PureSight User's Guide

Copyright Notice

NO WARRANTY: This technical documentation is delivered to you as is, and PURESIGHT makes no warranty as to its accuracy or use. Any use of the technical documentation, or the information contained therein, is at the user's risk. Technical or other inaccuracies, as well as typographical errors, may occur in this document. PURESIGHT reserves the right to make changes without prior notice.

Trademark

The PURESIGHT logo is a trademark of PURESIGHT INC. All rights reserved.

Other company and brand products, as well as service names, are trademarks or registered trademarks of their respective holders.

Technical Support

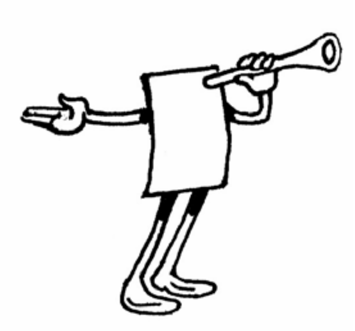
If you require technical support services, contact us at support@puresight.com

About This Guide

This guide provides instructions for using and configuring PureSight. It contains the following chapters:

- **Chapter 1, Introduction**, introduces PureSight and describes its main features.
- **Chapter 2, Getting Started**, describes the functionality of the PureSight Administration page and how to access it, and provides an overview of the workflow.
- **Chapter 3, Managing PureSight Content Filtering Servers**, describes how to initialize and edit the settings of a PureSight Content Filtering Server.
- **Chapter 4, Defining Users and Groups**, describes how to add and edit users and user groups.
- **Chapter 5, Defining Filters**, describes PureSight's filters, and provides instructions on how to customize them.
- **Chapter 6, Defining Policies**, describes PureSight's policies, and how to create or edit policies.
- **Chapter 7, Settings**, describes the configurable options for the messages, rating systems, log server and system settings.
- **Chapter 8, Reports**, describes PureSight's report options, and how to generate reports.
- **Chapter 9, System Diagnostics,** describes the system analysis tools provided in PureSight to identify potential problems.

Table of Contents



Chapter 1

Introduction

About This Chapter

This chapter provides an introduction to PureSight™ and the PureSight Administration tool.

Introducing PureSight

PureSight was created especially for the complex requirements of the modern online corporation or institution. PureSight combines precision Internet filtering capabilities with powerful management tools to offer a highly accurate and reliable Internet content-filtering solution. PureSight is suitable for small, medium, and large organizations, as well as service providers.

PureSight is based on proprietary Artificial Content Recognition™ (ACR) technology. Using Artificial Intelligence (AI) algorithms, ACR enables PureSight to analyze the HTML page of each requested Web site and categorize the page based on its content. PureSight allows Internet usage policies to be defined, implemented and modified according to the changing needs of the organization.

DisCo System Architecture

PureSight employs an advanced Distributed Collaborative (DisCo) System architecture. This modular system architecture is designed to maximize management investments by providing flexible integration, improved performance and scalability.

Designed to simplify management of a high availability network, PureSight's distributed architecture utilizes three basic modules: PureSight Management Server, PureSight Content Filtering Server and PureSight Log Server.

This next generation architecture provides for:

- ✦ Centralized management and configuration of all PureSight Content Filtering Servers by a single PureSight Management Server. This also enables large organizations to manage remote branch office sites using the same Management Server, and thereby implementing a centralized policy throughout the organization regardless of physical location.
- ✦ Automatic, unified distribution of configuration changes to all Content Filtering Servers, eliminating the need to configure each server individually.
- ✦ Scalability. One or more additional Content Filtering Servers can be installed as new gateways are added or increased performance is required. PureSight is easily deployed in systems where load-balancing is used to distribute traffic between multiple Content Filtering Servers.

- Reduced risk for single point of failure. The distributed modular structure enables the PureSight Content Filtering servers to continue filtering, even if the PureSight Management Server or the PureSight Log Server fails or other PureSight Content Filtering Servers are down for maintenance.
- Cross platform support. Each module can be installed on a different operating system (Windows or Linux) and each PureSight Content Filtering Server can be installed on a different platform (Squid, MSProxy, or ISA). The selected platform is transparent to the other modules installed.

The role of each of the system modules is described in the next section.

System Modules

The basic system architecture is comprised of three modules that interact to provide a complete content-filtering solution. The functionality of each of the modules is clearly defined as follows:

- **PureSight Management Server** - responsible for configuring and managing all PureSight modules and functions, including the PureSight Log Server and the PureSight Content Filtering Server(s). The PureSight Management Server features an intuitive user-interface that allows the administrator to define and manage the users and filtering policies that support the organization's Internet Acceptable Use Policy.

- **PureSight Content Filtering Server(s)** - responsible for analyzing all Internet traffic on the network. PureSight Content Filtering Servers can be installed on platforms located in the organization's Server Farm or on remote machines. The PureSight Content Filtering Server analyzes all HTTP traffic on the gateway where it is installed, and categorizes the content in real-time. According to the Internet Acceptable Use Policy defined on the PureSight Management Server, the PureSight Content Filtering Server then executes an Allow, Block, Monitor or Warn response, as required.

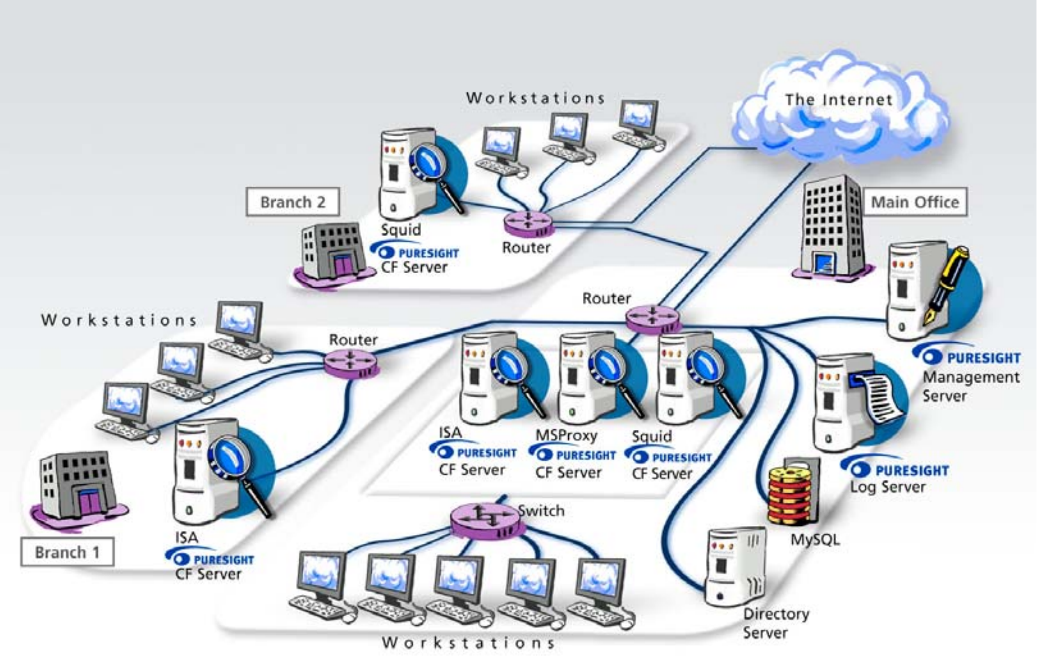
  All PureSight Content Filtering Servers on the network, regardless of their location, are configured by the PureSight Management Server. This system-wide configuration includes the users and filtering policies that support the organization's Internet Acceptable Use Policy. The PureSight Content Filtering Servers also interact with a single PureSight Log Server, which is responsible for logging all of the filtering activity that takes place in the network.
- **PureSight Log Server** - provides real-time tracking, monitoring and accounting information for all Internet activity - the details of all HTTP requests and replies, including time, users and the resulting filtering actions (allow/block/warn).

The PureSight Management Server accesses the data on the PureSight Log Server to generate reports on the sites that were visited, the users that access those sites and other information that helps managers to evaluate employee productivity, bandwidth consumption and Internet usage. A single PureSight Log Server logs the activity for all PureSight Content Filtering Servers in the network, regardless of location or platform to enable generating unified reports for all activity. The PureSight Log Server supports logging to the file system or to an SQL database (MySQL).

These independent modules can be installed together on one machine or on separate machines, on varying combinations of platforms and operating systems. This architecture is highly flexible and customizable, allowing the systems administrator to easily adapt the deployment to the organization's network environment.

Network Architecture Diagram

One possible implementation of the PureSight network architecture is shown in the following diagram:



This example shows PureSight deployed in a network with a headquarters and two remote branch offices.

This network includes one PureSight Management Server for the system-wide configuration of five PureSight Content Filtering Servers and one PureSight Log Server. This system-wide configuration includes the users and filtering policies that support the organization's Internet Acceptable Use Policy.

Internet traffic originating in the Headquarters' workstations is monitored by one of three PureSight Content Filtering Servers located in the PureSight Server Farm. Internet traffic originating in the remote branch workstations is monitored by the PureSight Content Filtering Server located on the branch gateway routers.

Logs are generated by the PureSight Log Server and the log contents are stored in a file system or in an SQL database (MySQL) on a separate server.

PureSight Administration

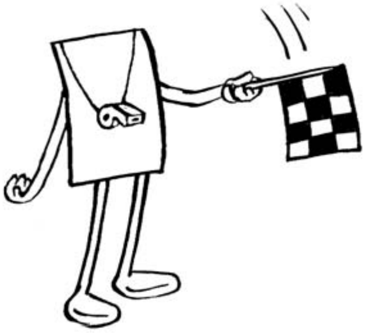
The PureSight Administration tool provides the management tools necessary to configure PureSight's features and settings for all connected PureSight Content Filtering Servers. Using the Administration user interface, PureSight enables administrators and IT managers to:

- **Define Users**: Set up user groups or individual users, and assign them a filtering policy.
- **Define Usage Policies**: Create different policies for different users and/or user groups. Policies for each user or group dictate whether a given category of sites will be allowed, blocked or warned against. Each policy can be implemented on specific days and/or at specific times.
- **Improve Network Bandwidth Management**: Create policies that block specific file types, such as mp3 extensions.
- **Customize Site Filtering**: Create lists of specific Web sites to be allowed or denied, independent of PureSight's categorization. Review blocked sites that were reported by end users and configure PureSight filters according to company policy.
- **Manage PureSight Content Filtering Servers**: Centralize management of multiple PureSight Content Filtering Servers by applying the same configuration settings for users, policies, filters and general settings to multiple PureSight Content Filtering Servers.
- **Define and Configure PureSight Log Server**: PureSight Log Server settings, including the log storage type, log size and log storage location, are conveniently configured in the PureSight Administration tool.

- **Generate Reports**: Generate comprehensive reports of Internet activity and bandwidth activity.
- **Review System Diagnostics:** Detailed analysis of all installed modules including PureSight Content Filtering Servers and PureSight Log Server, provide detailed information regarding server activity and potential problems.

Any management settings and changes made in the PureSight Administration tool are automatically distributed to all connected PureSight Content Filtering Servers and the PureSight Log Server. However, depending on network traffic, there may be a brief delay until all servers are updated with the most recent configuration settings. Changes should be implemented within minutes.

This User's Guide provides directions and explanations for using the PureSight Administration tool.



Chapter 2

Getting Started

About This Chapter

This chapter describes the PureSight Administration tool and the workflow. It contains the following sections:

- **Before You Begin**, page 2-2, provides background information.
- **Accessing PureSight Administration**, page 2-2, describes how to log in to the PureSight Administration.
- **PureSight Administration Page**, page 2-3, describes the components of the PureSight Administration page and introduces the menu options.
- **Default Policy**, page 2-6, describes the PureSight default policy and how it can be changed.
- **System Status**, page 2-7, describes how to stop and start PureSight.
- **PureSight Administration Workflow**, page 2-8, describes the typical workflow for configuring PureSight.

Before You Begin

After successfully installing all PureSight modules (the PureSight Management Server, the PureSight Content Filtering Servers, and, optionally, the PureSight Log Server), initializing the PureSight Content Filtering Servers and setting the software license keys for each of the PureSight Content Filtering Servers, the PureSight filtering mechanism is immediately activated using its default settings, blocking user requests as defined by the default policy. These settings can be refined using the PureSight Administration, so that PureSight can cater to the specific requirements of your organization and support your organization's Internet usage policy.

The PureSight Administration tool is accessed using a Web browser after the installation procedure is complete. (Refer to the appropriate *PureSight Installation Manual* for a description of the installation procedure). Configuration can be done locally or remotely using an Internet Explorer web browser.

NOTE:

A basic PureSight Enterprise installation consists of one PureSight Management Server and a minimum of one PureSight Content Filtering Server. In addition, the installation of one PureSight Log Server is optional.

Accessing PureSight Administration

Only one user at a time can access the PureSight Administration, using the PureSight administrator password.

➢ **To access PureSight Administration:**

1 Enter: **http://**<**PureSight Management Server address**>**:**<**port number**>
in the URL Address bar of your Web browser. The PureSight Management Server address is either the IP

address of the Management Server machine or the machine name. The port number must be the port number that was defined during the installation process for the PureSight Management Server. By default, the PureSight Administration port number is 5000.

2 When the login page is displayed, enter the PureSight administrator password as requested, and then click the **Proceed** button.

After successful login, the PureSight Administration page is displayed, as shown in the following section.

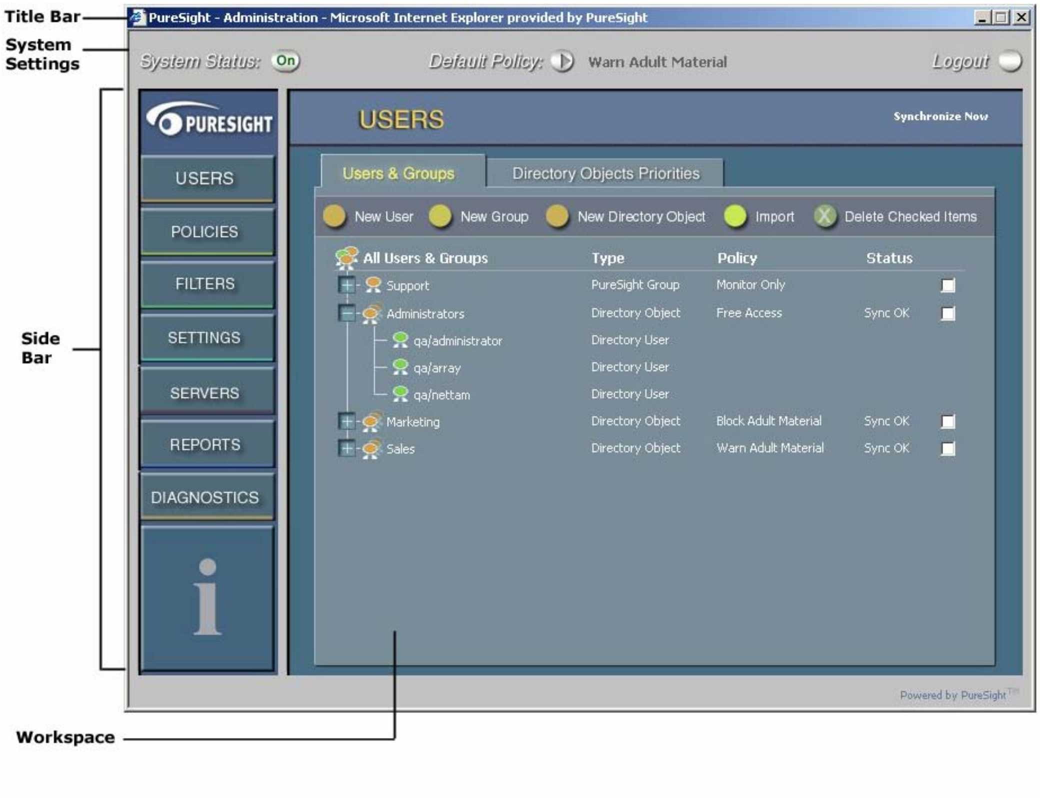
NOTE:

In the event of an unsuccessful login, an error message is displayed. The following are the basic types of error messages that may be encountered and their probable causes:

- Wrong password - indicates that there is an error in the password entered.
- Error connecting to configuration server - indicates that the slapd is down.
- An Internal error has occurred - indicates that the LDAP configuration files may be corrupt or that the slapd is running with a non valid user.

PureSight Administration Page

The PureSight Administration page provides easy access for the user to configure the settings available in PureSight.



All Users & Groups	Type	Policy	Status	
Support	PureSight Group	Monitor Only		□
Administrators	Directory Object	Free Access	Sync OK	□
qa/administrator	Directory User			
qa/array	Directory User			
qa/nettam	Directory User			
Marketing	Directory Object	Block Adult Material	Sync OK	□
Sales	Directory Object	Warn Adult Material	Sync OK	□

Last printed: 2/19/2004 3:26 PM
Last saved: 2/19/2004 10:05 AM

The PureSight Administration page contains the following elements:

✦ **Title Bar**: Displays application information.

✦ **System Settings Area**: Displays PureSight's current working mode and the name of the current default policy, and contains the tools for changing these settings. Refer to *Default Policy*, page 2-6, and *System Status*, page 2-7, for more information. This area also contains a **Logout** button, enabling you to log out of PureSight Administration tool when required.

✦ **Side Bar**: Displays the PureSight menu options and the help area. Clicking a menu option displays the relevant pane in the workspace, enabling you to configure the required functions, as described in *PureSight Administration Tool Menu Options*, below. Placing the cursor over one of the menu options displays information regarding that option in the help area.

✦ **Workspace**: Displays the currently open pane.

PureSight Administration Menu Options

Selecting an option from the menu in the side bar displays the selected option in the workspace. You can then access all the configurable features and settings available for each option.

The menu options are:

✦ **Users**: Enables you to define users and user groups, and to assign policies to these users. Refer to *Chapter 4*, *Defining Users and Groups*, for more information.

✦ **Policies**: Enables you to define new filtering policies and to edit existing ones. Refer to *Chapter 6*, *Defining Policies*, for more information.

- **Filters**: Enables you to refine the PureSight engine filters and bandwidth filters, and to create your own custom filters. Refer to *Chapter 5*, *Defining Filters*, for more information.
- **Settings**: Enables you to configure additional PureSight settings. This includes setting the displayed blocking and warning messages, configuring the Log Server, and configuring the Administrator password. Refer to *Chapter 7*, *Settings*, for more information.
- **Servers**: Enables you to initialize PureSight Content Filtering Servers and to edit server information, as required. Refer to *Chapter 3, Managing PureSight Content Filtering Servers*, for more information.
- **Reports**: Enables you to view reports that provide information on users' Internet activity and bandwidth consumption. Refer to *Chapter 8, Reports*, for more information.
- **Diagnostics:** Displays the System Diagnostics page, which runs system tests to determine the status of all components and modules installed.

