting components have been installed, start your antivirus software again and continue with initial configuration tasks.

Initial configuration

After installation, perform the following steps on the filtering machine:

- Launch Websense Manager and enter your subscription key (see *Getting started with Websense Manager*, page 9).
- Configure Master Database download settings (see *Schedule Master Database downloads*, page 10). The database contains the URLs and protocol definitions that Websense software uses to filter Internet requests.
- Enable the Messenger Service on workstations being filtered, so protocol block messages can be received (see *Protocol block messages*, page 11).
- Verify that Websense software is configured to monitor traffic from all workstations that you want to filter (see *Define your network*, page 11).

Getting started with Websense Manager

Websense Manager is the configuration interface to Websense filtering software. This Web-based tool is used to manage filtering policies, configure Websense software, and generate reports. You can access Websense Manager from anywhere in the network.

Each time you open Websense Manager, you connect to **Policy Server**, the Websense component that stores Internet filtering policy and server configuration information. Initially, you use a default administrative account, **WebsenseAdministrator**, to connect to Policy Server.

1. To launch Websense Manager, either:
   - Log on to the Websense filtering machine and double-click the Websense Manager desktop icon.
   - Launch a supported browser (Internet Explorer 7 or Firefox 2) anywhere in the network and go to:

     ```
     https://<Filtering IP Address>:9443/mng/
     ```

   Access to Websense Manager is secured with an SSL security certificate issued by Websense, Inc. Because the browser does not recognize Websense, Inc., as a known Certificate Authority (CA), a security warning is displayed.
2. To access Websense Manager, do one of the following:
   - Select the option to ignore the warning and continue. (The exact phrasing of this option varies between browsers.)
   - Permanently accept or install the certificate. (See Accepting the Websense Manager security certificate in the Websense Knowledge base for instructions).
3. On the Websense Manager logon page, enter the user name **WebsenseAdministrator** and the password that you created during installation, and then click **Log On**.
4. You are offered the option of launching a Quick Start tutorial. Quick Start tutorials provide an excellent method for becoming familiar with Websense software. To continue following the steps in this guide, click **Skip** to continue to Websense Manager.

   Websense Manager opens, showing the **Status** > **Today** page. Because you have not yet entered a subscription key, the Health Alert Summary at the top of the page shows a series of errors and warnings.
5. Click the **Settings** tab of the left navigation pane. The **Settings** > **Account** page is displayed.

6. Enter your **Subscription key** exactly as you received it, and then click **OK**.
7. Click **Save All** at the top of the right shortcut pane to save the key and start downloading the Websense Master Database.

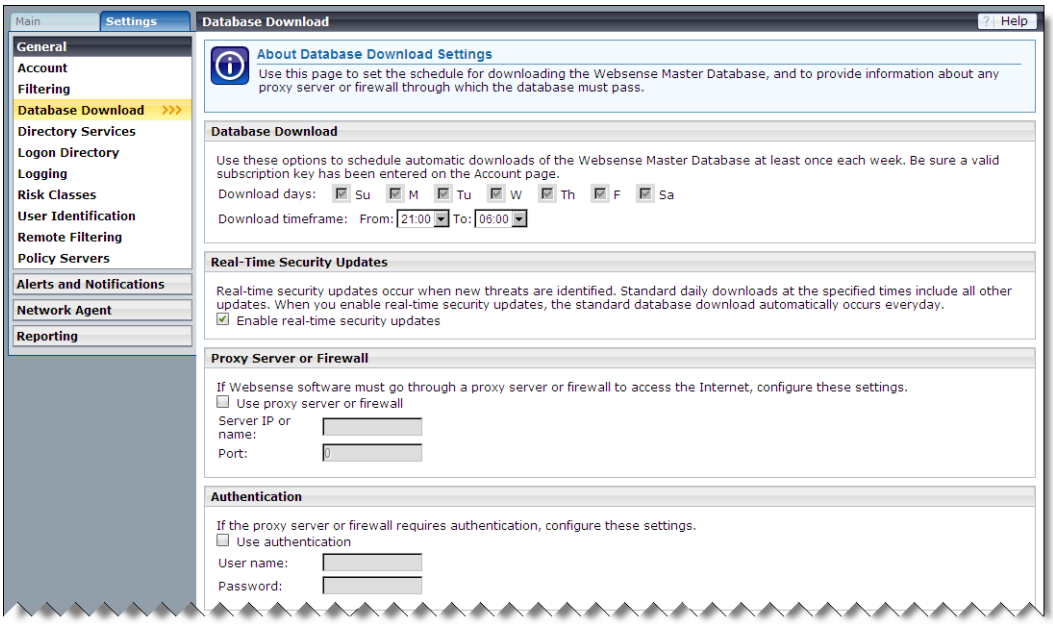
   No filtering occurs until you enter a subscription key. Downloading the database ensures full and accurate filtering.

To configure future database downloads, continue with *Schedule Master Database downloads*, page 10.

Schedule Master Database downloads

Once you have entered your subscription key in Websense Manager, verify that your local copy of the Websense Master Database will be updated regularly. The Master Database contains the category and protocol definitions used to determine how Web sites are filtered.

1. On the **Settings** tab of the left navigation pane, select **Database Download**.



2. Next to **Download days**, determine how frequently updates to the Master Database are downloaded. By default, downloads occur daily.
   - At an absolute minimum, you must download the database at least every 14 days to continue filtering without interruption. As a best practice, download the database daily (the default).
   - If you have subscribed to Websense Web Security, the Download days check boxes are selected and disabled by default. In the Real-Time Security Updates area, **Enable real-time security updates** is also selected.

     When Real-Time Security Updates are enabled, in addition to receiving complete, daily database updates, you receive interim updates each time new threats are identified.
3. Use the **Download timeframe** fields to specify a time period for each database download attempt.