Default Policy

PureSight allows you to define a default policy to be used for all users on the network who are not specifically defined in PureSight and associated with a PureSight Policy.

In most organizations, a single policy will cover the filtering requirements for the majority of users. Setting that policy as the default option avoids the need to specifically define those users in the system. Only users requiring a different policy need be defined, thus streamlining the definition process.

The options available for the default policy include all currently defined policies.

➢ **To change the default policy:**

1 Click the **Default Policy** icon in the system settings area of the PureSight Administration page. The *Change Default Policy* window is opened.

2 Select the new default policy from the dropdown list.

3 Click **Change**. The new default policy is displayed in the **Default Policy** field.

System Status

PureSight can be temporarily stopped (disabled), without being removed completely. The current working mode of PureSight is displayed on the **System Status** button. The status can be either **On**, meaning that PureSight is actively filtering, or **Off** indicating that filtering is not active. The **System Status** button toggles between **On** and **Off** to indicate the current working mode.

➢ **To stop and start PureSight:**

1 If you wish to stop PureSight filtering, click the **System Status** button (**On**) in the system settings area.

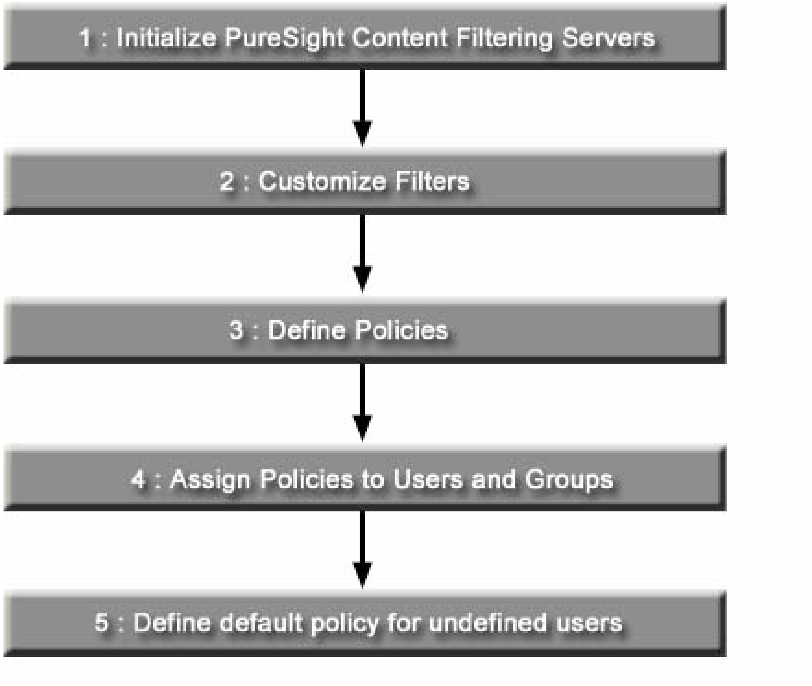
2 If you wish to restart PureSight, click the **System Status** button (**Off**) in the system settings area.

A warning message is displayed.

3 Click **YES**. The **System Status** button toggles to display the new status, **On** or **Off**, as appropriate.

PureSight Administration Workflow

The workflow displayed below gives one example of the PureSight configuration process using PureSight Administration.

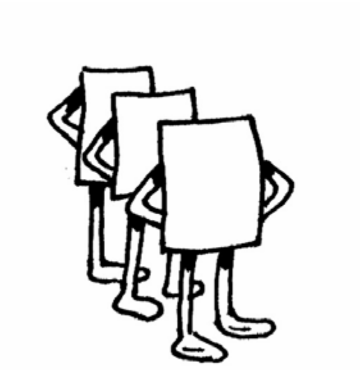

1 : Initialize PureSight Content Filtering Servers
2 : Customize Filters
3 : Define Policies
4 : Assign Policies to Users and Groups
5 : Define default policy for undefined users

The tasks included in the configuration process, and the order in which they are performed, will vary depending on the particular needs of your organization. The following bullets summarize when each step of the workflow applies.

✦ **Step 1: Initialize PureSight Content Filtering Servers**: for each PureSight Content Filtering Server installed, the server must be initialized in order for the server to actively filter Internet access. Once initialized, a license key must be generated.

- **Step 2: Customize filters**: If a new policy is to include custom filters or additional bandwidth filters, you need to define them before the new policy is created. However, you can refine and edit the filters at any time. The changes are automatically updated to all policies that include the relevant filters.
- **Step 3: Define policies**: If a new policy is required to assign to users, you must first create it with at least a policy name and policy type. However, you can edit all policies at any time, whether or not they are assigned to users.

  If the PureSight predefined policies are the only policies required for your organization's users, you can skip steps 2 and 3 and continue the PureSight configuration process at Step 4.
- **Step 4: Assign policies to users and groups**: If different policies are to be assigned to different users and/or user groups in your organization, you must define those users in PureSight. However, if one filtering policy applies for all users on the network, you can define that policy as the default Policy option, without the need to specifically define users.
- **Step 5: Define default policy for undefined users**: If a default filtering policy is required for all users not specifically defined in PureSight, you need to select the appropriate default policy.



Chapter 3

Managing the Content Filtering Servers

About This Chapter

This chapter describes how to initialize PureSight Content Filtering Servers and edit server information and settings. It includes the following sections:

- **Overview**, page 3-2, describes the centralized management of the PureSight Content Filtering Servers.
- **Servers Pane**, page 3-3, describes the information displayed in the main *Servers* pane.
- **Initializing a Server**, page 3-5, describes how to initialize a PureSight Content Filtering Server with the configuration settings defined in the PureSight Management server.
- **Setting the License Key,** page 3-6, describes how to set the license key for the PureSight Content Filtering Server.
- **Editing Server Information**, page 3-9, describes how to edit existing server information.
- **Advanced Server Settings**, page 3-13, describes how to customize the advanced settings of a PureSight Content Filtering Server.

✦ **Deleting a Server**, page 3-16, describes how to delete a PureSight Content Filtering Server.

Overview

The centralized management of multiple PureSight Content Filtering Servers simplifies the server configuration process by applying the same configuration settings for users, policies, filters and general settings to multiple PureSight Content Filtering Servers connected to a single PureSight Management server.

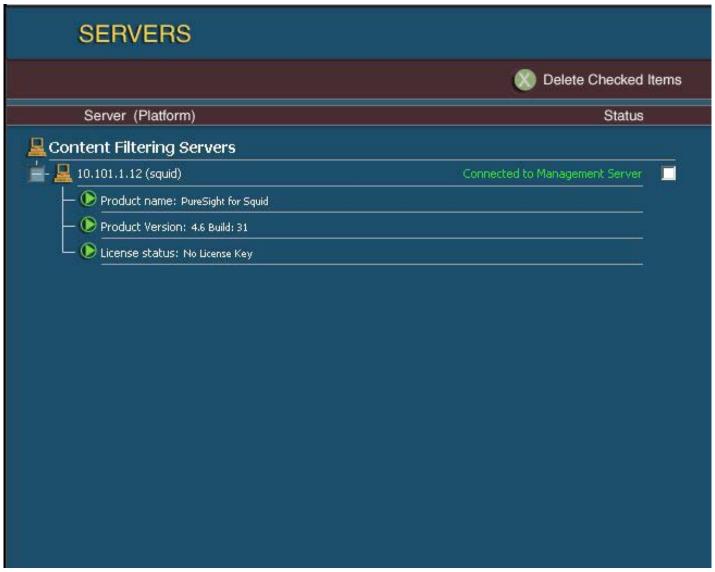
A PureSight Content Filtering Server can be installed on the same machine as the PureSight Management server or on a separate machine. Multiple PureSight Content Filtering Servers may be connected to a single Management Server.

Before a PureSight Content Filtering Server can be activated, the server must be initialized in the system and the license key for the server must be set. The initialization process distributes the system-wide configuration parameters defined in the PureSight Management Server and applies them to the PureSight Content Filtering Server.

Once installed, the PureSight Content Filtering Servers are managed in the *Servers* pane of the PureSight Administration Tool.

Servers Pane

The *Servers* pane, shown below, is accessed from the menu in the Administration side bar by clicking **SERVERS**.



Content Filtering Servers

10.101.1.12 (squid) Connected to Management Server □

Product name: PureSight for Squid

Product Version: 4.6 Build: 31

License status: No License Key

The *Servers* pane displays the following information:

- **Server (Platform)**: The IP address of the PureSight Content Filtering Server and the platform on which the server is to operate (Squid, Microsoft ISA Server, or MS Proxy Server).
- **Status**: The current status of the server, as follows:
  - **Not initialized**: The server has been installed in the system however it has not been initialized.
  - **Connected to Management Server**: The server has been initialized and is connected to the PureSight Management server.
  - **Uninstalled –** The Server was uninstalled prior to being deleted from the PureSight Administration Tool.

Expanding the tree for a specific server displays the following information:

- **Product Name**: The name of the product installed on the server, including the platform on which the server is to operate (Squid, Microsoft ISA Server, or MS Proxy Server).
- **Product Version**: The version and build number of the PureSight Content Filtering Server installed.
- **License Status**: The status of the product license. PureSight Content Filtering Server is active only after registration using a valid license key. The following are the possible license statuses:
  - **Permanent License** - provides full functionality of the PureSight Content Filtering Server for an unlimited period of time. (To obtain a permanent license, contact your local PureSight distributor or email to sales@puresight.com.
  - **Temporary License** - provides full functionality of the PureSight Content Filtering Server for a limited time period days. The remaining duration of the trial period is indicated in the following format: Temporary - Day x of y Days.
  - **No License** - PureSight is not yet functional. A valid license key (temporary or permanent) must be obtained.
  - **License expired** – Temporary license has expired, time limit has been reached**.**
  - **Error in license** – an illegal license key has been provided.

  Both temporary license keys and permanent license keys depend on the hardware, version and platform the system is installed on and therefore cannot be transferred from one filtering server to another.

From the *Servers* pane, you can initialize PureSight Content Filtering Servers, edit server information and delete Content Filtering Servers, as described in the following sections.

Initializing a Server

Before a Content Filtering Server can become operational it must be initialized in the system. The initialization process distributes the system-wide configuration parameters defined in the PureSight Management Server and applies them to the selected PureSight Content Filtering Server.

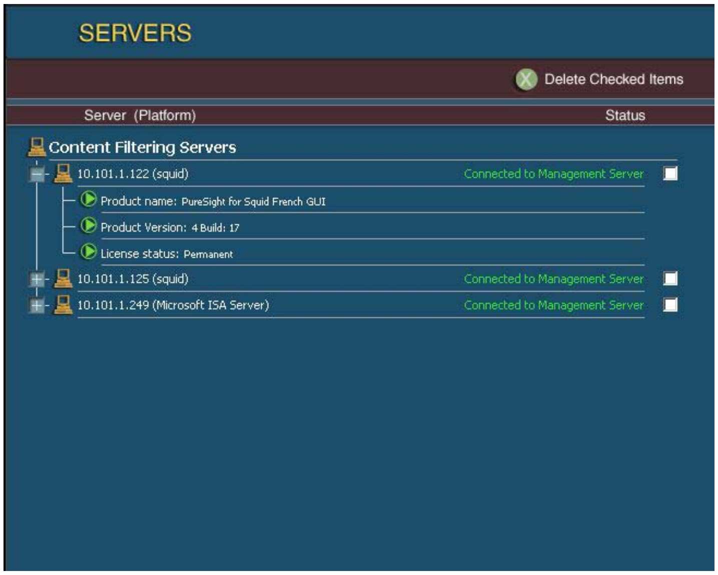
NOTE:

Initializing the server does not start the server! It only updates the server with the Management Server configuration and settings.

➢ **To initialize a new server:**

1 In the *Servers* pane, click the name (IP address) of the server to be initialized. A message is displayed indicating that the server is not connected and asking for authorization to begin the initialization process.

2 Click **OK**. A message is displayed indicating that the server is now connected. The initialization process is performed and configuration data is transferred from the PureSight Management server to the PureSight Content Filtering Server.



Server (Platform)	Status
Content Filtering Servers	
10.101.1.122 (squid)	Connected to Management Server
Product name: PureSight for Squid French GUI	
Product Version: 4 Build: 17	
License status: Permanent	
10.101.1.125 (squid)	Connected to Management Server
10.101.1.249 (Microsoft ISA Server)	Connected to Management Server

NOTE:

Initializing the server may take a few minutes, depending on the size of the configuration data on the PureSight Management Server.

Setting the License Key

The next step after initializing the PureSight Content Filtering Server is to enter a valid license key for the PureSight Content Filtering Server. The license key must be set before the PureSight Content Filtering Server can be activated.

The PureSight license key defines the license type, as follows:

- **Temporary** - a license that is limited to a given period.
- **Permanent** - a license that is valid for an unlimited period of time.

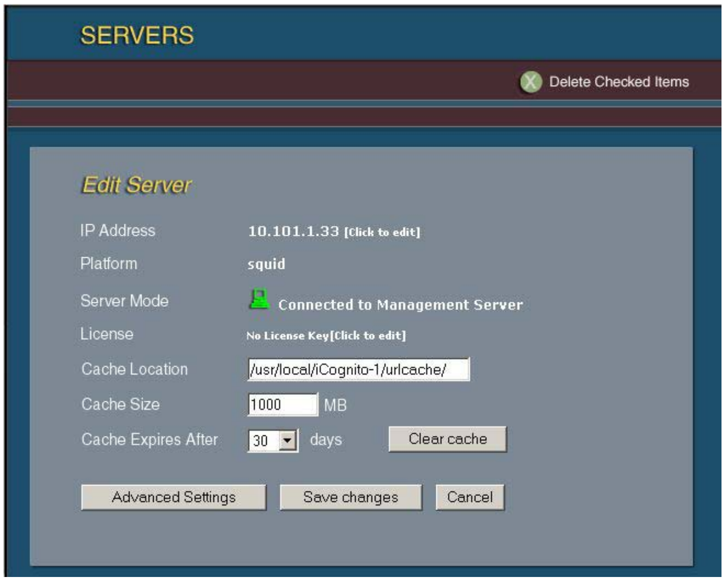
To change a license type, it is necessary to change the license key. The license key is set and edited in the *Edit Server License* pane, which is accessed from the Edit Servers pane.

NOTE:

Both temporary license keys and permanent license keys are hardware dependent and cannot be transferred between machines or hardware environments.

➢ **To set the license key:**

1 In the *Servers* pane, click on the IP address for the required server in the **Servers** tree. The *Edit Server* pane is displayed.



Edit Server

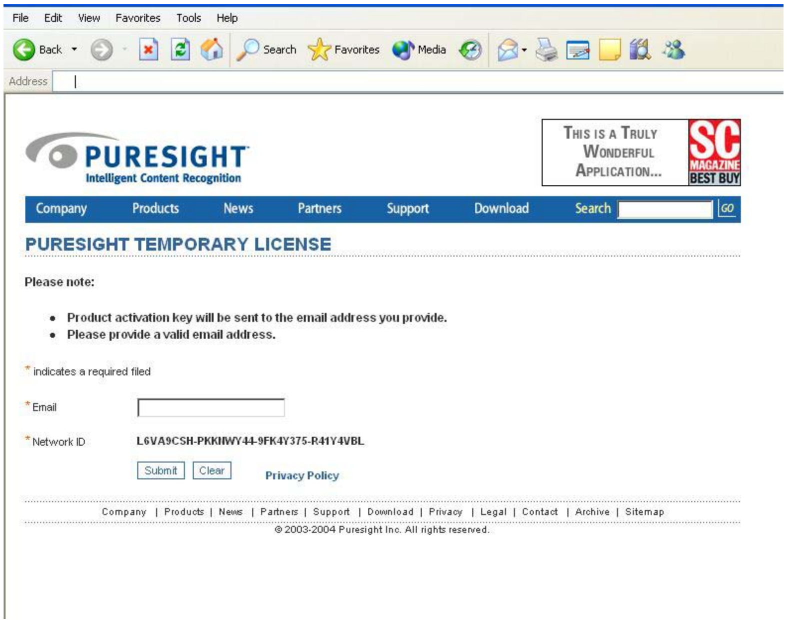
IP Address 10.101.1.33 [Click to edit]
Platform squid
Server Mode Connected to Management Server
License No License Key[Click to edit]
Cache Location /usr/local/iCognito-1/urlcache/
Cache Size 1000 MB
Cache Expires After 30 days

2 Click the **Click to edit** link adjacent to the License field. The *Edit Server License* pane is displayed.

3 Enter the license details provided by your PureSight distributor in the **New License** field,

or,

Click **Get a Temporary License** to register for the Temporary License (30 days only) of PureSight. An Internet form is displayed requesting an **email** address and the **Network ID** of the PureSight Content Filtering Server. The Network ID should already be populated.


File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Address
PURESIGHT
Intelligent Content Recognition
THIS IS A TRULY WONDERFUL APPLICATION...
SC MAGAZINE BEST BUY
Company
Products
News
Partners
Support
Download
Search
GO

PURESIGHT TEMPORARY LICENSE

Please note:

- Product activation key will be sent to the email address you provide.
- Please provide a valid email address.

* indicates a required filed

* Email

* Network ID L6VA9CSH-PKKIWY44-9FK4Y375-R41Y4VBL

Submit
Clear
Privacy Policy
Company | Products | News | Partners | Support | Download | Privacy | Legal | Contact | Archive | Sitemap

© 2003-2004 Puresight Inc. All rights reserved.

4 Enter a valid email address in the **Email** field.

5 If the Network ID is not already populated, enter the Network ID provided in the Edit Server License pane in the **Network ID** field.

6 Click **Submit Form** and close the browser window displaying the *Register PureSight* page. The *Edit Server License* pane is redisplayed.

7 An email will be sent to the designated email address with the license information. Copy and paste the temporary license key into the **New License** field in the PureSight Administration Tool.

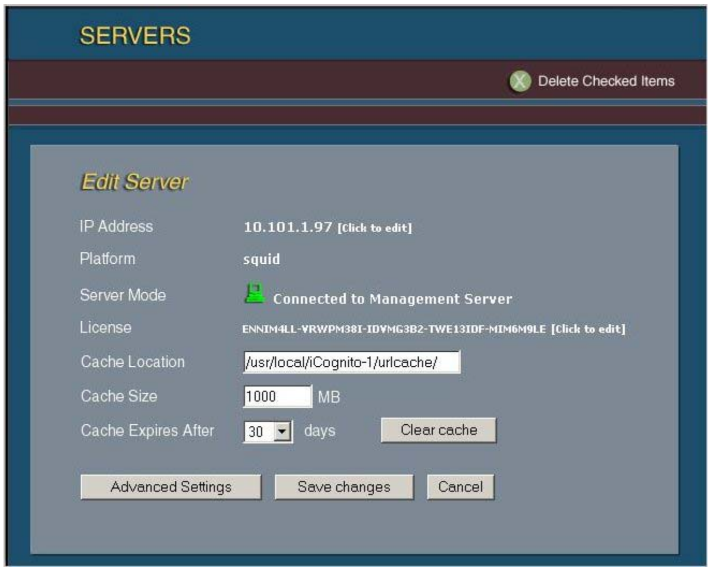
8 Click **Save changes** in the *Edit Server License* pane. The *Edit Server* pane is redisplayed.