   Because the process of loading database updates into memory is CPU-intensive, schedule the download for a low-traffic time.
4. If Web browsers in your network are configured to send requests through a proxy server, configure the database download process to use the same proxy settings as the browsers:

a. Check **Use proxy server**.

b. Identify the proxy server or firewall machine in the **Server IP or name** field.

> **Note**
> It is best to identify the machine by IP address. You can use a machine name, but do not use a machine name that contains extended ASCII or double-byte characters.

c. Enter the **Port** used by the proxy server or firewall (default is 8080).

5. If your network includes an external firewall or proxy that requires authentication to access the Internet, configure the database download process to provide valid credentials:
   a. Check **Use authentication**.
   b. Enter the **User name** and **Password** required by the proxy server or firewall.
   c. Configure the proxy server or firewall to accept clear text or basic authentication. For instructions, see the documentation for your proxy server or firewall.
6. Click **OK** to cache your changes, and then click **Save All** in the right shortcut pane.

   If Websense software was unable to download the database when you entered the subscription key because of missing proxy or firewall settings, a database download starts automatically.

It is best to wait until the Master Database has finished downloading before performing any policy-related configuration. To monitor the progress of the download:

1. Click the **Main** tab of the left navigation pane to go to the Status > Today page.
2. Click **Database Download** at the top of the content pane.
3. Click the Filtering Service IP address for detailed progress information.

When the database update reaches the **Completing update** stage, log off of Websense Manager, wait a few minutes, and then log back on. This ensures that any changes to categories and protocols can be properly stored in the Policy Database.

Protocol block messages

When your filtering settings block access to Internet protocols, your can determine whether protocol block messages are displayed on user machines. Protocols are filtered according to your specifications regardless of whether users can see the block messages.

For protocol block messages to display in supported Windows operating systems, the **Messenger Service** must be enabled on each client machine being filtered. Check the Windows Services manager to see if the Messenger Service is running. If your company policy requires Messenger Service to be disabled, advise users that certain protocols will be blocked without notification.

Define your network

During installation, you indicate which network card on the filtering machine Websense software should use to monitor Internet requests. After installation, when the first database download is complete, **Network Agent**, the Websense component that monitors requests in a stand-alone configuration, uses some simple guidelines to identify the machines in your network and start filtering requests.

- Machines in the following IP address ranges are assumed to be internal machines. Requests sent **to** these machines, and communication between these machines, are ignored.

```
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255
224.0.0.0 - 239.255.255.255
```

- Requests sent to the Internet **from** all internal machines visible to Network Agent software are monitored.

If this basic configuration is adequate for your network, no additional configuration is necessary.

If, however, you want to configure Network Agent to monitor requests sent **to** some internal machines (like an internal Web server), or to ignore Internet requests sent **from** certain machines, you can make those changes in Websense Manager.

Complete instructions for configuring Network Agent monitoring and blocking behavior can be found in the *Quick Start for Network Agent*, or in the Websense Manager Help (*Network Configuration* topic).

Customize the Default policy

Websense software includes a predefined **Default** policy. The Default policy is used to filter:

- Anyone to whom no other policy has been applied.
- Anyone whose current policy does not enforce a **category filter** or **protocol filter** for the current time period.

The Default policy acts as a safety net, ensuring that a certain fundamental set of filtering restrictions is applied to those not explicitly identified as requiring a different filtering policy. This means that even if you have not identified a single client, a filtering policy is still enforced for everyone in the monitored network.

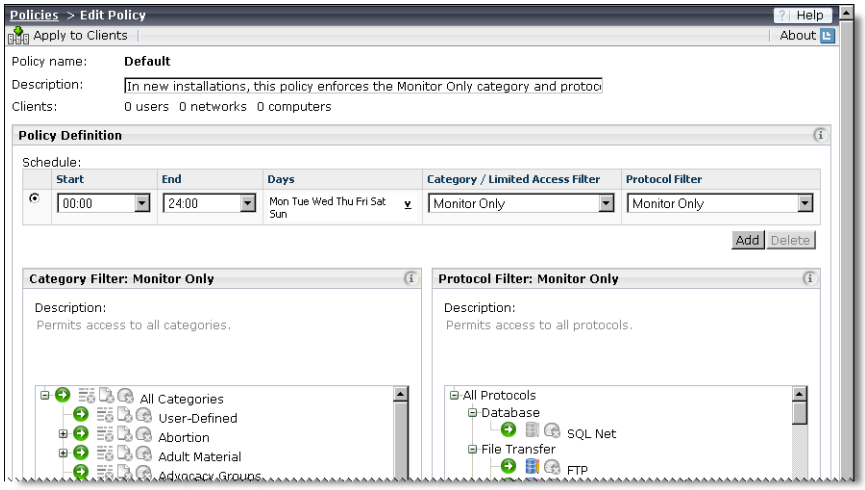
Initially, the Default policy monitors all traffic without blocking any requests.

Like other policies, the Default policy is a **schedule**, used to determine when a specific **category filter** and **protocol filter** pair is enforced. A policy can enforce the same category and protocol filter pair 24 hours a day, 7 days a week, or it can enforce different category and protocol filters at different times.

For example, to limit access to high-bandwidth sites during peak hours, but allow access to those sites during low usage periods, you could define a Peak Hours category and protocol filter, and an After Hours category and protocol filter.See *Create category filters for the Default policy*, page 13, and *Create protocol filters for the Default policy*, page 14.

Use the schedule component of your Default policy to determine when each category/protocol filter pair is enforced. See *Edit the Default policy*, page 15.

To view and edit the Default policy in Websense Manager, go to **Policy Management** > **Policies**, and then click **Default**.



Create category filters for the Default policy

A category filter is a listing of all URL categories with a corresponding action, or filtering option (like block or permit), assigned to each. The category filter applies actions both to Websense categories, defined in the Master Database, and to any custom categories that you have created.

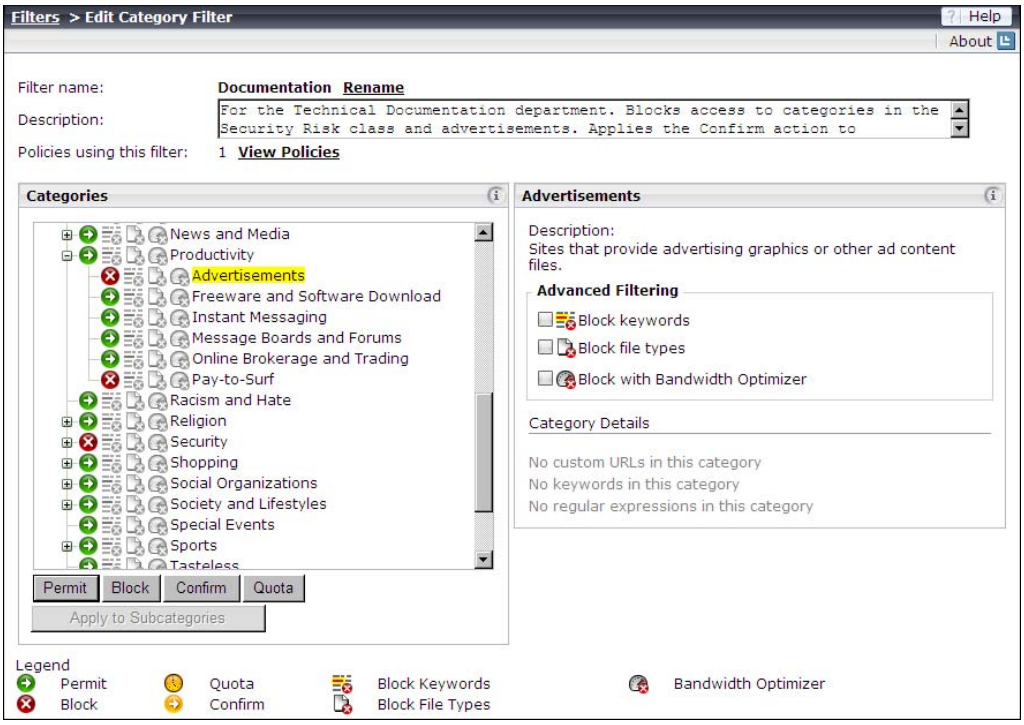
1. On the Main tab of the left navigation pane, go to **Policy Management** > **Filters**.
2. Under Category Filters, click **Add**.
3. Enter a unique **Filter name**. The name must be between 1 and 50 characters long, and cannot include any of the following characters:

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Filter names can include spaces, dashes, and apostrophes.
4. Enter a short **Description** of the filter (up to 255 characters). This description appears next to the filter name in the Category Filters section of the Filters page, and should explain the filter's purpose.

   The character restrictions that apply to filter names also apply to descriptions, with 2 exceptions: descriptions can include periods (.) and commas (,).
5. Select an entry from the drop-down list to establish the foundation for the new filter. You can either make a copy of an existing filter, or use one of the following templates:
   - **Default** applies nuanced filtering, assigning the permit, block, confirm, and quota actions to different categories.
   - **Basic** blocks categories commonly considered to present a liability or security risk, and permits the rest.
   - **Basic Security** blocks only categories in the Security Risk class, and permits the rest.
   - **Monitor Only** permits all categories. (The Default policy initially enforces the Monitor Only category filter).
6. Click **OK** to cache your changes and go to the Edit Category Filter page.

7. Select any category in the **Categories** list, and then use the buttons below the list to change the action (Permit, Block, Confirm, Quota) applied to the category. If you have completed a *Category Filter Planning Worksheet*, use it to help you customize the filter.



Note that some parent categories include subcategories. The action applied to the parent category is not necessarily applied also to its subcategories.

- Expand each parent category to see its subcategories.
- To apply the same action to a parent category and all of its subcategories, apply the action to the parent, and then click **Apply to Subcategories**.

8. When you have finished making changes to the category filter, click **OK** to cache the changes and return to the Filters page. Changes are not implemented until you click **Save All** in the right shortcut pane.

Repeat this procedure to create any additional category filters required for the Default policy.

Create protocol filters for the Default policy

After creating category filters, create the protocol filters used to filter requests for non-HTTP protocols. If you do not want to filter non-HTTP protocols, select the Permit All protocol filter in every time block.

1. On the **Policy Management > Filters** page, under Protocol Filters, click **Add**.
2. Enter a unique **Filter name**. The name must be between 1 and 50 characters long, and cannot include any of the following characters:

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Filter names can include spaces, dashes, and apostrophes.
3. Enter a short **Description** of the filter (up to 255 characters). This description appears next to the filter name in the Protocol Filters list, and should explain the filter's purpose.

The character restrictions that apply to filter names also apply to descriptions, with 2 exceptions: descriptions can include periods (.) and commas (,).

4. Select an entry from the drop-down list to establish the foundation for the new filter. You can either make a copy of an existing filter, or use one of the following templates:
   - **Default** blocks the Instant Messaging / Chat protocols, as well as the P2P File Sharing, Proxy Avoidance, Instant Messaging File Attachments (if subscribed), and Malicious Traffic (Websense Web Security).
   - **Basic Security** blocks the P2P File Sharing and Proxy Avoidance protocols, as well as Instant Messaging File Attachments (if subscribed) and Malicious Traffic (Websense Web Security).
   - **Monitor Only** and **Permit All** permit all protocols. (The Default policy initially enforces the Monitor Only protocol filter).
5. Click **OK** to cache your changes and go to the Edit Protocol Filter page.
6. Select any protocol in the **Protocols** list, and then use the buttons below the list to change the action (Permit or Block) applied to the protocol. If you have completed a *Protocol Filter Planning Worksheet*, use it to help you customize the filter.