9 Click **Save changes** in the *Edit Server* Pane. The licensing information is updated.

After setting the software license key for each of the servers, the PureSight filtering mechanism can now be started for the first time using its default settings, blocking user requests as defined by the default policy.

Editing Server Information

The *Edit Server* pane, shown below, enables you to edit the server information.



SERVERS

Edit Server

IP Address 10.101.1.97 [Click to edit]

Platform squid

Server Mode Connected to Management Server

License ENNIM4LL-VRWPM38I-IDVMG3B2-TWE13IDF-MIM6M9LE [Click to edit]

Cache Location /usr/local/iCognito-1/urlcache/

Cache Size 1000 MB

Cache Expires After 30 days

The *Edit Server* pane displays the following information:

- **IP Address**: The IP address of the server. (The server's IP address should be changed only if the IP address of the PureSight Content Filtering machine has been physically changed.)
- **Platform**: The platform on which the server operates (Squid, Microsoft ISA Server, or MS Proxy Server). (The Platform field cannot be edited.)
- **Server Mode**: The current status of the server.
- **License**: The license key set for the server. (The license key is changed only when it is necessary to activate a PureSight Content Filtering server permanently or for a temporary period.)
- **Cache Location**: The path to the location of the URL cache. The URL Cache is used to save classifications of recently classified requests.

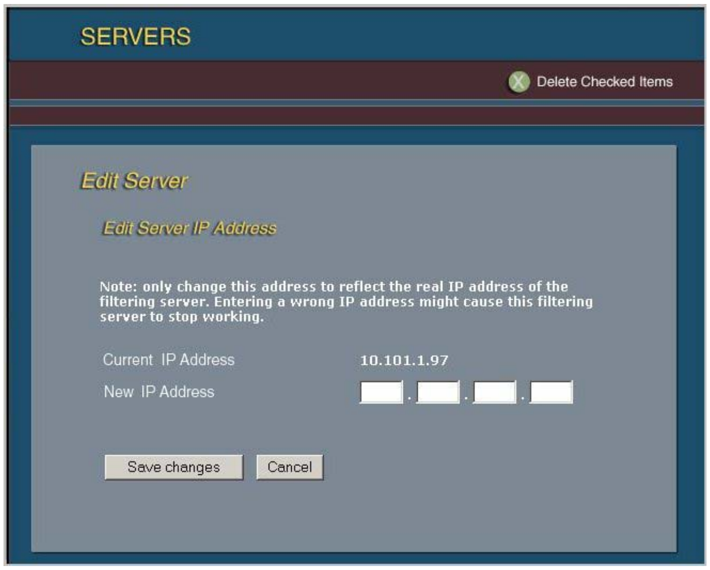
  Cache Size: The cache size (in megabytes). This is the maximum size of the cache on the hard disk. When maximum size is reached new entries to the cache will overwrite existing ones.
- **Cache Expires After**: The length of time before classifications in the URL Cache expire (in days). After the specified time passes, a request for the same page will be reclassified to support content changes in the requested page.

The *Edit Server* pane also includes the following buttons:

- **Clear cache**: Enables you to clear the URL cache on demand, regardless of the timing or size of the cache.
- **Advanced Settings**: Enables you to view and edit the advanced server settings. Refer to *Advanced Server Settings*, page 3-13 for more information.)

➢ **To edit server information:**

1. In the *Servers* pane, click on the IP address for the required server in the **Servers** tree. The *Edit Server* pane is displayed.
2. Edit the IP address as follows (if required):
   - ❖ Click the **Click to Edit** link adjacent to the IP Address field. The *Edit Server IP Address* pane is displayed.



Note: only change this address to reflect the real IP address of the filtering server. Entering a wrong IP address might cause this filtering server to stop working.

Current IP Address 10.101.1.97

New IP Address . . .

   - ❖ Enter the new IP address in the **New IP Address** field.

> **NOTE:**
> Change the server's IP address only if the IP address of the PureSight Content Filtering machine has been physically changed. The new address provided must be the IP address of an existing PureSight Content Filtering Server. The physical IP address of the PureSight Content Filtering Server machine is not changed. Changing the Server IP Address in the PureSight Administration distributes configuration data to the server whose IP address is now entered.

   - ❖ Click **Save changes**. The IP address is updated. The *Edit Server* pane is redisplayed.

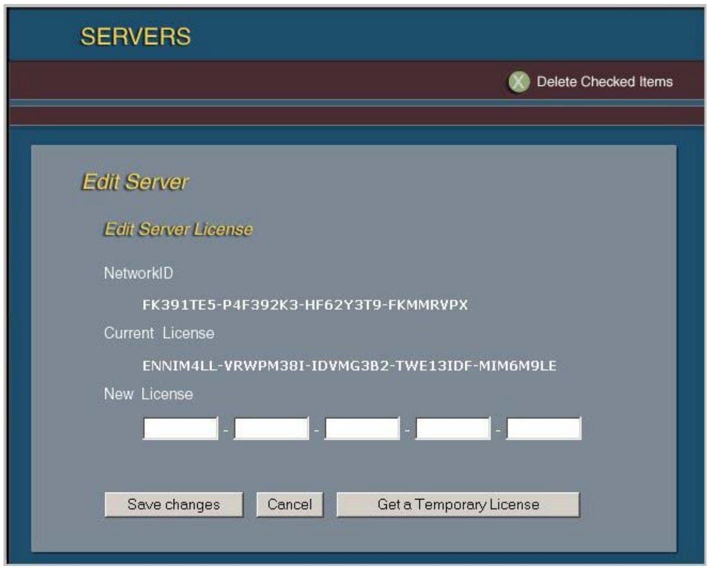
3 Edit the licensing information as follows (if required):

❖ Click the **Click to Edit** link adjacent to the License field. The *Edit Server License* pane is displayed, showing the server's Network ID and current license information.

NOTES:

The license key is changed when it is necessary to activate a PureSight Content Server permanently or for a temporary period.

Both temporary license keys and permanent license keys are hardware dependent and cannot be transferred between machines or hardware



NetworkID

FK391TE5-P4F392K3-HF62Y3T9-FKMMRVPX

Current License

ENNIM4LL-VRWPM38I-IDVMG3B2-TWE13IDF-MIM6M9LE

New License

❖ Enter the license details provided by your PureSight distributor in the New License field,

or,

Click **Get a Temporary License** to register for the Trial Version of PureSight. (Refer to *Setting the License Key*, page 3-6, for details on how to obtain a temporary license.)

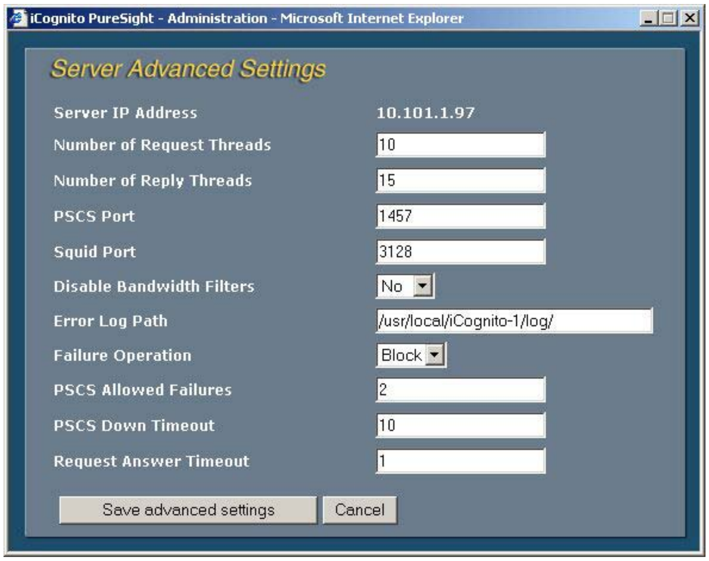
❖ Click **Save changes** in the *Edit Server License* pane. The *Edit Server* pane is redisplayed.

4 Edit additional information in the *Edit Server* pane, as required.

5 Click **Save changes**. The server information is updated.

Advanced Server Settings

Additional, more advanced server settings are displayed in the *Server Advanced Settings* pane. Depending on the platform of the HTTP server, the appropriate configuration settings will be displayed. The Squid platform Advanced Settings are shown below.


iCognito PureSight - Administration - Microsoft Internet Explorer

Server Advanced Settings

Server IP Address	10.101.1.97
Number of Request Threads	10
Number of Reply Threads	15
PSCS Port	1457
Squid Port	3128
Disable Bandwidth Filters	No
Error Log Path	/usr/local/iCognito-1/log/
Failure Operation	Block
PSCS Allowed Failures	2
PSCS Down Timeout	10
Request Answer Timeout	1

Save advanced settings
Cancel

NOTES:

Although advanced server settings can be edited, it is recommended that the default settings not be changed.

The *Server Advanced Settings* pane may display the following information:

- **Server IP Address**: The IP address of the server.
- **Number of Request Threads**: The number of threads handling the HTTP request stage. This is used for tuning the system in high load situations. Squid platform only.

- **Number of Reply Threads**: The number of threads handling the HTTP reply stage. This is used for tuning the system in high load situations. Squid platform only.
- **PSCS Port**: The port used by the PureSight Content Server (PCSC) that handles all replies. Squid platform only.
- **Squid Port**: The port used by Squid to receive HTTP requests. Squid platform only.
- **Disable Bandwidth Filters**: Setting this value to Yes will cause the PureSight Request Handler (PSRH) to allow all requests for non-HTML sites (e.g., pictures) and therefore disable the PureSight bandwidth filtering feature. This should improve performance (known file extensions are not examined), however, requests will not be logged and therefore will not be included when reports are generated. (Refer to *Chapter 5, Defining Filters* for more information on bandwidth filters.) Squid platform only.
- **Error Log Path**: The path to the PureSight Error logs (both PSRH and PSCS). Squid platform only.
- **Failure Operation**: The action to be taken by the system in the event of failure. When a system failure occurs in the PureSight content filter, or if the system is loaded beyond its ability to filter, the system tries to avoid total disabling of surfing and constantly attempts to restore itself. When a failure situation is reached, all pages may be either blocked or allowed. Squid platform only.
- **PSCS Allowed Failures**: The number of consecutive requests that can time out in the PSRH before a failure condition is pronounced. Squid platform only.
- **PSCS Down Timeout**: The timeout before the PSRH tries again to contact the PSCS when the PSCS is pronounced to be in a failure condition. Squid platform only.

- **Request Answer Timeout**: The amount of time that the PSRH will wait for a reply from the PSCS before pronouncing a single failure (URL delivered according to failure operation). Squid platform only.
- **ISA Port:** The HTTP port of the ISA cache server. ISA platform only.

➢ **To edit advanced settings:**

1. In the *Servers* pane, click the required server in the **Servers** tree.
2. The *Edit Server* pane is displayed, containing the previously defined information for the server.
3. Click the **Advanced Settings** button. The *Server Advanced Settings* pane is displayed.
4. Edit the server settings, as required.
5. Click **Save advanced settings**. The *Edit Server* pane is redisplayed.
6. Click **Save changes**. The changes are saved in the database.

NOTE:

If your Squid proxy is not running on the default HTTP port you must edit the Squid port prior to starting the PureSight Content Filtering Server.

Deleting a Server

Servers can be deleted from the *Servers* pane at any time, for example, if a server has been disconnected from the system.

➢ **To delete a server:**

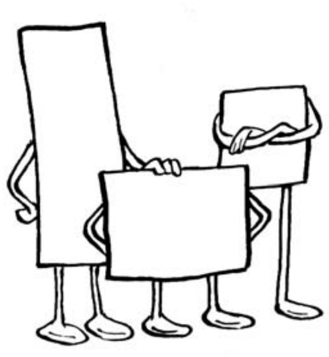
1 Select the appropriate checkbox at the right end of the row for the server to be deleted.

2 Click the **Delete Checked Items** button. A warning message is displayed.

3 Click **OK**. The checked server is deleted from the **Servers** tree.

NOTE:

Deleting a server does not stop or uninstall the PureSight Content Filtering Server.



Chapter 4

Defining Users and Groups

About This Chapter

This chapter describes how to assign policies to new users and user groups, and edit existing users and groups. It includes the following sections:

- **Overview**, page 4-2, provides an overview of defining users and groups.
- **Users Pane**, page 4-4, describes the information displayed in the main *Users* pane.
- **Adding New Groups**, page 4-5, describes how to define new groups.
- **Editing Groups**, page 4-6, describes how to edit existing group information.
- **Adding New Users**, page 4-6, describes how to define new users and assign them to groups.
- **Editing Users**, page 4-10, describes how to edit existing user information.
- **Adding New Directory Objects,** page 4-10, describes how to define directory objects as PureSight groups.
- **Importing Users**, page 4-12, describes how to import directory users from a text file.

- **Deleting Users and Groups**, page 4-14, describes the deletion process for users and groups.
- **Setting Directory Objects priorities,** page 4-14, describes how to change priorities of directory object groups.

Overview

PureSight enables you to define users or groups of users within your organization, and to then assign specific filtering policies to those users and groups.

Users are identified by an IP address or subnet, or by a directory user name. The policies available are all policies defined in PureSight. If you want to define new policies, you should proceed to *Chapter* 6, *Defining Policies*, before returning to this chapter to define users and groups.

PureSight also supports definition of Directory Objects. Directory Objects are containers of users: domains, organizational units or directory groups, which are defined on the Directory Server and are associated with a PureSight group. This group is called a Directory Object group and is not editable, i.e. all users of the group are automatically defined according to the definition of the Directory Object on the Directory Server. This synchronization process between the PureSight Directory Object groups and the directory server occurs at a predefined interval according to the configuration of the Directory Server settings. Refer to *Chapter 7, Settings*, for additional information. It is also possible to invoke synchronization by clicking **Synchronize Now**. If a directory user belongs to more than one Directory Object group, then the user is associated to the group with the highest priority. Priorities of Directory Object groups are defined in the Directory Objects Priorities tab. All the users of a directory object group will be displayed in the Directory Object's user list. Users who are not associated with the specific group because they belong to a higher priority group will be marked with a grey icon.

NOTE:

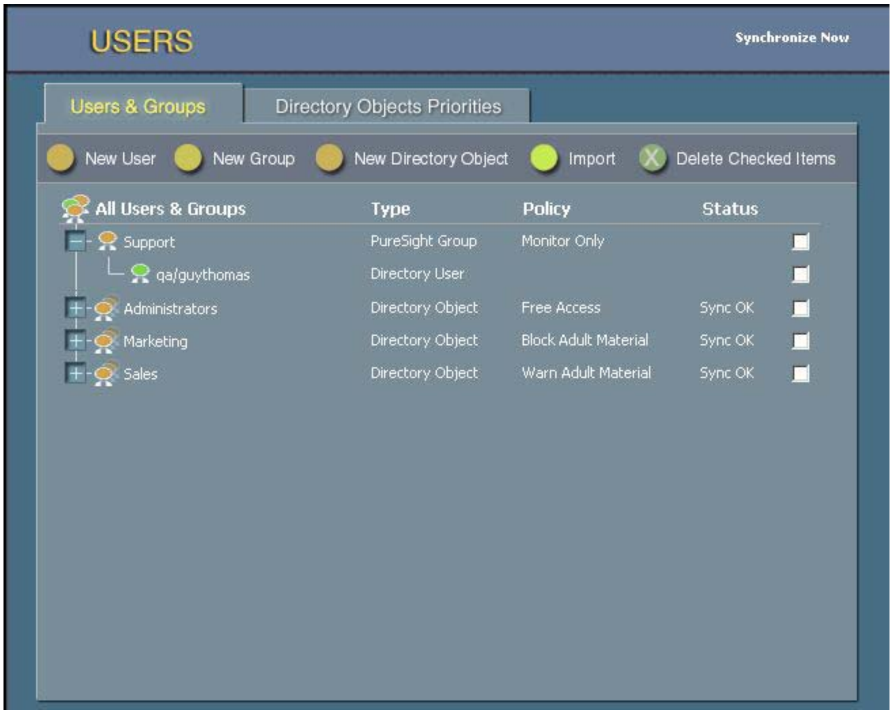
Directory users that were specifically defined and are not part of a Directory Object group have a higher priority than any Directory Object group.

It is not possible to manually add the same directory user to a number of different PureSight groups. However, the same directory user may belong to a PureSight group and to a number of Directory Object groups.

All users that are not specifically defined in the *Users* pane are automatically filtered according to the defined default policy. Refer to *Chapter 2*, *Getting Started*, for more information.

Users Pane

The main *Users* pane, shown below, is accessed from the menu in the Administration side bar by clicking **Users**.



All Users & Groups	Type	Policy	Status	
Support	PureSight Group	Monitor Only		☐
qa/guythomas	Directory User			☐
Administrators	Directory Object	Free Access	Sync OK	☐
Marketing	Directory Object	Block Adult Material	Sync OK	☐
Sales	Directory Object	Warn Adult Material	Sync OK	☐

The *Users* pane displays the following information:

- **Group/User**: Expanding the **All Users & Groups** tree displays all defined users, user groups and Directory Object groups.
- **User Type**: This column identifies the defined users as a single **IP** address, a **Subnet** range of user IP addresses or a **Directory user** name.
- **Policy**: This column identifies the policy assigned to the user or user group. All users within a group automatically inherit the policy assigned to the group.

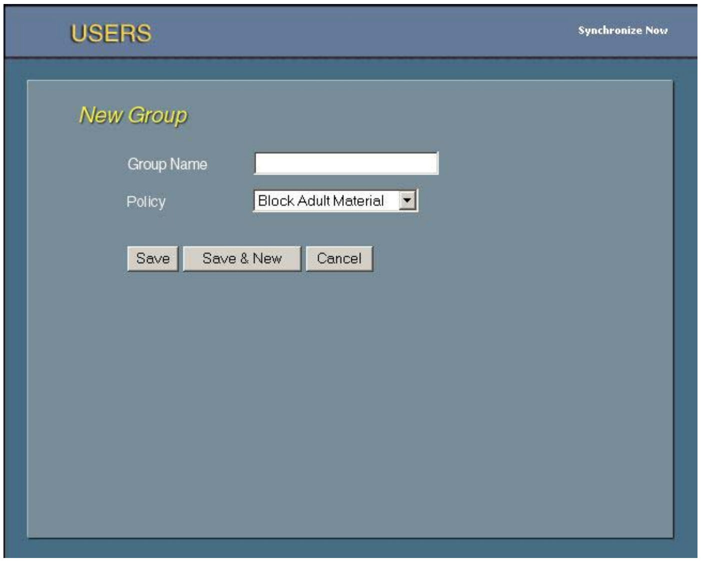
From the *Users* pane, you can add and edit groups, add and edit users, and delete groups and users, as described in the following sections.