   Note that the action applied to one protocol in a protocol group is not automatically applied to other protocols in the group. To apply the same action to all protocols in a protocol group, apply the action to one protocol, and then click **Apply to Group**.
7. When you have finished making changes to the protocol filter, click **OK** to cache the changes and return to the Filters page. Changes are not implemented until you click **Save All** in the right shortcut pane.

Repeat this procedure to create any additional protocol filters required for the Default policy.

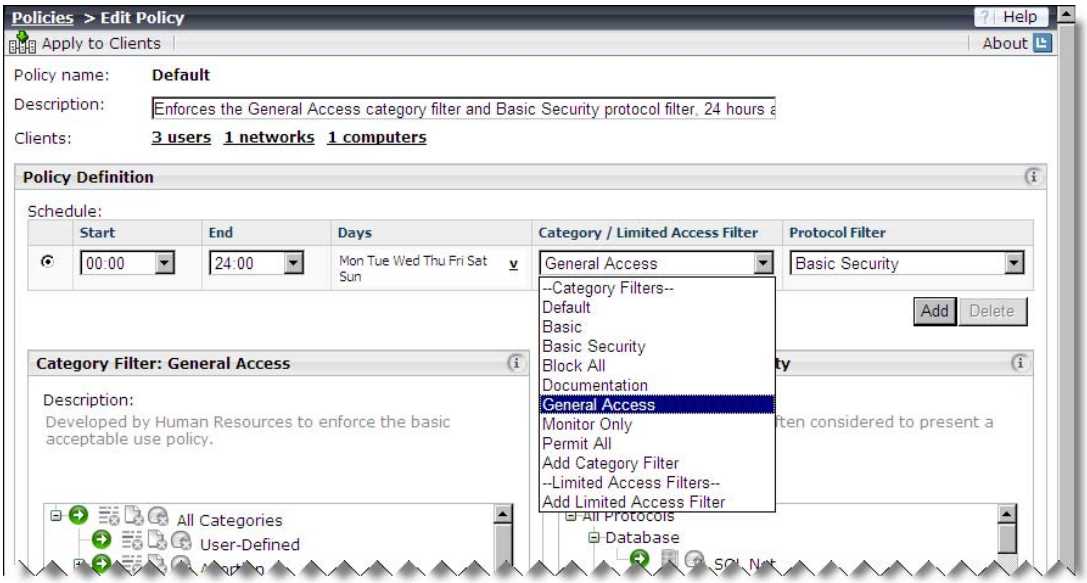
Edit the Default policy

When you are finished creating category and protocol filters, you are ready to edit the Default policy. You may want to use the Policy Planning Worksheet to design the Default policy before you begin.

1. In Websense Manager, go to **Policy Management > Policies**, and then click **Default**.

   The Edit Policy page opens, showing the current policy schedule. By default, the Default policy enforces the same category and protocol filter at all times, every day.
2. If you want to enforce different category and protocol filters at different times, start by creating the time periods that you need.
   a. Click **Add** (below the Schedule table) to add a time block to the schedule.
   b. Use the drop-down lists to change the **Start** time and **End** time in the new time block.
   c. Click the down arrow (**v**) in the Days column to determine which **Days** of the week are included in this time block.

3. To specify which category and protocol filter you want to enforce during each time period, click the appropriate Category / Limited Access Filter or Protocol Filter entry, and then select a category or protocol filter from the list.



4. When you are finished editing the policy, click **OK** to cache your changes and return to the Policies page. Changes are not implemented until you click **Save All**.

After you click Save All, it takes only a few seconds for the customized Default policy to take effect.

Next, learn how to add filtering clients to Websense Manager. Once clients have been identified in Websense Manager, you can assign them custom policies.

Add filtering clients to Websense Manager

To filter clients using policies other than Default, first add them to Websense Manager. In all environments, you can define **computer** (IP address) and **network** (IP address range) clients. If your network includes a directory service, you can also define **directory** (user, group, or domain/ organizational unit) clients.

> **Note**
> Even if your network includes a supported directory service, Websense software always identifies computer clients by IP address, and not by name.

Before you can add directory clients, you must configure Websense software to communicate with your directory service. This configuration is performed on the **Settings > Directory Services** page. Websense software can communicate with Windows Active Directory (Native Mode), Novell eDirectory, or Sun Java Directory via LDAP, or with Windows NT Directory / Active Directory (Mixed Mode) via NTLM.

See the Websense Manager Help (available in HTML or PDF format) for complete configuration instructions for your directory service.

Add workstation and network clients

1. In Websense Manager, go to **Policy Management > Clients**, and then click **Add**.
2. Use the **Computer** or **Network** fields to enter an IP address or contiguous IP address range to identify a machine or group of machines for filtering.
3. Click the right arrow (>) to add computer or network clients to the Selected Clients list.
4. Repeat steps 2 and 3 to add additional clients. Note that all clients in the Selected Clients list are initially assigned the same policy.
5. Use the **Policy** list (below the Selected Clients list) to select which policy will be assigned to the new clients. The Default policy is initially selected.
6. Click **OK** to cache your changes and return to the Clients page.
   - Individual IP addresses are shown in the Clients tree under **Computers**.
   - IP address ranges are displayed under **Networks**.
7. When you have finished adding clients, click **Save All** in the right shortcut pane.

Add directory clients (users, groups, and domains/organizational units)

Once you have configured Websense software to communicate with a supported directory service, you can add users and groups from the directory as filtering clients.

1. In Websense Manager, go to **Policy Management > Clients**, and then click **Add**.
2. Expand the **Directory Entries** folder and browse to find users, groups, domains, or organizational units to add as filtering clients.