Adding New Groups

To create a new group, you first define the group name and assign a policy to that group. You can then assign as many users as you want to the group.

➢ **To add a new PureSight group:**

1 In the *Users* pane, click the **New Group** button. The *New Group* pane is displayed.



Group Name
Policy: Block Adult Material

2 Enter the new group name in the **Group Name** field.

3 Click the arrow in the **Policy** field and select a policy for the group from the dropdown list.

4 Click **Save** to add the group and return to the *Users* pane,

or

Click **Save & New** to add another new group.

Each new group is automatically added to the **All Users & Groups** tree in the *Users* pane.

Editing Groups

The *Edit Group* pane enables you to edit the information in the *New Group* pane.

➢ **To edit a group:**

1 In the *Users* pane, click the required group in the **All Users & Groups** tree.

2 The *Edit Group* pane is displayed, containing the previously defined information for the group. Enter the changes in the appropriate fields and save, as described in *Adding New Groups*, page 4-5.

Adding New Users

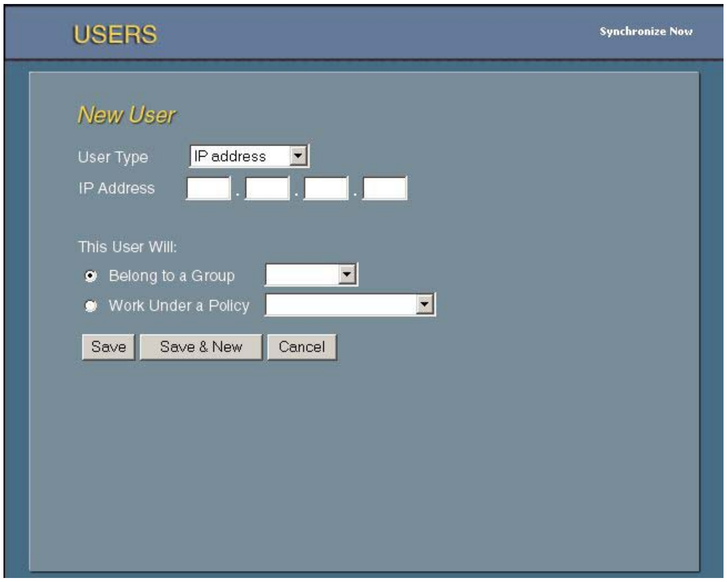
A new user can be a single IP address, a Subnet (range of IP addresses) or a directory user, and can be assigned a policy directly or be assigned to a group. All users in a group inherit the policy defined for that group.

NOTE:

Each user can only be defined once. Make sure that subnets do not overlap other subnets or individual defined IP addresses.

➢ **To add a new user(s):**

1 In the *Users* pane, click the **New User** button. The *New User* pane is displayed.

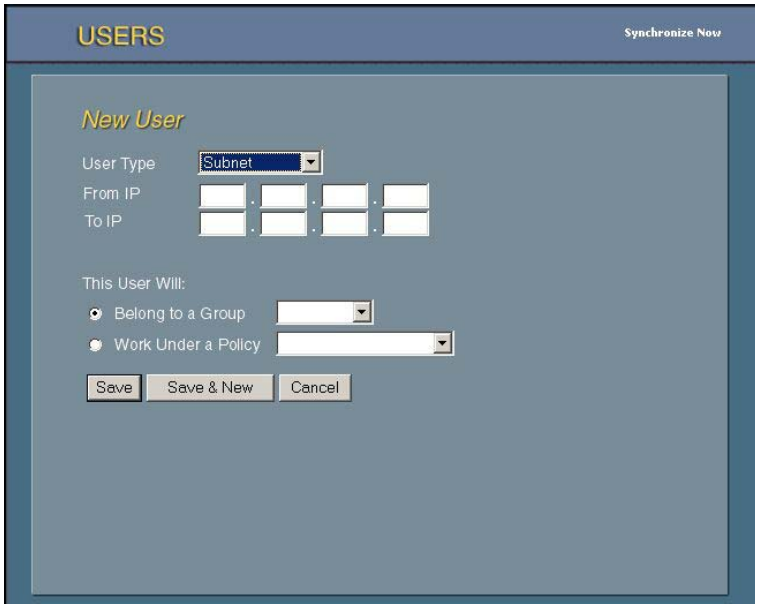


2 Select a **User Type** in the dropdown box.

a. If you selected **IP Address** as the user type, enter the new user's IP address in the **IP Address** field.

or

b. If you selected **Subnet** in the **User Type** dropdown box then enter the relevant range start and end IP addresses in the **From IP** and **To IP** fields.



USERS

New User

User Type: Subnet

From IP . . .

To IP . . .

This User Will:

● Belong to a Group

○ Work Under a Policy

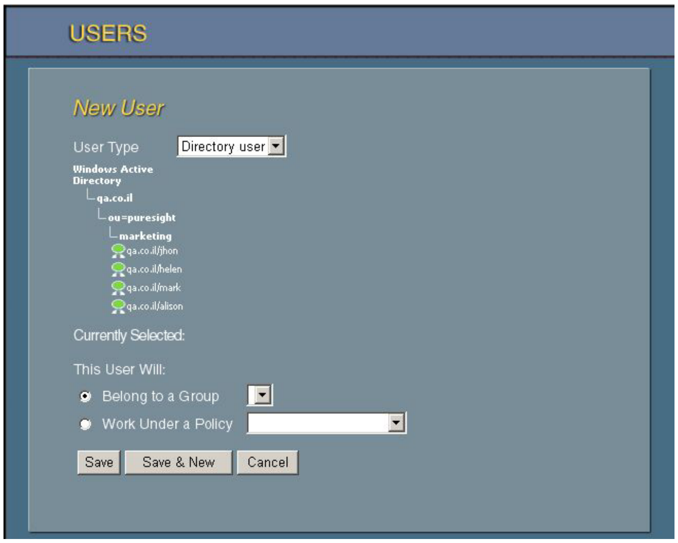
or

c. If you selected **Directory user** in the **User Type** dropdown box, a username must be entered. You can either type in the username or browse for the user in the User Directory according to the Directory Settings defined. Refer to *Chapter 7, Settings*, for more information about directory server settings.

NOTE:

Directory Server settings must be set before adding a new directory user. Refer to *Chapter 7, Settings*, for information about directory server settings.

i. Navigate through the Directory groups and users to select the required user.



USERS

New User

User Type: Directory user

Windows Active Directory
└ **qa.co.il**
  └ **ou=puresight**
    └ **marketing**
      qa.co.il/jhon
      qa.co.il/helen
      qa.co.il/mark
      qa.co.il/alison

Currently Selected:

This User Will:

● Belong to a Group
○ Work Under a Policy

ii. The Selected user is displayed next to the **Currently Selected** title.

3 To assign the new user to an existing group, select the **Belong to a Group** radio button in the **This User Will** area, and then select the group from the dropdown list,

or

To assign a policy directly to the user(s), select the **Work Under a Policy** radio button in the **This User Will** area, and then select the policy from the dropdown list.

4 Click **Save** to add the new user(s) and return to the *Users* pane,
or
Click **Save & New** to add another new user(s).

Each new user is automatically added to the **All Users & Groups** tree in the *Users* pane.

Editing Users

The *Edit User* pane enables you to edit the information entered in the *New User* pane.

➢ **To edit a user:**

1 In the *Users* pane, click the required user in the **All Users & Groups** tree.

2 The *Edit User* pane is displayed, containing the previously defined information for the user. Enter the changes in the appropriate fields and save, as described in *Adding New Users* page 4-6.

Adding New Directory Objects

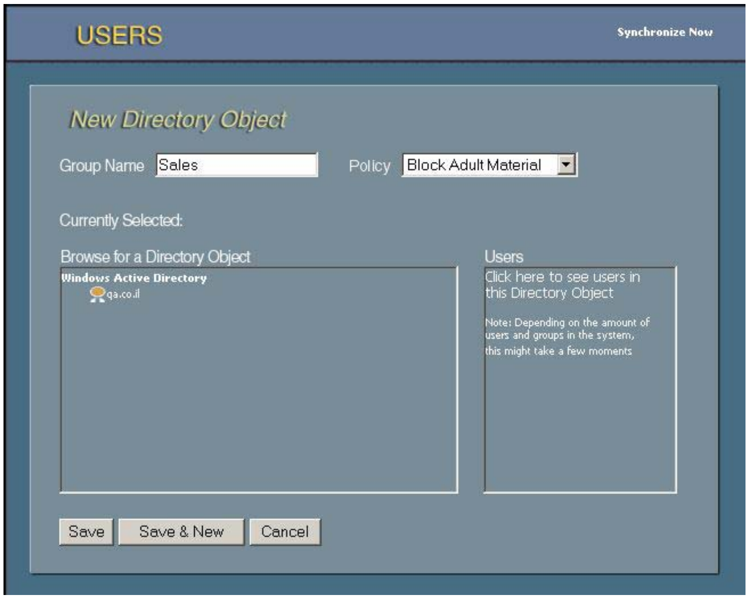
A directory object is a container of users as defined in the Directory Server. A Directory Object can either be a Domain, an Organizational Unit or a directory Group. The definitions of all three containers are located in the Directory Settings. Refer to *Chapter 7, Settings*, for more information on Directory Settings. Defining a Directory Object associates a PureSight group and policy with all the directory users of the selected container as defined in the Directory Server. Any change applied to the Directory Server regarding users association with a Directory Object, is automatically reflected in PureSight when assigning policies to users.

In order to avoid conflict between users associated with a number of different Directory Objects, a priority is defined between the different Directory Objects. A user will be associated to the group with the highest priority. Refer to *Setting Directory Objects Priorities* page 4-14for more information.

Pane examples are provided for Windows Active Directory. The process is similar for other directory servers.

➢ **To add a Directory Object:**

1 In the *Users* pane, click the **New Directory Object** button. The *New Directory Object* pane is displayed.



Group Name: Sales

Policy: Block Adult Material

Click here to see users in this Directory Object

Note: Depending on the amount of users and groups in the system, this might take a few moments

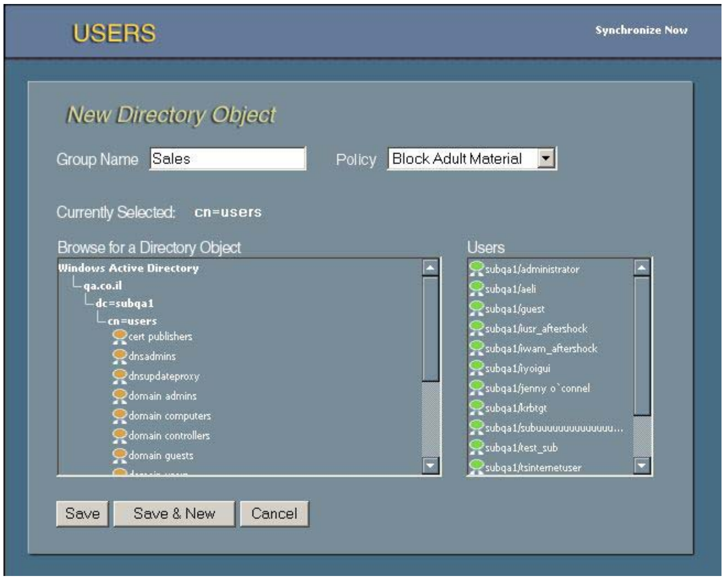
3 Enter the new group name in the **Group Name** field.

4 Click the arrow in the **Policy** field and select a policy for the group from the dropdown list.

5 Navigate through the Directory tree on the left and select the Directory Object with which this group is associated. The Directory Object selected is displayed next to the **Currently Selected** title. The Users of the selected Directory Object can be displayed in the right pane by clicking on the appropriate link in the left pane.

NOTE:

Retrieval of users of a directory object may take some time, depending on the size of the directory object.



Group Name: Sales

Policy: Block Adult Material

Currently Selected: cn=users

6 Click **Save** to add the Directory Object and return to the *Users* pane,

or

Click **Save & New** to add another new Directory Object.

7 Each new Directory Object group is automatically added to the **All Users & Groups** tree in the *Users* pane

Importing Users

Directory users can be imported from a text file into a PureSight group and be assigned the filtering policy used for that group. The format of the text file is so that each username is in the beginning of a new line. For example, a text file named import.txt can contain the following:

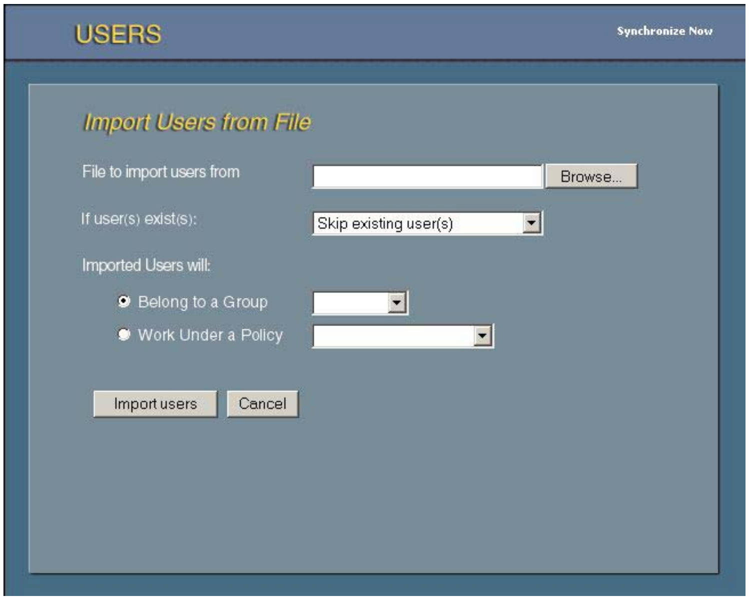
john.k

jerry.p

hellen.o

➢ **To import the users from a text file:**

1 In the *Users* pane, click the **Import** button. The *Import Users from File* pane is displayed.



Import Users from File

File to import users from

If user(s) exist(s): Skip existing user(s)

Imported Users will:

● Belong to a Group

○ Work Under a Policy

2 Enter the full path to the import file in the **File to import users from** field or click **Browse** to browse for the file.

3 Select what you want to do with directory users that are already defined in the PureSight policy manager. You can either skip these users, and add all the rest, or abort the import command altogether.

4 To assign the new users to an existing group, select the **Belong to a Group** radio button in the **This User Will** area, and then select the group from the dropdown list,

or

To assign a policy directly to the user(s), select the **Work Under a Policy** radio button in the **This User Will** area, and then select the policy from the dropdown list.

5 Click **Import users** to add the directory users and return to the *Users* pane.

Deleting Users and Groups

Defined users and user groups can be deleted from the *Users* pane at any time. Deleting a user group also deletes all the users defined for that group.

➢ **To delete a user or group:**

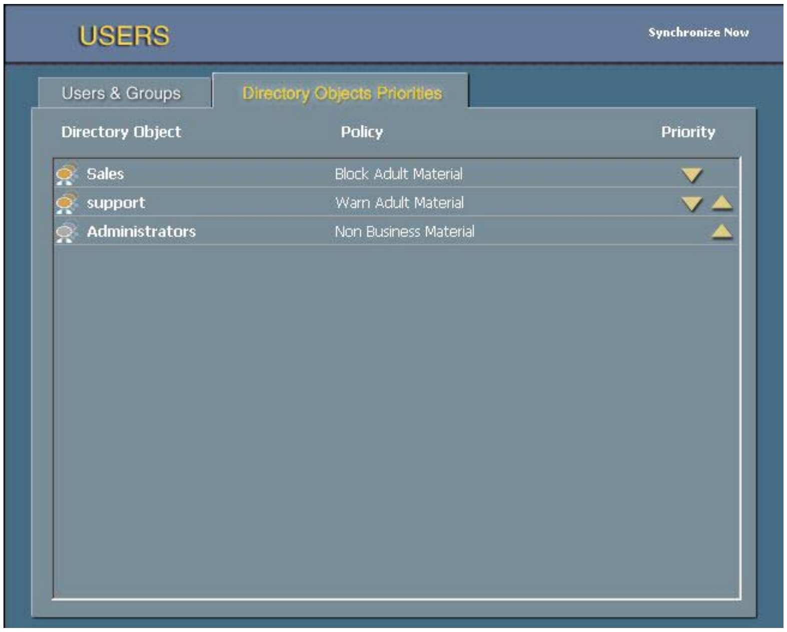
1. Select the appropriate checkboxes at the right end of each row.
2. Click the **Delete Checked Items** button. A warning message is displayed.
3. Click **OK**. The checked users and groups are deleted from the **All Users & Groups** tree.

Setting Directory Objects Priorities

Directory Objects are displayed in the Directory Objects Priorities tab based on their priority, the highest priority directory group is displayed on top. Users belonging to a number of different directory object groups will be associated, in PureSight, to the directory object group with the highest priority.

➢ **To set directory objects priorities:**

1. In the *Users* pane, click the **Directory Objects Priorities** tab.



Directory Object	Policy	Priority
Sales	Block Adult Material	▼
support	Warn Adult Material	▼ ▲
Administrators	Non Business Material	▲

2 To set a higher priority for a directory object group, press the **up** arrow for that directory object. To set a lower priority for a directory object group, press the **down** arrow for that directory object.

Chapter 5

Defining Filters

About This Chapter

This chapter describes the PureSight filters and how to refine and customize them. It includes the following sections:

- **Overview**, page 5-2, provides an overview of the PureSight filters.
- **Engine Filters**, page 5-2, describes the engine filters and how to refine them.
- **Bandwidth Filters**, page 5-8, describes the bandwidth filters and how to add and edit file extensions.
- **Custom Filters**, page 5-11, describes the custom filters and how to create, edit, and import or export from them.
- **Reported URLs,** page 5-15, describes how to review URLs which have been reported by end users as being blocked.

Overview

PureSight filters define the type of information that can be blocked, allowed or warned against in the different filtering policies. PureSight contains three different types of filters:

- **Engine Filters**: Internet categories that the PureSight engine can identify, and block or warn accordingly.
- **Bandwidth Filters**: Bandwidth consuming files that can be blocked.
- **Custom Filters**: User-defined lists of sites to be blocked, allowed or warned against. These lists are independent of PureSight's categorization process.

To assist in customizing PureSight filters, it is possible to enable URL reporting in the PureSight blocking and warning messages. Refer to *Chapter 7, Settings* for information on how to enable URL reporting. If enabled, users can report URLs which have been blocked to the Administrator. These URLs will appear in the Reported URLs where the Administrator can decide whether to allow future access to the specific URL or not by refining the appropriate filter.

The main *Filters* pane containing the **Engine**, **Bandwidth, Custom Filters** and **Reported URLs** tabs is accessed from the menu in the Administration side bar by clicking **FILTERS**.