   If you are using an LDAP-based directory service, you can also click **Search** to enable a directory search tool.
3. Click the right arrow (>) to add selected directory clients to the Selected Clients list.
4. Repeat steps 2 and 3 to add additional clients. Note that all clients in the Selected Clients list are initially assigned the same policy.
5. Use the **Policy** list (below the Selected Clients list) to select which policy will be assigned to the new clients. The Default policy is initially selected.
6. Click **OK** to cache your changes and return to the Clients page. The new clients are added to the Directory node of the Clients tree.
7. When you have finished adding clients, click **Save All** in the right shortcut pane.

Design and implement custom policies

Once you have customized the Default policy to establish a filtering baseline (and safety net) for your organization, create additional policies as needed to provide appropriate Internet access to all groups within your organization.

Before creating a new policy:

1. Identify the particular needs of clients to be filtered by the new policy.
2. Create the category filters or **limited access filters** required to filter the clients appropriately.

A limited access filter is an alternative to a category filter. Instead of URL categories, it identifies individual Web sites, identified by URL or IP address, that users can access. When a limited access filter is in effect, all sites not appearing in the list are blocked.

3. Create the necessary protocol filters.

For example, suppose that you have created a Default policy for a small credit union. Due to privacy, security, and liability concerns, this policy is very restrictive, allowing access only to applications used in banking transactions and the bank's own external Web site.

A group of financial counsellors and loan officers, however, need broader access to get current financial information and help customers compare their options.

- The Default policy enforces the All Tellers limited access filter and Restricted protocol filter at all times.
- The Counsellors policy will require a Finance category filter that permits:
  - The Business and Economy parent category and Financial Data and Services subcategory
  - The Education > Educational Materials and Reference Materials subcategories
  - A Financial Counselling custom category listing additional approved sites
- The Counsellors policy will also require an Extended Communications protocol filter to allow some access to approved communications tools (including instant messaging and chat).

Create category and protocol filters for a custom policy just as you did for the Default policy. You can use the category and protocol filters enforced by the Default policy as templates for the new category and protocol filters that you create.

How does Websense software determine which policy to apply?

When you apply custom policies, situations may arise when multiple policies could potentially apply to the same request. For example, one policy could be assigned to a user, while a different policy is assigned to the machine where the user is logged on. In these cases, Websense software determines which policy to enforce as follows:

1. Apply the policy assigned to the user making the request. If the policy does not exist, or has no category filter scheduled at the time of the request, use the next applicable policy.
2. Look for a policy assigned to the computer (first) or network (second) from which the request was made.
3. If there is no computer or network-specific policy, or the policy has no category filter scheduled at the time of the request, look for a policy assigned to any group to which the user belongs.

   In cases where a user belongs to multiple groups with different policies assigned, Websense software uses a configurable setting to determine which policy applies. See the Websense Manager Help for details.
4. If there is no group policy, look for a policy assigned to the user's domain or OU.
5. If no applicable policy is found, enforce the Default policy.

Refine category filtering beyond permit and block

When you create or edit a category filter, you determine whether to assign the Block, Permit, Confirm, or Quota action to each URL category. You can further refine users' options by

implementing keyword and file type blocking, creating limited access filters, and defining custom URLs.

- **Keywords** are strings (words, or other groups of characters) used to match URLs to categories. You define keywords and associate them with a category, then enable keyword blocking in a category filter. When Websense software finds a keyword in a URL, the site is recategorized and blocked.
- **File Types** are groups of related file extensions, used to filter access to specific Internet content formats. With file types, you can block access to specific kinds of files (like music or video files) from sites in an otherwise-permitted category.
- **Custom URLs** allow you to change the way individual sites (URLs or IP addresses) are filtered. There are 2 kinds of custom URLs:
  - **Recategorized URLs** are sites (URLs or IP addresses) assigned to a category other than the one assigned by the Master Database.
  - **Unfiltered URLs** are sites that are permitted even when their Master Database category is blocked, except for clients governed by a limited access filter or the Block All category filter.

Custom URLs are often used in combination with custom categories. These are subcategories that you add to any Master Database parent category, or to the User-Defined category. First create the custom category, and then recategorize URLs to populate it.

Go to **Policy Management > Filter Components** in Websense Manager to work with keywords, file types, custom URLs and custom categories. Limited access filters can be created and edited from the **Policy Management > Filters** page.

See the Websense Manager Help for detailed instructions, and to understand filtering precedence (the order in which filtering settings are enforced).

Filter categories and protocols based on bandwidth

Bandwidth Optimizer provides the ability to limit Internet access based on either available network bandwidth or bandwidth usage by a specific protocol (HTTP, FTP, IRC, and so on).

Bandwidth Optimizer settings:

- Can be applied to any category or protocol
- Can be configured separately for each category or protocol filter

See the Websense Manager Help for detailed instructions.

Create a custom policy

When all of the pieces of the policy are in place:

1. Go to the **Policy Management > Policies** page and click **Add**.
2. Enter a unique **Policy name**. The name must be between 1 and 50 characters long, and cannot include any of the following characters:

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Policy names can include spaces, dashes, and apostrophes.
3. Enter a short **Description** of the policy (up to 255 characters). This description appears next to the policy name in the Policies list, and should explain the policy's purpose.

The character restrictions that apply to policy names also apply to descriptions, with 2 exceptions: descriptions can include periods (.) and commas (,).

4. To use an existing policy as the starting point for the new policy, mark **Base on existing policy**, and then select an entry from the drop-down list.
5. Click **OK** to cache your change and go to the Edit Policy page.
6. Edit the policy schedule, category filters, and protocol filters as needed.

   Note that the filters enforced by the selected time block in the schedule are displayed in the bottom portion of the page. You can make changes to these filters from directly within the Edit Policy page. Remember that changes that you make to a filter here affect all policies that enforce that filter.
7. When you are finished making changes, click **OK** to cache your changes and go to the Policies page. Changes are not implemented until you click **Save All**.

Assign policies to clients

There are 2 methods that you can use to assign policies to clients of any type (directory, computer, or network):

- Edit the client entry on the **Clients** page.
- Apply the policy to clients from the **Edit Policy** page.

To edit a client entry:

1. Go to **Policy Management > Clients**.
2. Select one or more clients in the Clients tree. The clients do not need to be of the same type.
3. Click **Edit**.
4. To change the policy assigned to the selected clients, click **Change** under Policy (near the top of the page).
5. Select a policy from the **Name** list.
6. Click **OK** to cache the change and return to the Clients page. Changes are not implemented until you click **Save All**.

To apply a policy that you are editing:

1. Go to **Policy Management > Policies**, and then click a policy name.
2. Click **Apply to Clients** at the top of the Edit Policy page.
3. Use the Select Clients tree to select one or more clients to whom the policy should be applied. Only clients that you have already added to Websense Manager appear in this tree.

   The clients to whom you apply the policy do not need to be of the same type.
4. Click **OK** to cache the change and return to the Edit Policy page. Changes are not implemented until you click **Save All**.

Once you click Save All, the selected clients are filtered according to the restrictions of the policy you assigned. (It may take a few seconds for the change to go into effect.)

Assess your implementation

Once you have implemented Internet filtering, Websense reporting tools can help you to evaluate the results and overall effectiveness of your filtering policies.

- Identify Internet usage patterns for your organization.
- Investigate unexpected surges or dips in Internet usage.
- Verify that policies are being enforced correctly.
- Identify high-traffic uncategorized sites for investigation and possible recategorization.

When you install the Websense Log Server component on a Windows machine, Websense reporting tools are shown in Websense Manager.

- The **Status > Today** and **Status > History** pages show graphs and bar charts with information about current and recent filtering activity.
  - Get an overview of how Websense filtering has protected your network from unproductive and security risk browsing.
  - View user activity for today, or the previous 30 days, to determine what factors need further investigation.
  - Click a chart to launch an investigative report with related information.
- **Reporting > Presentation Reports** offers a formatted view into the Internet filtering information stored in the Websense Log Database. Predefined charts and tabular reports make it easy to generate a consistent presentation of data on a particular topic, such as the categories that have been blocked the most during a particular time frame. You can:
  - Run reports for specific time frames.
  - Copy predefined reports, and edit the filter that determines which clients, categories, protocols, and actions are reported.
  - Schedule reports to run at a specific time or on a repeating schedule.
- **Reporting > Investigative Reports** provides an interactive interface that provides summaries of current Internet usage and tools for performing detailed usage analysis. You can:
  - See a quick overview of Internet usage information.
  - Drill down to more detailed information on Internet activity of particular interest or concern.
  - Generate customizable detail reports on specific areas of interest.
  - Save and schedule Favorite Reports to run at your convenience.

Generate formatted reports

The **Reporting > Presentation Reports** page in Websense Manager displays a catalog of predefined reports, organized into logical groups.

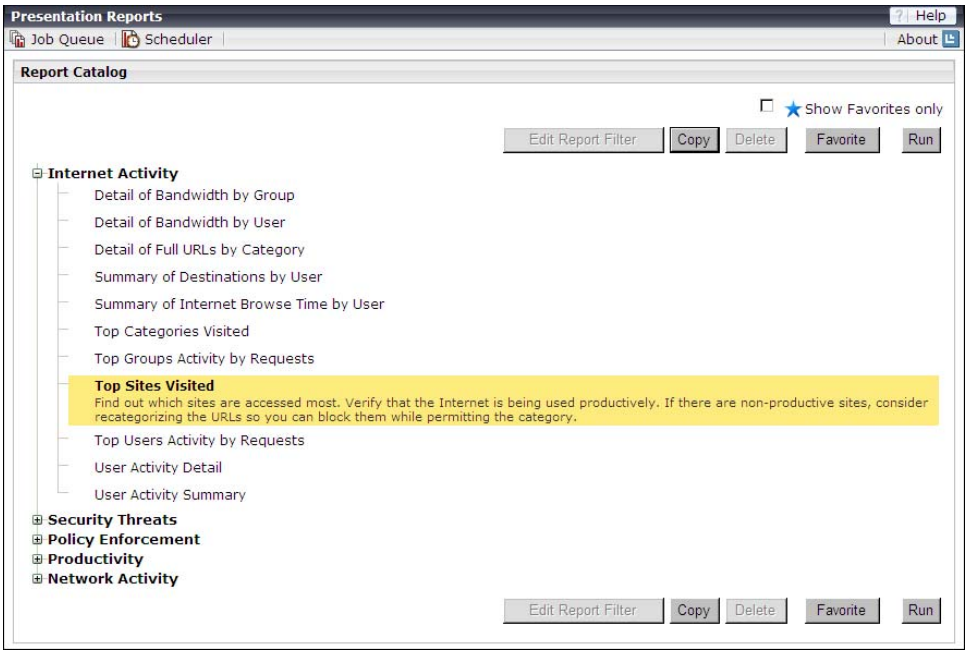
To select and generate a report:

1. Click the plus sign (+) beside a group name to open that portion of the list.
2. Select any report. A brief description of the selected report is displayed.
3. Use the buttons above and below the catalog to copy or run the selected report, or to make it a Favorite.

   If you have selected a custom report, you can also edit the report filter or delete the report.