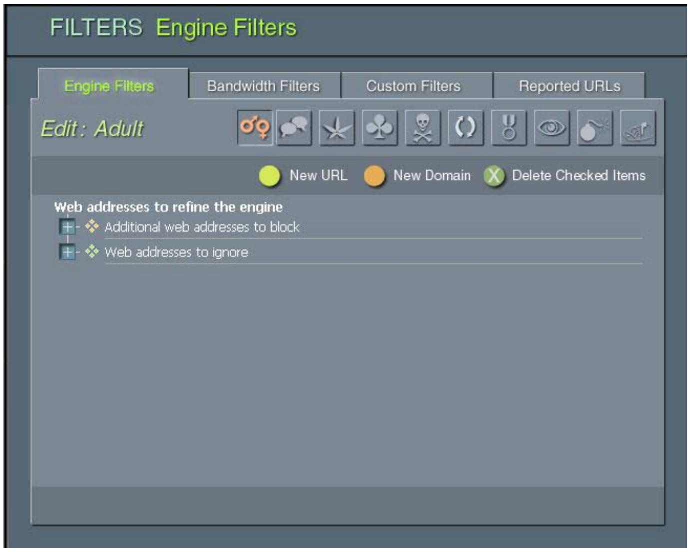
Engine Filters

The engine filters are comprised of general categories of Internet sites that PureSight's ACR technology can automatically recognize on-the-fly, for example, **Adult**, **Gambling** or **Drugs**. Each of these engine filters can be refined according to the specific requirements of your organization. This refinement is achieved by adding Web addresses that are currently associated with a specific category, but should not be. For example, if PureSight is blocking an adult site that you want to permit user access to, you can define the site as a Web address to be ignored in the Adults engine filter.

➢ **To open the Edit Engine Filters pane:**

✦ The **Engine Filters** tab is displayed by selecting the appropriate tab in the *Filters* pane. Clicking one of the icons, for example **Adult** , opens the appropriate *Edit* pane for that engine filter category.

The example below displays the *Edit: Adult* pane.



Each engine filter *Edit* pane contains a **Web addresses to refine the engine** tree. The expanded tree displays branches for **Domains** and **URLs** under **Additional Web addresses to block**, and branches for **Domains** and **URLs** under **Web addresses to ignore**. When a new URL or domain is added, it is displayed under the appropriate branch.

TIP:

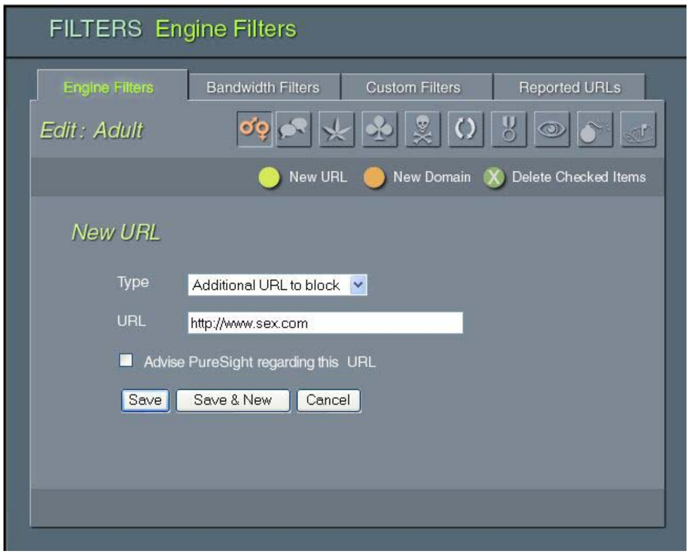
URLs and domains can be deleted from the engine filter *Edit* pane by selecting the appropriate checkboxes and clicking the **Delete Checked Items** button.

Adding URLs

New URLs to be blocked or ignored can be added to any of the engines. There is no limit to the number of URLs that can be added.

➢ **To add a URL:**

1 In the *Edit* pane for the appropriate engine category, click the **New URL** button. The *New URL* pane is displayed. The example below shows the *New URL* pane for the Adult engine filter.



FILTERS Engine Filters

Edit: Adult

New URL

Type: Additional URL to block

URL: http://www.sex.com

☐ Advise PureSight regarding this URL

2 In the **Type** field, select **Additional URL to ignore** or **Additional URL to block** from the dropdown list.

3 Enter the URL address in the **URL** field, for example, **http://www.xxx.com**.

NOTE:

An error message is displayed if the URL format entered is incorrect.

4. Select the **Advise PureSight regarding this URL** checkbox if this is a URL that PureSight has mistakenly classified or misclassified.
5. Click **Save** to add the URL and return to the engine filter *Edit* pane,

   or

   Click **Save & New** to add another new URL.

   Each new URL is automatically added to the tree in the engine filter *Edit* pane, under **Additional web addresses to block** or **Web addresses to ignore**.

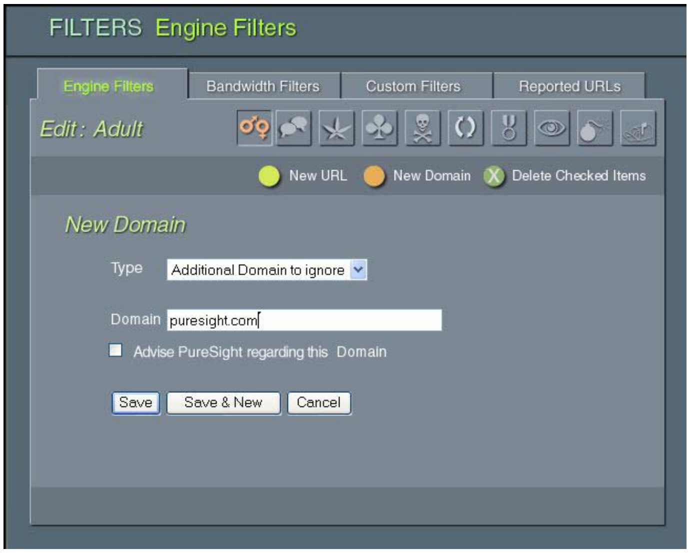
Adding Domains

New domains to be blocked or allowed can be added to any of the engines. Any HTTP request for a URL under the specified domain will be blocked or allowed accordingly.

There is no limit to the number of domains that can be added.

➢ **To add a domain:**

1 In the *Edit* pane for the appropriate engine category, click the **New Domain** button. The *New Domain* pane is displayed. The example below shows the *New Domain* pane for the Adult engine filter.



Type: Additional Domain to ignore

Domain: puresight.com

□ Advise PureSight regarding this Domain

2 In the **Type** field, select **Domain to block** or **Domain to ignore** from the dropdown list.

3 Enter the domain in the **Domain** field, for example, **xxx.com**.

NOTE:

An error message is displayed if the domain format entered is incorrect.

4 Select the **Advise PureSight regarding this Domain** checkbox if this is a domain that PureSight has mistakenly classified or misclassified.

5 Click **Save** to add the domain and return to the engine filter *Edit* pane,

or

Click **Save & New** to add another new domain.

Each new domain is automatically added to the tree in the engine filter *Edit* pane, under **Additional web addresses to block** or **Web addresses to ignore**.

Editing URLs and Domains

URLs and domains that have been added to an engine filter can be edited in the appropriate *Edit* pane. PureSight checks for format when a URL or domain is being added, but is not able to check spelling. Incorrect spelling can be edited, as described in the following procedure.

➢ **To edit a URL or domain:**

1. Click the URL or domain to be edited in the *Edit* pane of the appropriate engine filter. The *Edit URL* or *Edit Domain* pane is displayed, containing the previously defined information for the URL or domain.
2. Enter the required changes.
3. Click **Save**. The URL or domain information is automatically updated in the *Edit* pane of the appropriate engine filter.

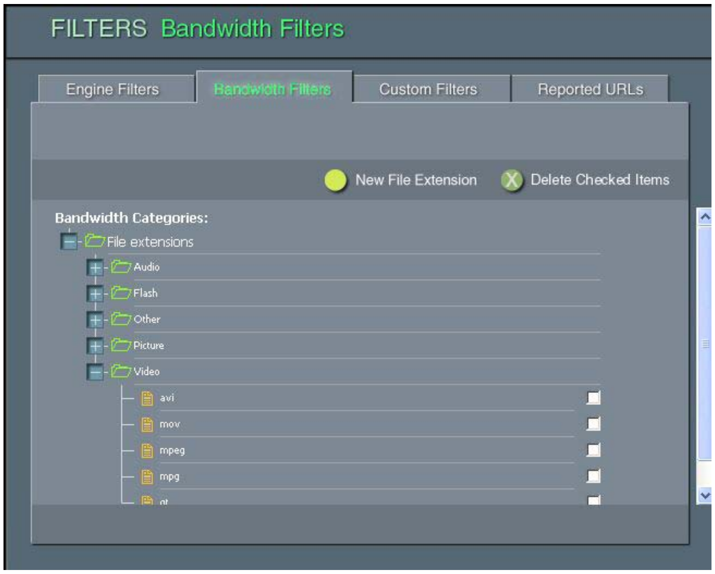
Bandwidth Filters

Bandwidth filters are used to filter access to bandwidth consuming files and protocols. You can block or allow access to the various bandwidth categories included in the bandwidth filters by defining them in a policy, as described in *Chapter 6*, *Defining Policies*. For example, you can define a policy that blocks access to all audio files with .mp3 extensions and also block all ftp requests.

You can configure the specific file extensions to be included in the bandwidth filters, according to your organization's requirements.

➢ **To display the Bandwidth Filters tab:**

✦ The **Bandwidth Filters** tab, shown below, is displayed by selecting the appropriate tab in the *Filters* pane.



The **Bandwidth Filters** tab contains a **Categories** tree, with the following main branches:

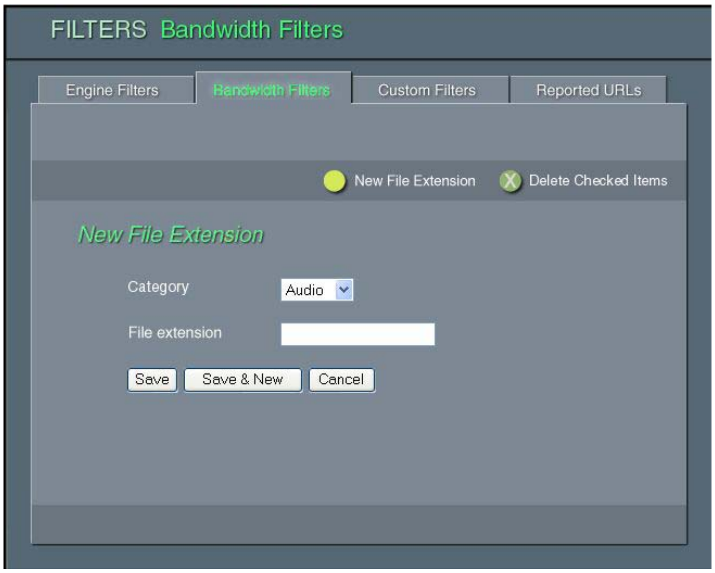
- **File Extensions**, divided into the executables **Audio**, **Video**, **Flash**, **Pictures** and **Other**. You can add, edit and delete file extensions in each of these categories, as described in the following procedure.

Adding and Editing New Bandwidth Extensions

From the **Bandwidth Filters** tab, you can add new file extensions and edit existing ones.

➢ **To add a new bandwidth extension:**

1 In the **Bandwidth Filters** tab, click **New Bandwidth Extension**. The *New File Extension* pane is displayed, as shown below.



2 Select the required file extension category from the dropdown list in the **Category** field.

3 Enter the file extension in the **File Extension** field.

4 Click **Save** to add the new file extension and return to the **Bandwidth Filters** tab,

or

Click **Save & New** to add another new file extension.

Each new file extension is automatically added to the tree in the **Bandwidth Filters** tab.

➢ **To edit a bandwidth extension:**

1 Click the required file extension in **Bandwidth Filters** tab. The *Edit File Extension* pane is displayed, containing the previously defined information for the file extension.

2 Enter the required changes.

3 Click **Save**. The file extension information is automatically updated in the **Bandwidth Filters** tab.

TIP:

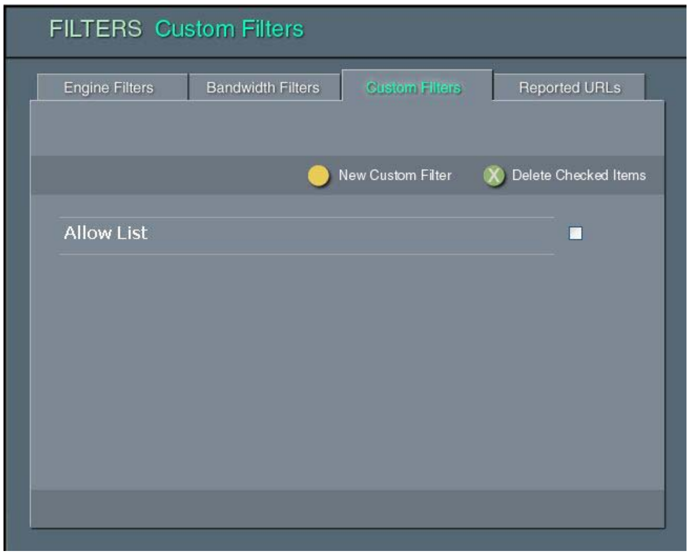
File extensions can be deleted from the **Bandwidth Filters** tab by selecting the appropriate checkboxes and clicking the **Delete Checked Items** button.

Custom Filters

Custom filters are user-defined lists of URLs and domains that can be filtered. Custom filters are used to create policies catering to the specific needs of your organization, for example, permitting access solely to the Intranet.

➢ **To open the Custom Filters tab:**

✦ The **Custom Filters** tab, shown below, is displayed by selecting the appropriate tab in the *Filters* pane.



Allow List □

The **Custom Filters** tab displays any previously defined custom filters. If no custom filters have been defined, the tab appears empty.

TIP:

Defined custom filters can be deleted from the **Custom Filters** tab by selecting the appropriate checkboxes and clicking the **Delete Checked Items** button.

Creating and Editing New Custom Filters

From the **Custom Filters** tab, you can create a new custom filter and then use the edit function to define URLs and domains to be included in the custom filter.

➢ **To create a new custom filter:**

1. In the **Custom Filters** tab, click **New Custom Filter**. The *New Custom Filter* pane is displayed.
2. Enter the filter name in the **Filter Name** field.
3. Click **Save** to create the custom filter and return to the **Custom Filters** tab,

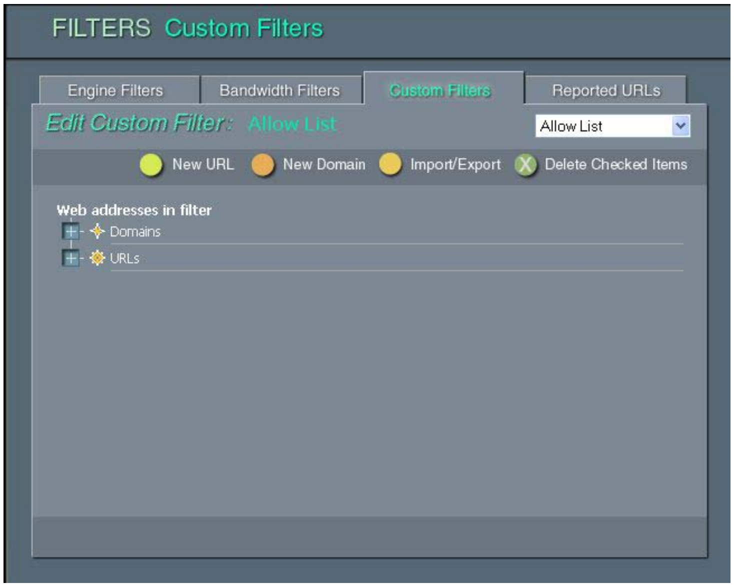
   or

   Click **Save & New** to create another new custom filter.

   Each new custom filter is automatically displayed in the **Custom Filters** tab.

➢ **To edit a custom filter:**

1 In the **Custom Filters** tab, click the filter you want to edit. The *Edit Custom Filter* pane for the selected custom filter is displayed.



2 To add a new URL or a new domain to the custom filter, click the **New URL** or **New Domain** button. The *New URL* or *New Domain* pane is displayed, as appropriate. Refer to the procedures described for *Adding URLs*, page 5-4, or *Adding Domains,* page 5-5.

Importing and Exporting Custom Filters

From the **Custom Filters** tab, you can import/export URLs and domains to/from a custom filter list from/to a text file.

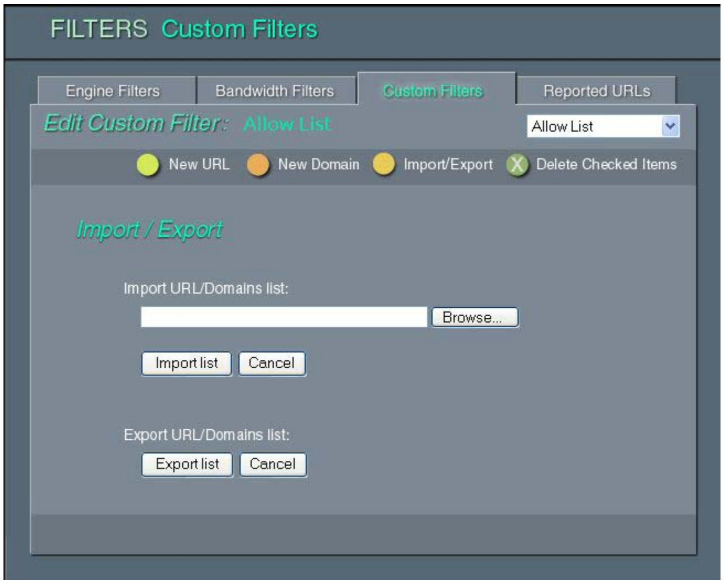
```
U http://www.hello.com
U http://www.hi.com/index.html
D h.com
D hellllo.com
```

Explanation: U / D is for URL or Domain.

➢ **To import to a custom filter:**

1 In the **Custom Filters** tab, click the filter you want to import URLs and domains to. The *Edit Custom Filter* pane for the selected custom filter is displayed.

2 Click **Import/Export**. The *Import/Export* pane is displayed, as appropriate.



3 In the **Import URL/Domain list** field enter the file path of the import file or click **Browse...** button and select the file with the **Choose File** dialog.