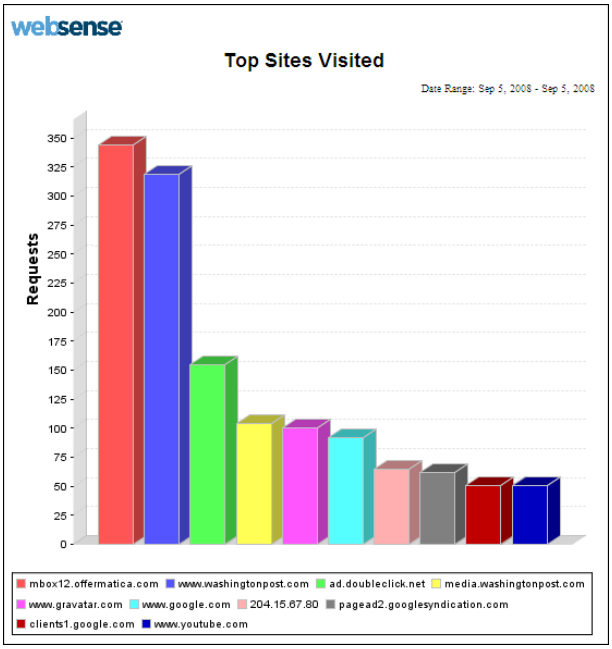
For example, to generate a Top Sites Visited report:

1. In the Report Catalog tree, expand the **Internet Activity** heading, and select the **Top Sites Visited** report.



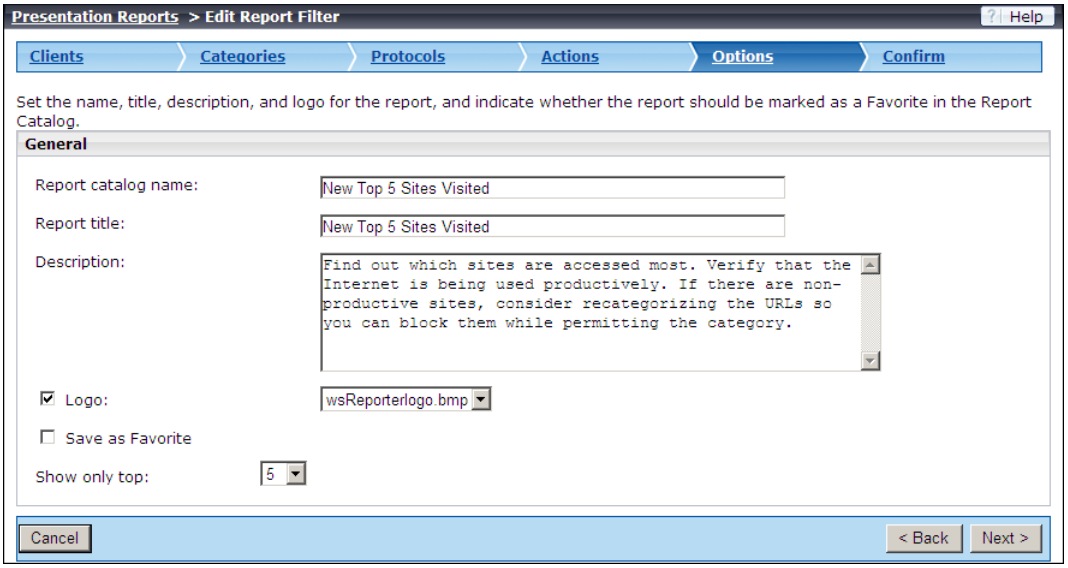
2. Click **Run** at the top or bottom of the list.
3. On the Run Report page, enter start and end dates, choose HTML as the output format, and accept the default of 10 as the number of reported sites.
4. Click **Run**.

   Websense software gathers the appropriate records from the Log Database, and displays the report in the Websense Manager content pane.



To create a custom report, first copy a predefined report, and then configure the clients, categories, protocols, and filtering actions to include on the report.

1. On the **Presentation Reports** page, select **Top Sites Visited** under the Internet Activity group.
2. Click **Copy** to create a duplicate of the predefined report in the Internet Activity section of the report list.
3. Select **Top Sites Visited(1)**, the duplicate you just created, and then click **Edit Report Filter**.
4. Accept the default (all items reported) or select items of interest, and click **Next** to move through the Clients, Categories, Protocols, and Actions tabs.
5. On the **Options** tab, change the **Report catalog name** and **Report title** to **New Top 5 Sites Visited**. This name appears on the Presentation Reports page in place of the name you clicked in step 3, and on the finished report.



6. For **Show only top**, select **5**, and then, click **Next**.
7. On the **Confirm** tab, select **Save and run**, and then click **Finish**.
8. On the **Run Report** page, set the **Output format** to **HTML**, and then click **Run**.

   Websense software gathers the appropriate records from the Log Database, and displays the report in the Websense Manager content pane.

   The changes you made in the report filter are saved with the new report. The new name appears on the Presentation Reports page. Any time you choose this report to run, it uses the filter you defined.

See the Websense Manager Help for information about presentation reports.

Analyze Internet access trends

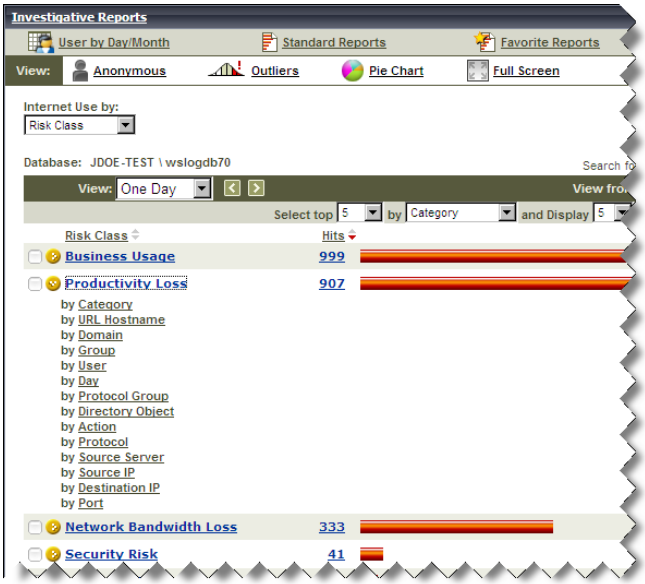
The **Reporting > Investigative Reports** page in Websense Manager lets you browse logged Internet activity data interactively.