4 Click **Import List**.

➢ **To export from a custom filter:**

1 Repeat steps 1 and 2 as described in **import to a custom filter**.

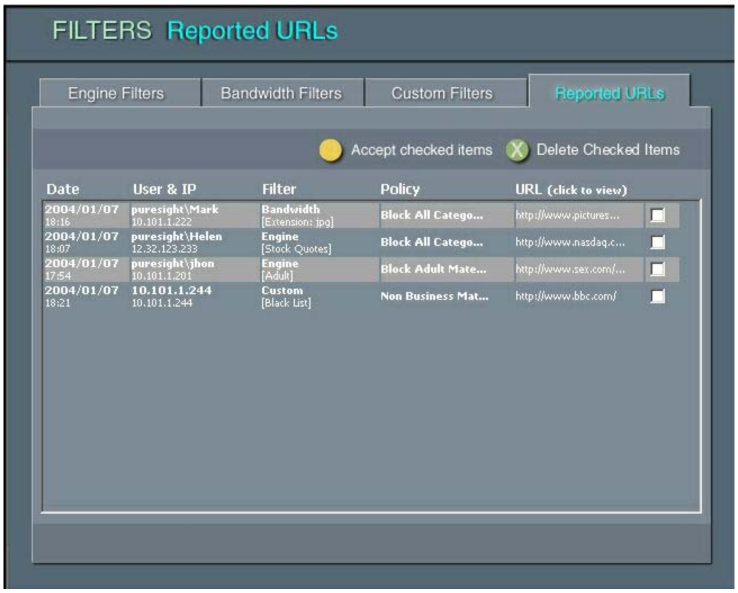
2 Click **Export URLs/Domains** and enter a file where the data will be saved.

Reported URLs

The Administrator can enable users to report URLs that they believe were wrongfully blocked (Refer to *Chapter 7, Settings*, for additional information). If enabled, the blocking and warning pages will include a **Report URL to Administrator** button. Clicking on the **Report URL to Administrator** button adds the blocking information to the **Reported URLs** pane. The Administrator can review all reported URLs and decide for each URL whether or not to refine the filter or policy that blocked the URL so that in future requests, this URL will not be blocked by the filter.

➢ **To display the Reported URLs tab:**

- ✦ The **Reported URLs** tab, shown below, is displayed by selecting the appropriate tab in the *Filters* pane.



Date	User & IP	Filter	Policy	URL (click to view)	
2004/01/07 18:16	puresight\Mark 10.101.1.222	Bandwidth [Extension: jpg]	Block All Catego...	http://www.pictures...	□
2004/01/07 18:07	puresight\Helen 12.32.123.233	Engine [Stock Quotes]	Block All Catego...	http://www.nasdaq.c...	□
2004/01/07 17:54	puresight\jhon 10.101.1.201	Engine [Adult]	Block Adult Mate...	http://www.sex.com/...	□
2004/01/07 18:21	10.101.1.244 10.101.1.244	Custom [Black List]	Non Business Mat...	http://www.bbc.com/	□

The **Reported URLs** tab contains a table, with the following information:

- **Date**: the time and day when the URL was reported.
- **User & IP**: the username and IP address for whom the URL was blocked.
- **Filter**: the name and type of the filter which blocked the URL. The type of the filter can be one of the following: engine bandwidth or custom list.
- **Policy**: the policy that was applied for the user.
- **URL**: the URL that was blocked.

For each reported URL, the Administrator can decide whether to accept the reported URL, i.e. refine the filter so that future requests to the specified URL will not be blocked or to delete the URL, i.e. ignore the report.

NOTE:

Accepting a URL will refine the appropriate filter or policy for all users.

TIP:

Before accepting a URL, make sure that:

1. The correct policy is applied for the reporting user
2. The policy schedule is appropriate
3. The policy filters are appropriate

Accepting Reported URLs

From the **Reported URLs** tab, you can accept reported URLs and refine the appropriate filters so that in future, these URLs will not be blocked.

The following table describes the refinement of the filters and policies when accepting a URL according on the filter type:

Filter Type	**Refinement**
Engine	If URL appears in the Additional list of the Engine filter then it is removed. Otherwise, the URL is added to the Engine filter Ignore list.
Bandwidth	Removes the appropriate extension from the policy.
Custom List	If the URL appears in the Custom List then it is removed. If the domain of the URL appears in the Custom List then the Administrator can decide whether to remove it or not.

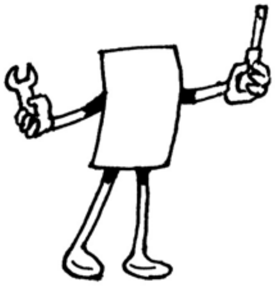
➢ **To accept reported URLs:**

1 In the **Reported URLs** tab, select all the URLs you wish to accept by clicking on the checkbox next to each URL.

2 Click **Accept checked items**.

TIP:

Reported URLs can be deleted from the *Reported URLs* pane by selecting the appropriate checkboxes and clicking the **Delete Checked Items** button.



Chapter 6

Defining Policies

About This Chapter

This chapter describes how to add and edit new policies. It contains the following sections:

- **Overview**, below, provides an overview of defining policies, and describes PureSight's predefined policies.
- **Policies Pane**, page 6-4, describes the main *Policies* pane and the color scheme used in the schedule grids.
- **Defining a New Policy**, page 6-5, guides you through the process of creating a new policy using the New Policy Wizard.
- **Editing a Policy**, page 6-15, describes how to edit an existing policy.

Overview

A policy defines when and what to filter. It consists of a group of one or more filters, with a defined operating schedule for the policy. The filters in a policy are active according to the policy schedule, and their active status can be defined as allow, block or warn.

There are three main types of policies:

- **Allow all except**: *Permits* access to all sites apart from those defined in the filters included in the policy. For example, the policy may permit access to all sites except gambling sites.
- **Block all except**: *Denies* access to all sites apart from those defined in the filters included in the policy. For example, the policy may deny access to all sites except the Intranet.
- **Monitor**: *Monitors* activity on all filters according to the policy schedule, without blocking any access, for reporting purposes.

If you want to include your own customized filters in a policy, or additional bandwidth filters beyond those currently defined in PureSight, you must first define these filters. Refer to *Chapter 5*, *Defining Filters*, for more information.

Once a policy has been created, it is automatically added to the lists of available policies for assigning to users and groups, and for use as the default policy.

Predefined Policies

PureSight is supplied with five predefined filtering policies. These predefined policies are available for assigning to users or using as the default policy, in addition to any new policies you define. All policies can be edited at any time.

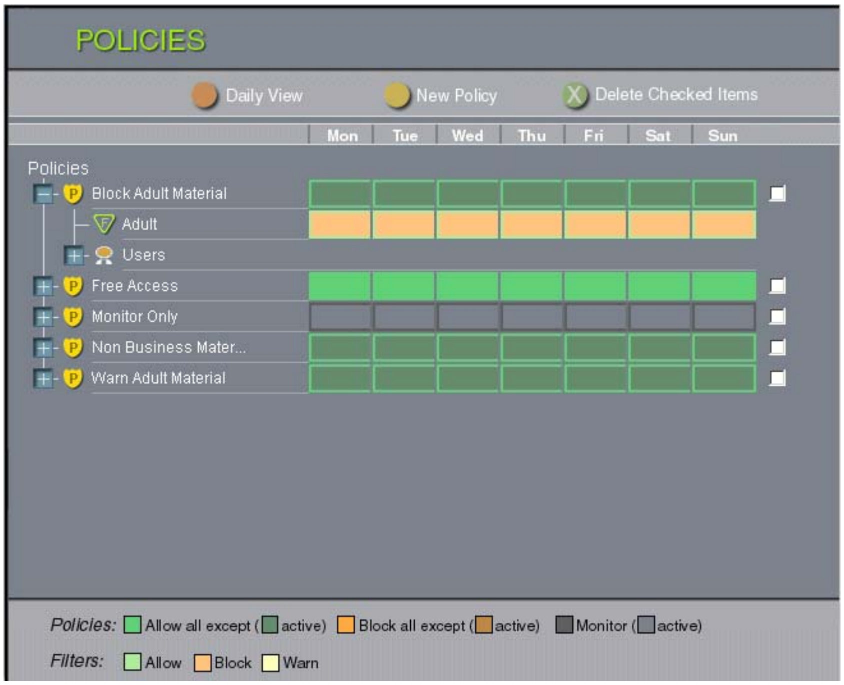
The predefined policies are as follows:

- **Free Access**: Allows access to all sites at all times, with no filtering.
- **Block Adult Material**: Blocks access to all adult material at all times. This is the default option that is immediately active after PureSight is installed.

- **Warn Adult Material**: Issues a warning before allowing access to all adult material at all times.
- **Non-Business Material**: Between the hours of 09:00 and 12:00 and 13:00 and 17:00, Monday to Friday, blocks or warns as follows:
  - Blocks access to all adult material at all times.
  - Issues a warning before allowing access to gambling sites, or the downloading of files with .mp3 extensions.
- **Monitor Only**: Monitors and logs all activities without blocking any access.
- **Block All Except:** Blocks all access except for sites that are listed in the custom filter: Allow List. By default the custom filter Allow List does not contain any sites.

Policies Pane

The main *Policies* pane, shown below, is accessed from the Administration toolbar by clicking **Policies**.



The *Policies* pane displays the following information:

- **Policies**: The **Policies** tree contains all PureSight's predefined policies, as described in the previous section, as well as any new policies you have created. Expanding the **Policies** tree displays all policies, the filters included within each policy and the user groups or individual users to which that policy has been assigned. (Users defined within user groups are not shown.)
- **Weekly**/**Daily Schedule**: The grid displayed for each policy shows the weekly or daily schedule for that policy and its included filters. You can use the **Daily View**/**Weekly View** button to toggle between the two views of the schedule.

The first line of a grid indicates activity for that policy during each 24-hour period by means of a color scheme. The grid row displayed beside each included filter indicates the filtering mode that is active for that filter during each 24-hour period.

✦ **Color Scheme:** At the bottom of the *Policies* pane you will find the color legend used in the visualization of the policies. A dark color means the policy is turned on (active) and a light color means the policy is turned off (inactive). The background color of each cell indicates if the policy type is **Allow all except** (green), **Block all except** (orange) or **Monitor** (gray).

The colored blocks within each cell indicate the type of filter activity, as follows:

❖ **Green**: Allowed

❖ **Orange**: Blocked

❖ **Yellow**: Warned

From the *Policies* pane, you can add new policies and edit existing ones, as described in the following sections.

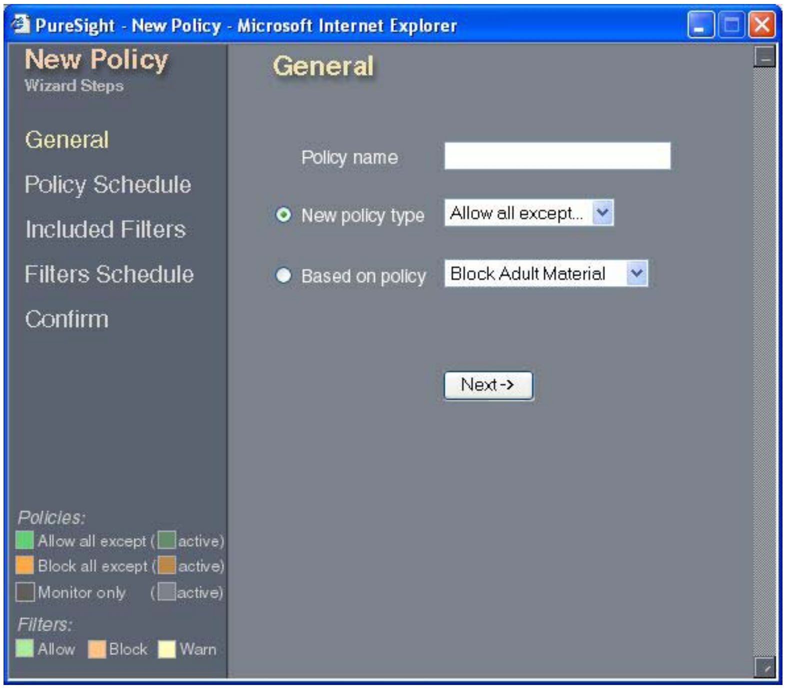
TIP:

To delete a policy, select the checkbox to the right of the policy you want to delete, and then click the **Delete Checked Items** button.

Defining a New Policy

New policies are created using the New Policy Wizard.

To access the New Policy Wizard, click the **New Policy** button in the *Policies* pane. The New Policy Wizard is displayed in a new browser page. The left side menu displays five steps that guide you logically through the process of creating a new policy and the color scheme used for the policy schedules. The workspace displays the step that is currently selected.



PureSight - New Policy - Microsoft Internet Explorer

New Policy
Wizard Steps

- General
- Policy Schedule
- Included Filters
- Filters Schedule
- Confirm

Policies:
🟩 Allow all except (🟩 active)
🟧 Block all except (🟧 active)
□ Monitor only (□ active)

Filters:
🟩 Allow 🟧 Block 🟨 Warn

General

Policy name [ ]

● New policy type: Allow all except...

○ Based on policy: Block Adult Material

The New Policy Wizard steps are:

- **Step 1: General**: Enables you to define a name and type for the policy.
- **Step 2: Policy Schedule**: Enables you to define the schedule for the policy.
- **Step 3: Included Filters**: Enables you to define the filters you want to include in the policy.
- **Step 4: Filters Schedule**: Enables you to refine the schedule for each filter.
- **Step 5: Confirm**: Enables you to view and confirm the policy and filter schedules.

Some of the steps are divided into substeps. Clicking **Next** at the bottom of each pane takes you on to the next step or substep. You can click **Back** at any stage of the process to return to previous steps. The currently open step or substep is highlighted in the side menu.

Step 1: General

The *General* pane, shown on the previous page, requires you to enter a name for the new policy. You can either select the type of policy you want to create or create a new policy based on an existing one. The policy type options are **Allow all except** (the default setting), **Block all except** and **Monitor**.

➢ **To define general policy data:**

1 Enter the name for the policy in the **Policy name** field. The name must be unique.

2 In the **Policy type** field, select the required option from the dropdown list.

or

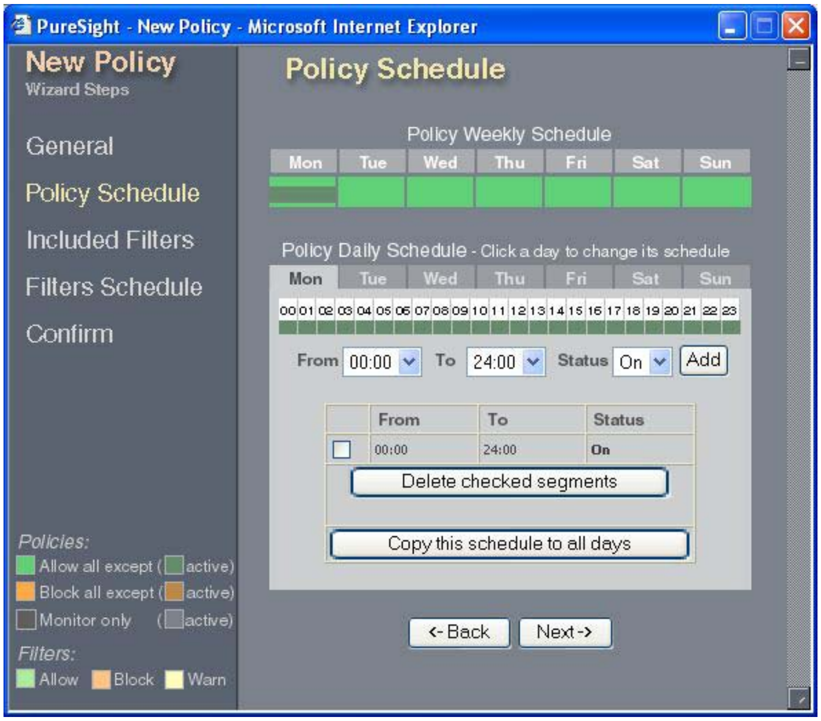
In the **Based on Policy** field, select the required policy from the dropdown list.

3 Click **Next** to proceed to the next step of the wizard.

Step 2: Policy Schedule

A policy schedule defines the working days and hours of the policy. The *Policy Schedule* pane, shown on the following page, enables you to define a separate schedule for each day of the week. When defining a new policy, the schedule for the policy is **Off** at all times. You must add a schedule in order for the policy to be activated.

For each day, you can define time periods during which the policy will be **On**, meaning that the filters are active, or **Off**, meaning that the filters are inactive. The filters included in a policy can be active only when the policy itself is **On**. Once a daily schedule is set for one of the days, it can be copied to rest of the days in the week.


PureSight - New Policy - Microsoft Internet Explorer
New Policy
Wizard Steps
General
Policy Schedule
Included Filters
Filters Schedule
Confirm
Policies:
🟩 Allow all except (🟩 active)
🟧 Block all except (🟧 active)
□ Monitor only (□ active)
Filters:
🟩 Allow 🟧 Block 🟨 Warn
Policy Schedule
Policy Weekly Schedule
Mon Tue Wed Thu Fri Sat Sun
Policy Daily Schedule - Click a day to change its schedule
Mon Tue Wed Thu Fri Sat Sun
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23
Add
Delete checked segments
Copy this schedule to all days
<- Back
Next ->

From 00:00 To 24:00 Status On

	From	To	Status
□	00:00	24:00	On

NOTE:

Refer to *Policies Pane*, page 6-4, for an explanation of the color schemes used in the grid.

The *Policy Schedule* pane contains the following areas:

- **Policy Weekly Schedule**: Indicates the schedule defined for that policy for each day of the week.
- **Policy Daily Schedule**: Indicates the times when the filters are active or inactive for each individual day, and enables you to define active or inactive time periods for each day. Every modification to the time periods is automatically updated to the Policy Weekly Schedule.

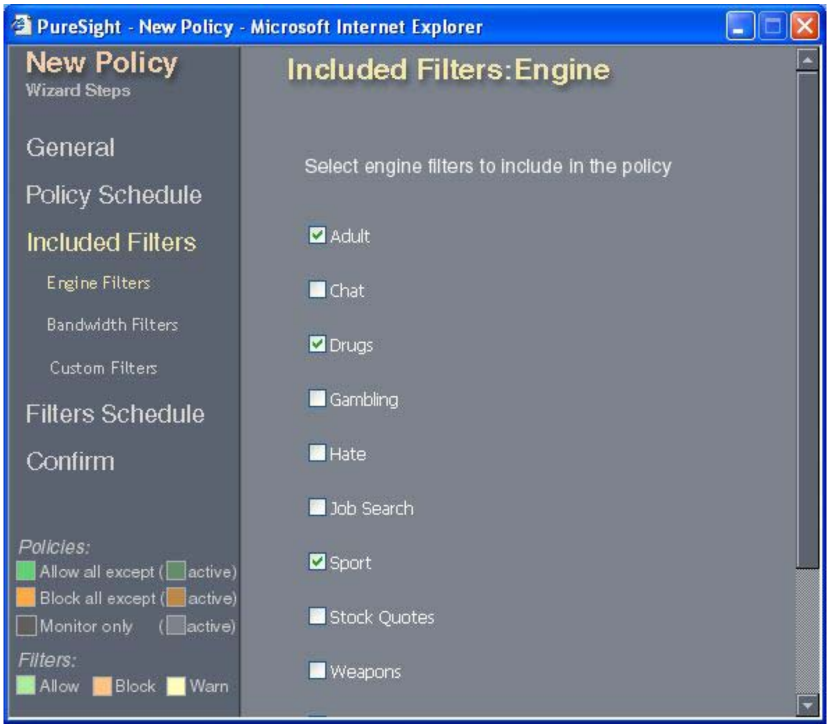
➢ **To define a policy schedule:**

1. In the *Policy Schedule* pane, click the appropriate day tab in the **Policy Daily Schedule** area. The tab for the selected day is displayed.
2. To select the times when you want the policy to be active or inactive, click the arrows in the **To** and **From** fields and select the times from the dropdown lists.
3. To define the status of the policy during the selected time period, click the arrow in the **Status** field and select **On** (policy active) or **Off** (policy inactive) from the dropdown list.
4. Click **Add** to add the time period to the schedule for that day. The selected times and status are displayed in the table below the fields, and are indicated by colored blocks in the weekly and daily schedule grids. The color of the blocks represents the different activation modes (**On** and **Off**).
5. Repeat steps 2 through 4 for each time period you want to add to the schedule for that day.
6. To remove a defined time period, select the checkbox next to the time period in the table and click **Delete checked segments**. The time period is deleted from the table and the schedule grids.
7. Repeat the entire procedure described above for each day, or use the **Copy this schedule to all days** button.
8. Click **Next** to proceed to the next step of the wizard.

Step 3: Included Filters

The **Included Filters** step of the New Policy Wizard enables you to define the filters to be included in the policy. The included filters automatically inherit the policy schedule: in an **Allow all except** policy, the filters are set to block, and in a **Block all except** policy, the filters are set to allow. Only filters that are relevant to the type of policy are displayed and available for selection.

The **Included Filters** step is divided into three substeps: **Engine Filters**, **Bandwidth Filters** and **Custom Filters**. The following example displays the *Included Filters: Engine* pane.



PureSight - New Policy - Microsoft Internet Explorer

New Policy
Wizard Steps

General
Policy Schedule
Included Filters
Engine Filters
Bandwidth Filters
Custom Filters
Filters Schedule
Confirm

Policies:
🟩 Allow all except (🟩 active)
🟧 Block all except (🟧 active)
⬛ Monitor only (⬛ active)

Filters:
🟩 Allow 🟧 Block 🟨 Warn

Included Filters:Engine

Select engine filters to include in the policy

☑ Adult
□ Chat
☑ Drugs
□ Gambling
□ Hate
□ Job Search
☑ Sport
□ Stock Quotes
□ Weapons

For more information about the filters, refer to *Chapter 5, Defining Filters*.

NOTE:
The **Included Filters** step is not available for the Monitor policy type.

➢ **To define which filters to include:**

1. In the *Included Filters: Engine* pane, select the engine filters you want to include in the policy and click **Next**.
2. The *Included Filters: Bandwidth* pane is displayed. Select the **Include Bandwidth Filter in this policy** checkbox if you want to include the bandwidth filter in the policy.
3. Select the file extensions and protocols that you want to include in the policy and click **Next**.
4. The *Included Filters: Custom* pane is displayed. Select the custom filters you want to include in the policy.
5. Click **Next** to proceed to the next step of the wizard.

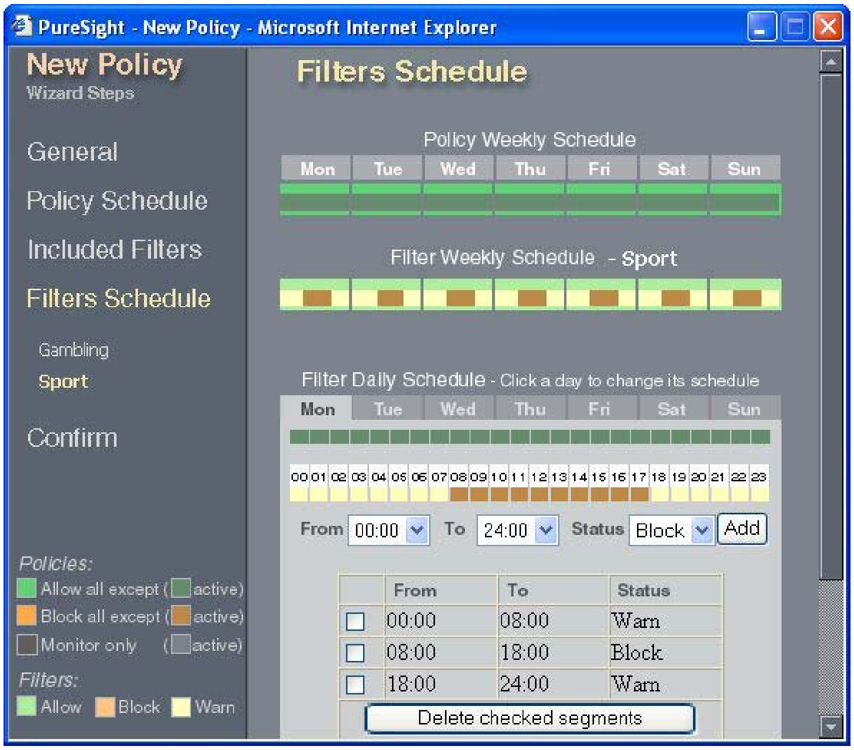
Step 4: Filters Schedule

The **Filters Schedule** step enables you to define individual schedules for each filter included in the policy, and to configure the PureSight **Warn** option.

By default, each filter inherits the policy schedule, as defined in *Step 2: Policy Schedule*, page 6-7. If required, changes can be made in the filter schedule to override the policy schedule settings; however, a filter can only be active at times that the policy is active. For example, a policy that is active from 09:00 to 17:00 can be edited so that a particular filter only blocks from 09:00 to 13:00. In addition, you can edit a filter schedule so that a warning is returned about a requested site, rather than blocking it.

The filters defined in the **Included Filters** step are automatically added as substeps in the **Filters Schedule** step.

The example below shows the *Filter Schedule* pane for the Gambling engine filter:



From 00:00 To 24:00 Status Block

	From	To	Status
□	00:00	08:00	Warn
□	08:00	18:00	Block
□	18:00	24:00	Warn

The *Filters Schedule* pane contains the following areas:

- **Policy Weekly Schedule**: Indicates the schedule defined for the policy for each day of the week.
- **Filter Weekly Schedule**: Indicates the schedule defined for that filter for each day of the week.
- **Filter Daily Schedule**: Indicates the times when the filter is blocking, allowing or warning on each individual day, and enables you to edit the filter schedule for each day. Each modification is automatically updated to the Filter Weekly Schedule.

NOTE:

Time periods defined in the filters schedule must be within the periods that the policy is active.

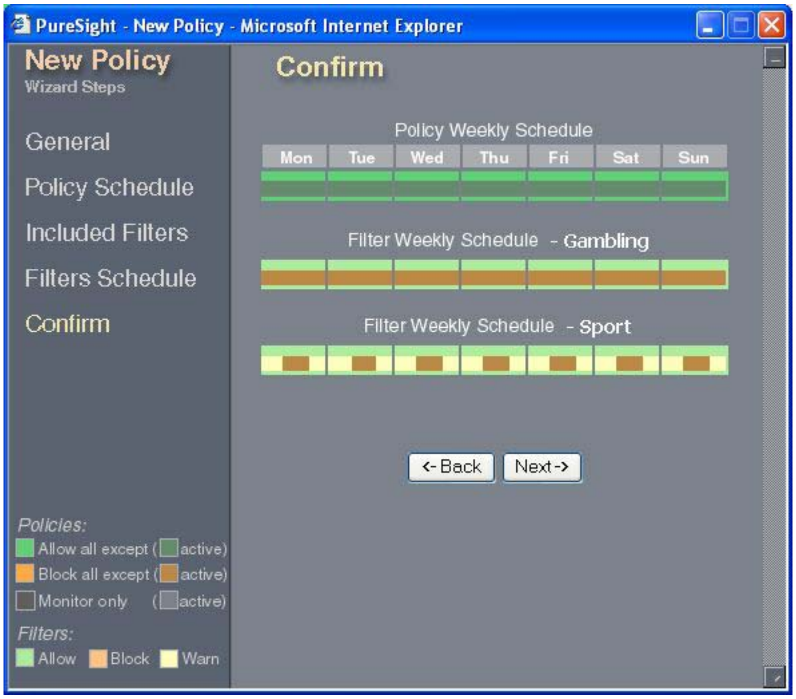
The following procedure should be repeated as necessary for each **Filters Schedule** substep.

➢ **To edit the filters schedule:**

1. In the *Filters Schedule* pane, click the appropriate day tab in the **Filter Daily Schedule** area. The tab for the selected day is displayed.
2. Click the arrows in the **To** and **From** fields and select the required times from the dropdown lists.
3. To define the status of the filter during the selected time period, click the arrow in the **Status** field and select **Allow**, **Block** or **Warn** from the dropdown list.
4. Click **Add** to add the change to the schedule for that day. The selected times and status are displayed in the table below the fields and are indicated by colored blocks in the filter weekly and daily schedule grids.
5. Repeat steps 2 through 4 for each change to the filter schedule for that day.
6. To remove a defined time period, select the checkbox next to the time period in the table and click **Delete checked segments**. The time period is deleted from the table and the schedule grids.
7. Repeat the entire procedure described above for each day, or use the **Copy this schedule to all days** button.
8. Click **Next** to proceed to the next step of the wizard.

Step 5: Confirm

The *Confirm* pane, shown below, gives an overall summary view of the new policy that you created using the New Policy Wizard.



NOTE:

Refer to *Policies Pane*, page 6-4, for an explanation of the color schemes used in the grid.

The *Confirm* pane displays the following information:

- **Policy Weekly Schedule**: This grid summarizes the weekly schedule created for the new policy.
- **Filter Weekly Schedule**: A grid is displayed for each filter included in the policy. This grid summarizes the weekly schedule for the filter.

If you want to make additional changes to the weekly schedules, click **Back** until you reach the relevant pane and make the required changes.

➢ **To confirm the new policy:**

1. Click **Next** to confirm the new policy. The *Confirm* pane displays a message confirming that the new policy was successfully created.
2. Close the New Policy Wizard. The new policy now appears in the **Policies** tree in the main *Policies* pane.

Assigning users to the policies is done from the *Users* pane. Refer to *Chapter 4*, *Defining Users and Groups* for more details.

Editing a Policy

Once a policy has been created, it can be edited at any time using the Edit Policy page. The Edit Policy page enables you to make changes in the policy schedule, the included filters and the included filters' schedules, all described in *Defining a New Policy*, page 6-5. You can also edit the predefined policies supplied with PureSight.

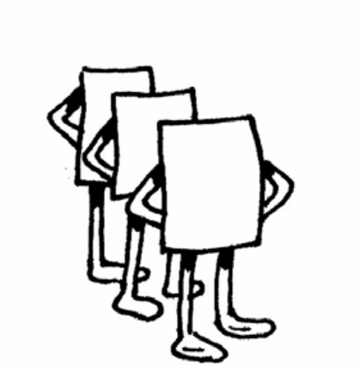
As in the New Policy Wizard, the options are displayed in a side menu. However, in the Edit Policy page, you can select an option from the menu to go directly to the required option.

➢ **To edit a policy:**

1. In the **Policies** tree in the main *Policies* pane, click the policy you want to edit. The Edit Policy page opens in a new browser page, containing the information previously defined for that policy.
2. Select an option from the menu, and make the required changes in the displayed pane for that option. Refer to the procedures described in *Defining a New Policy*, page 6-5.

3 When you have completed the changes in a pane, click **Save Changes**.

4 When you have finished editing the policy, close the Edit Policy page. The updated policy information is displayed in the **Policies** tree in the main *Policies* pane.



Chapter 7

Settings

About This Chapter

This chapter describes additional settings available for user configuration. It contains the following sections:

- **Message Settings**, below, describes how to set the blocking and warning messages.
- **Directory Server Settings,** page 7-4, describes how to set the directory server settings.
- **Log Server Settings**, page 7-10, describes how to set the PureSight Log Server settings.
- **System Settings**, page 7-14, describes how to set the PureSight Administrator password.

Message Settings

When a user requests a site that is either blocked or warned against, an appropriate message is returned to the user's workstation. This may be a redirection to a URL or a text message displayed in the browser. PureSight can be configured to use an internal URL for your organization, or to use your own text for the message. Default URL and message options are supplied with PureSight.

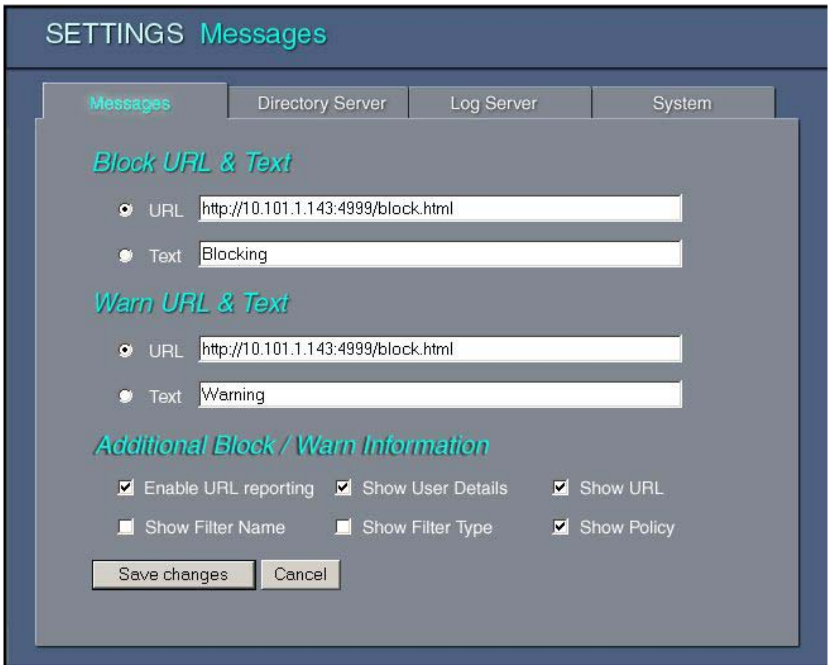
The Administrator can also define whether to enable users to report URLs that were blocked to the Administrator. If enabled, the blocking and warning messages will display a **Report URL to Administrator** button. If clicked, a reported URL will be added to the Reported URLs along with all of the blocking information. Refer to *Chapter 5, Filters*, for additional information.

Additional blocking information can be displayed in the blocking message. This information includes:

- ✦ **User Details**: IP address and username (if available) of the user that requested the URL that was blocked.
- ✦ **URL**: the address of the URL that was blocked.
- ✦ **Filter Name**: the name of the filter that the blocked URL was associated with.
- ✦ **Filter Type**: the type of the filter that the blocked URL was associated with. Filter type can be Engine, Bandwidth or Custom.
- ✦ **Policy**: the policy that was applied to the user at the time the requested URL was blocked.

➢ **To set the block and warn messages:**

1 In the *Settings* pane, click the **Messages** tab. The **Messages** tab is displayed.



Block URL & Text

● URL http://10.101.1.143:4999/block.html

○ Text Blocking

Warn URL & Text

● URL http://10.101.1.143:4999/block.html

○ Text Warning

Additional Block / Warn Information

☑ Enable URL reporting ☑ Show User Details ☑ Show URL

□ Show Filter Name □ Show Filter Type ☑ Show Policy

2 In the **Block URL & Text** area, select either the **URL** or **Text** radio button, as required.

3 If you want to change PureSight's default blocking URL, enter the path for the new URL in the **URL** field. Make sure to enter a valid URL.

4 If you want to change PureSight's default blocking text message, enter the new text in the **Text** field.

5 In the **Warn URL & Text** area, select either the **URL** or **Text** radio button, and repeat steps 3 and 4 above, as required.

6 To enable users to report URLs to be reviewed by the Administrator check the **Enable URL reporting** checkbox.

7 To enable blocking information to be displayed in the block and warn messages, select the appropriate checkboxes.

8 Click **Save** to save the changes.

NOTE:

Do not set the blocking and warning URL to point to a page that will be blocked by PureSight.

Directory Server Settings

The **Directory Server** tab enables you to define Directory Server settings. PureSight can then apply policies and generate reports based on these Directory user names.

PureSight supports the following Directory Servers:

- LDAP Directory Servers: iPlanet, Novell, and other custom LDAP servers.
- Windows Active Directory
- Windows Domain

The following table shows the platform support of the PureSight Content Filtering Servers for Directory Servers:

	Windows Domain	**Windows Active Directory**	**iPlanet Directory Server**	**Novell Directory Server**	**Custom LDAP Directory Server**
PureSight for MSProxy	+	+			
PureSight for Microsoft ISA Server	+	+			
PureSight for Squid	+ (*)	+	+	+	+

(*) Squid can work with Windows Domain if users are imported from a text file and an external authentication program is used..

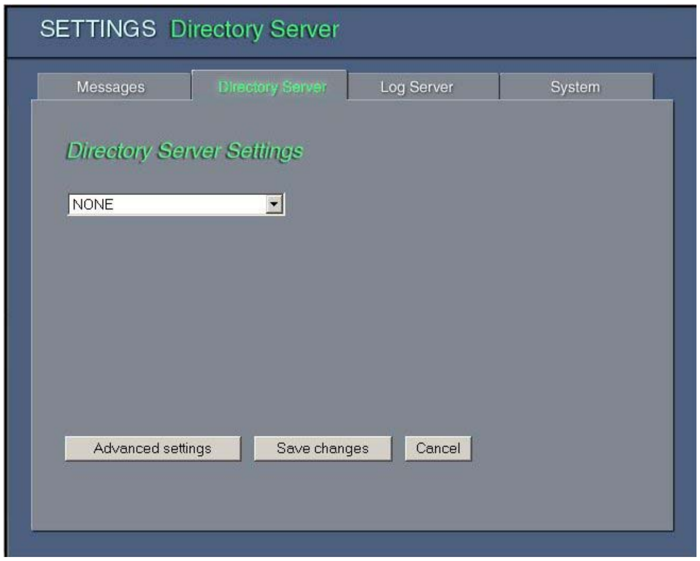
NOTE:
The data presented in this table refers to PureSight version 4.0 and later.

The selected Directory Server must be compatible with all the PureSight Content Filtering servers that are connected to the PureSight Management server. If a PureSight Content Filtering Server does not support the selected Directory Server, then directory user-based policies will not be enforced and PureSight reports will not contain directory user information for Internet surfing from that specific PureSight Content Filtering Server.

NOTE:
In order to import directory users from a Windows Domain, the PureSight Management Server must be installed on a Windows platform.