When you initially open investigative reports, the main page shows a summary of Internet use by risk class. Each risk class groups categories by their potential risk type (Security Risk, Legal Liability, Productivity Loss, Network Bandwidth Loss, or Business Usage). A category can appear in more than one risk class.

Browse current summary data, drill down to find more detailed information, customize the dates included, or use the **Search** function to view activity for a particular client or URL.

Drill down to uncover the details that matter most to your organization.

1. On the initial report, click **Productivity Loss** to display a list of drill-down options.



   If there is no Productivity Loss entry, clients in your network have not requested any sites in that risk class. In that case, select another risk class.

2. Click **by Category** in the list of options.

   The chart changes to show today's activity in the categories assigned to the selected risk class.

   Use the **View** options above the chart if you want to change the dates included in the report.

3. Click the first category name in the chart (for example, **News and Media**) to display a new list of drill-down options.

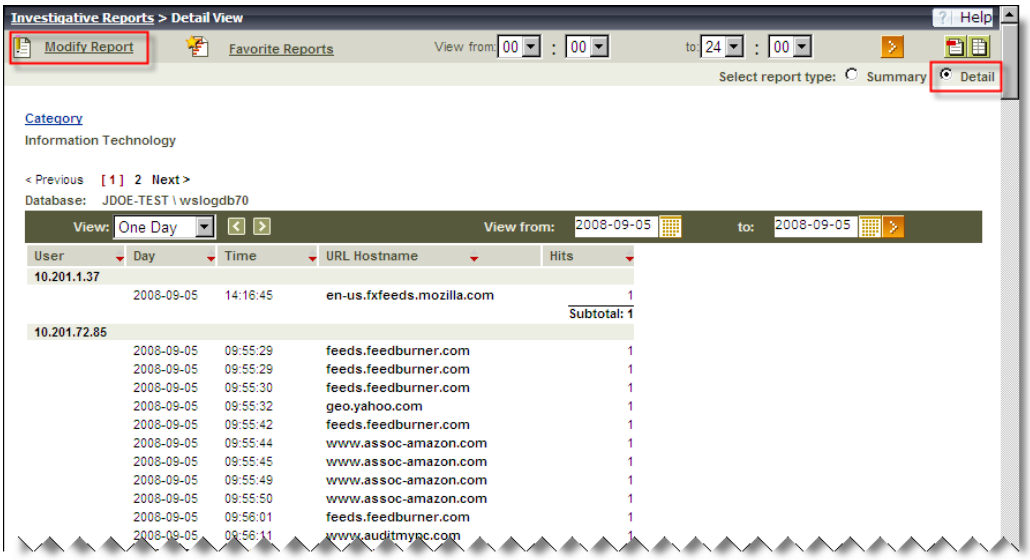
4. Click **User** to have the chart show a list of users who have requested sites in the selected category.

You can continue selecting drill-down options to see more detail about any item of interest.

Additionally, you can design your own report, showing just the details that interest you most. For example:

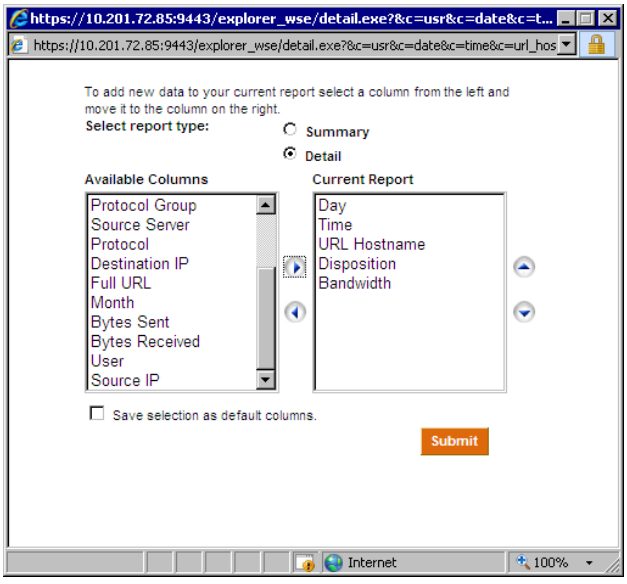
1. Go to **Reporting** > **Investigative Reports** to restore the default report.
2. Select **Category** from the **Internet Use by** list.
3. Click the bar or number for any category that shows a significant number of hits.

   The flexible detail view appears, showing a tabular report of today's traffic for the selected category. The default report includes columns for User, Date, Time, URL Hostname, and Hits.



4. Click **Modify Report** in the toolbar at the top of the content pane. A dialog box opens.

   The columns displayed in the current detail report are shown in the **Current Report** list.
5. To change the information that appears in the report, select a column name (User, Category, and so on), and then use the left and right arrow buttons to move selections between the **Available Columns** and **Current Report** lists.



   For descriptions of all available columns, see the Websense Manager Help.
6. Click the up and down arrow buttons to change the order of columns in the report. The first entry represents the first column in your report.
7. Click **Submit** to close the dialog box and update the report.

Notice that the new columns are now displayed, in the order you specified.

You can save any report as a Favorite by clicking **Favorite Report** in the toolbar at the top of the content pane. Then, run the same report quickly at any time, or schedule it to run on a recurring basis. See the Websense Manager Help for details on scheduling investigative reports.

Conclusion

This completes your initial configuration of Websense Web Security or Websense Web Filter. Please refer to the Websense Manager Help for detailed information about continuing to configure and manage your filtering setup.

Also see Websense Knowledge Base for access to articles, technical papers, video tutorials, and other resources that you can use to make the most of your Websense filtering and reporting software.