➢ **To set Directory Server settings:**

1 In the *Settings* pane, click the **Directory Server** tab. The **Directory Server** tab is displayed.



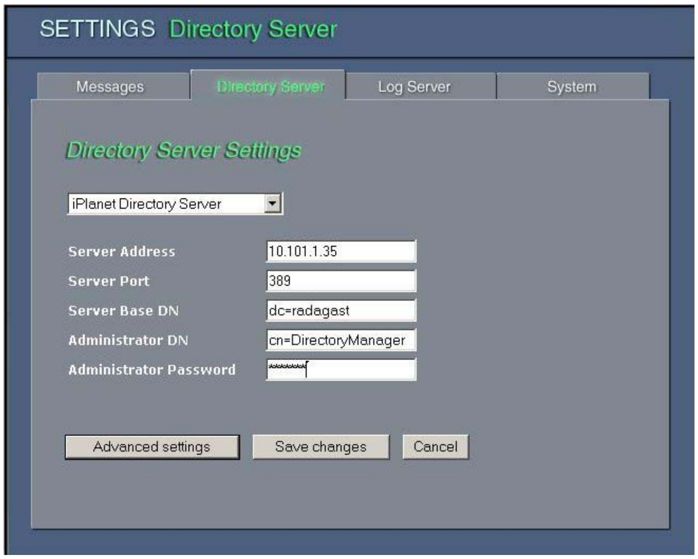
2 Select the appropriate directory server in the dropdown list box. According to the type of the Directory Server selected, the appropriate settings for each selection are displayed as follows:

✦ **LDAP Directory Servers**:

NOTE:

The following steps describe the procedure for configuring the iPlanet Directory Server. This same procedure should be followed for configuring the Novell Directory Server and the Custom LDAP Directory Server.

3 The *Directory Server Settings* pane for iPlanet is displayed.



iPlanet Directory Server

Server Address: 10.101.1.35

Server Port: 389

Server Base DN: dc=radagast

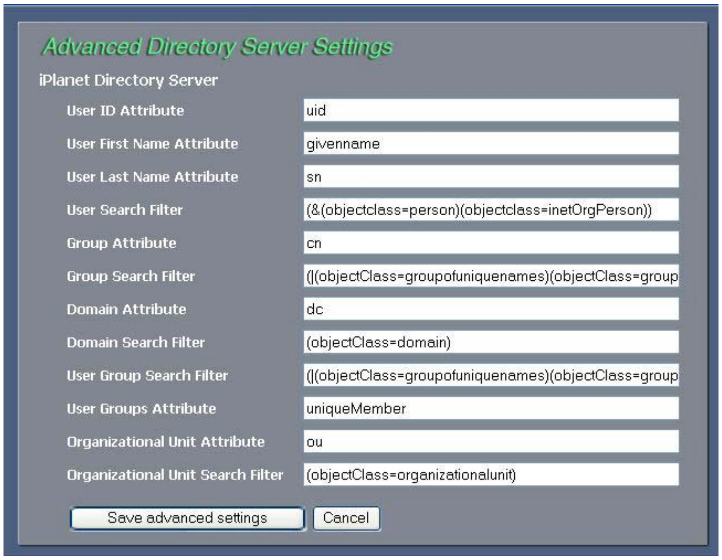
Administrator DN: cn=DirectoryManager

Administrator Password: ******

4 Enter the values for the Server Address, Server Port to connect to, Server Base DN, Administrator DN and Administrator Password.

5 To save, click **Save Changes**.

6 If required, click **Advanced Settings,** to customize attributes and filters, and enter the fields, as shown below in *the Advanced Directory Server Settings* pane for the iPlanet Directory Server.

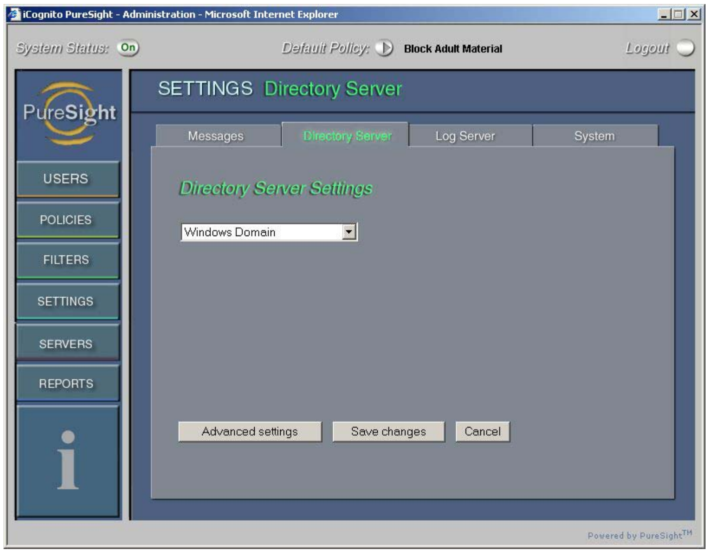


User ID Attribute	uid
User First Name Attribute	givenname
User Last Name Attribute	sn
User Search Filter	(&(objectclass=person)(objectclass=inetOrgPerson))
Group Attribute	cn
Group Search Filter	(|(objectClass=groupofuniquenames)(objectClass=group
Domain Attribute	dc
Domain Search Filter	(objectClass=domain)
User Group Search Filter	(|(objectClass=groupofuniquenames)(objectClass=group
User Groups Attribute	uniqueMember
Organizational Unit Attribute	ou
Organizational Unit Search Filter	(objectClass=organizationalunit)

7 When finished, click **Save changes**.

✦ **Windows Domain Directory Server**:

8 The *Directory Server Settings* pane for the Windows Domain Directory Settings is displayed.



Default Policy: Block Adult Material

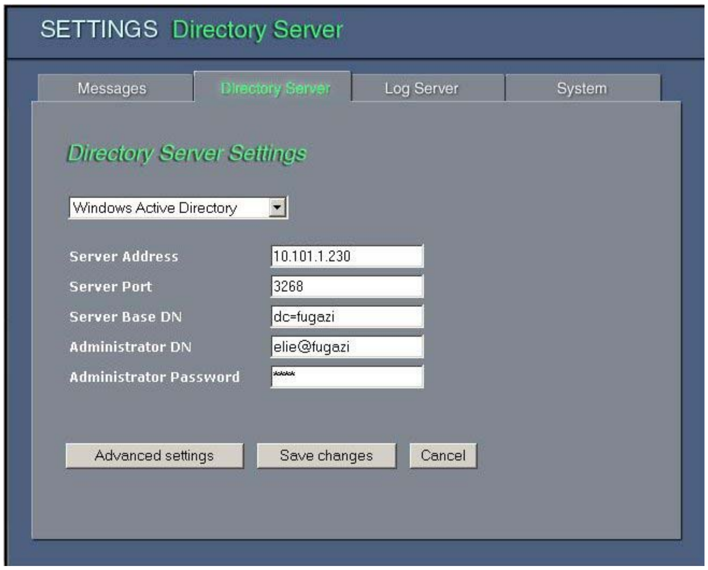
Windows Domain

No additional settings are required. The process is automatic.

9 When finished, click **Save changes**.

✦ **Windows Active Directory Server**:

10 The *Directory Server Settings* pane for the Windows Active Directory Settings is displayed.



Windows Active Directory

Server Address 10.101.1.230

Server Port 3268

Server Base DN dc=fugazi

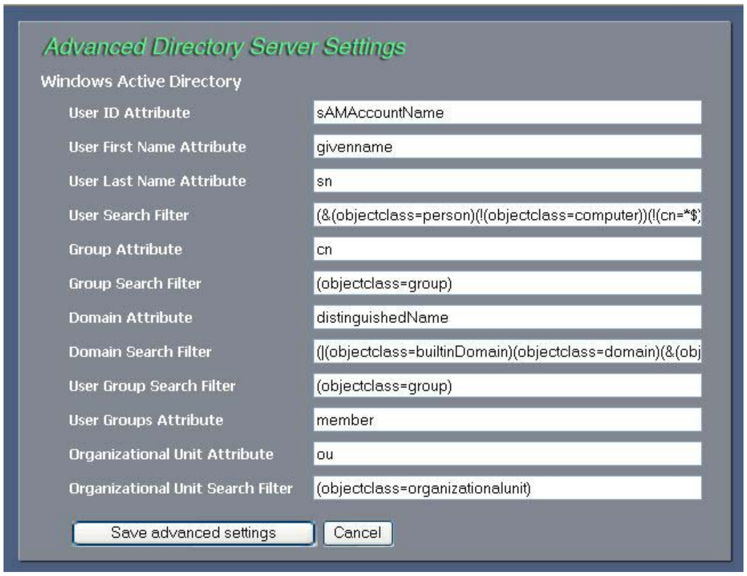
Administrator DN elie@fugazi

Administrator Password *****

11 Enter the values for the Server Address, Server Port to connect to, Server Base DN, Administrator DN and Administrator Password.

12 To save, click **Save Changes**.

13 If required, click **Advanced Settings,** to customize attributes and filters, and enter the fields, as shown in the following Active Directory *Advanced Directory Server Settings* pane example.



User ID Attribute	sAMAccountName
User First Name Attribute	givenname
User Last Name Attribute	sn
User Search Filter	(&(objectclass=person)(!(objectclass=computer))(!(cn=*$)
Group Attribute	cn
Group Search Filter	(objectclass=group)
Domain Attribute	distinguishedName
Domain Search Filter	(|(objectclass=builtinDomain)(objectclass=domain)(&(obj
User Group Search Filter	(objectclass=group)
User Groups Attribute	member
Organizational Unit Attribute	ou
Organizational Unit Search Filter	(objectclass=organizationalunit)

14 When finished, click **Save changes**.

Log Server Settings

The PureSight Log Server is responsible for the centralized logging of user activity in the system, including the user who requested the URL, time and date of URL requests, their classification and the action taken, according to user and IP address. The PureSight Log Server logs activities for all of the PureSight Content Filtering Servers connected to the associated Management server. The data collected is used to generate reports regarding users' Internet activity and bandwidth consumption. (For more on reporting, refer to *Chapter 8, Reports*.)

There are two log storage methods: log files stored in the file system or in a MySQL database.

When working with file system storage, log files are created. Each log file is limited both in size (MB) and in the length of time the log file can stay open. When using the SQL database storage, the log files are created and then imported to the SQL database once they are closed. Reports that are generated will not include data that has not yet been imported to the SQL database.

The total volume of log files saved in the file system is restricted by the amount of space allocated for log file storage. When the storage location is full, files are automatically removed on a first-in-first-out-basis.

When working with a MySQL database, the content of the log files is imported into the database and are then deleted from the file system. Data that is stored in a MySQL database is saved indefinitely, unless it is manually removed by the database administrator. When the PureSight Log Server is uninstalled, you will be prompted to indicate whether to remove the PureSight database.

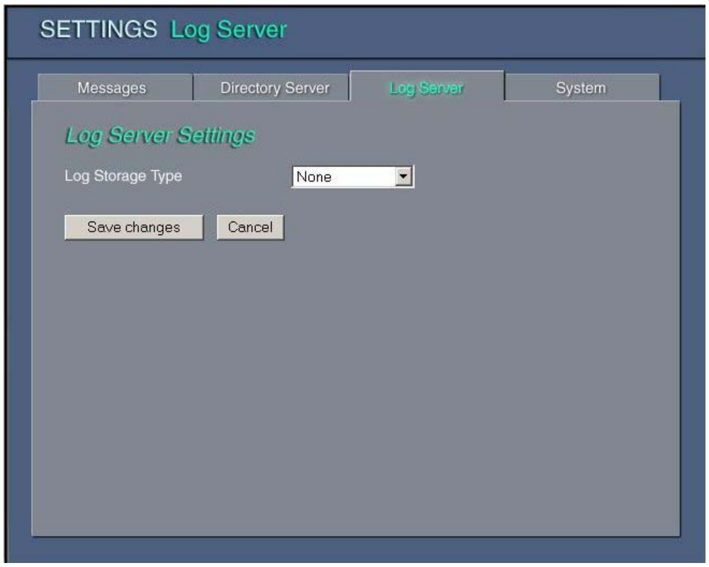
Although PureSight Log Server settings are designated during the installation process, PureSight Log Server settings can be configured in the PureSight Administration. These settings, including the log storage type, log size and log storage location, are configured in the Log Server tab of the *Settings* pane. The PureSight Log Server settings can be edited, as required.

NOTE:

Refer to the *PureSight Log Server Installation Manual* for further details regarding the structure of the PureSight Log Server database tables.

➢ **To configure the Log Server settings:**

1 In the *Settings* pane, click the **Log Server** tab. The **Log Server** tab is displayed.



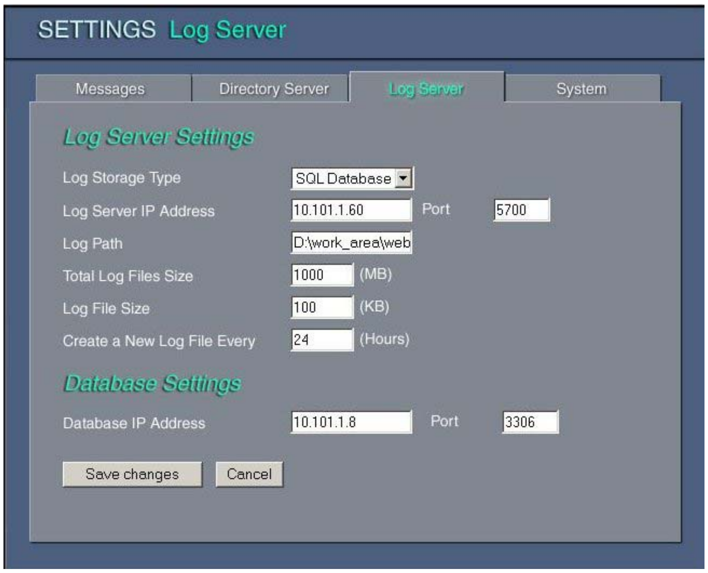
2 In the **Log Storage Type** field, select the required storage type from the dropdown list, as follows:

❖ **None**: The log server will not generate a log file and reports cannot be produced.

❖ **File System**: The log content will be stored in log files on the PureSight Log Server machine.

- **SQL Database**: The log content will be stored in a MySQL database.

Additional parameters are displayed according to the selected log storage type.



Log Server Settings

Log Storage Type: SQL Database

Log Server IP Address: 10.101.1.60 Port 5700

Log Path: D:\work_area\web

Total Log Files Size: 1000 (MB)

Log File Size: 100 (KB)

Create a New Log File Every: 24 (Hours)

Database Settings

Database IP Address: 10.101.1.8 Port 3306

3 If File System or SQL Database is selected as the log storage type, enter the following information in the **Log Server Settings** area:

- **Log Server IP Address**: The IP address of the Log Server.

NOTE:

If the Log Server is replaced for any reason, the IP address of the new Log Server must be entered in this field.

- **Port**: The port used for connecting to the Log Server.
- **Log Path**: The path to the location where the log files are generated on the PureSight Log Server machine.
- **Total Log Files Size**: The maximum amount of disk space in MB, allocated to all log files at the designated path.

- **Log File Size**: The maximum log file size in KB. When this log file size is reached the log file is closed and a new log file is created.
- **Create a New Log File Every**: The maximum time interval (in hours) that a log file can remain open. When this time interval has passed, the log file is closed (regardless of its size) and a new log file is created.

NOTE:

A new log file is created once the maximum file size is exceeded or the maximum time interval has passed, whichever comes first.

4 If SQL Database is selected as the log storage type, enter the following additional information in the **Database Settings** area:

- **Database IP Address**: The IP address of the MySQL database. (The database does not necessarily reside on the same machine as the PureSight Log Server.)
- **Port**: The port used for connecting to the MySQL database. The default port is 3306.

NOTES:

If SQL Database was not selected as the log storage type during installation, you will be prompted to enter the MySQL administrator username and password. Providing a MySQL administrator username and password will install the initial PureSight database.

5 Click **Save changes**. The updated Log Server Settings are distributed automatically to all connected PureSight Content Filtering Servers for immediate implementation.

NOTES:

If the Log Server is running, it does not need to be restarted. If the Log Server is not running, the changes will be accepted, however they will not be distributed to the PureSight Content Filtering Servers until the Log Server is started.

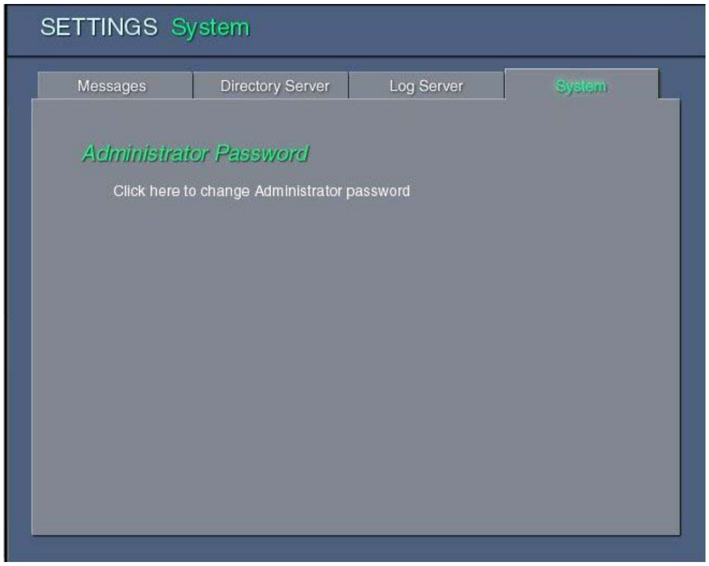
Although the changes are distributed for immediate implementation, depending on network traffic, a brief delay may be experienced. In such a case, the changes should be implemented within minutes.

System Settings

The **System** tab enables you to set a new PureSight Administrator password. The PureSight Administrator password is used to access the PureSight Administration graphical user interface. When installing the PureSight Management Server on a Windows operating system, the PureSight Administrator password is set during installation.

➢ **To set a new Administrator password:**

1 In the *Settings* pane, click the **System** tab. The **System** tab is displayed.



2 Click on the **Click here to change Administrator password** link. The *Change Administrator password* window is displayed.

3 Enter the current Administrator password in the **Current Password** field.

4 Enter the new Administrator password in the **New Password** and **Confirm New Password** fields.

5 Press the **Confirm** button.

Chapter 8

Reports

About This Chapter

This chapter describes how to generate comprehensive reports of users' Internet activity and bandwidth consumption. It includes the following sections:

- **Overview**, below, provides an overview of the reports feature.
- **Reports Pane**, page 8-2, describes the main *Reports* pane.
- **Generating a Report**, page 8-3, describes how to define report parameters and generate a report.
- **Report Descriptions**, page 8-6, provides a brief description of each report available in PureSight.

Overview

PureSight monitors general Internet usage in your organization, as well as activity of the filters as recorded by each connected PureSight Content Filtering Server. This information is automatically saved by the PureSight Log Server, and can be used to generate up-to-date reports at any time.

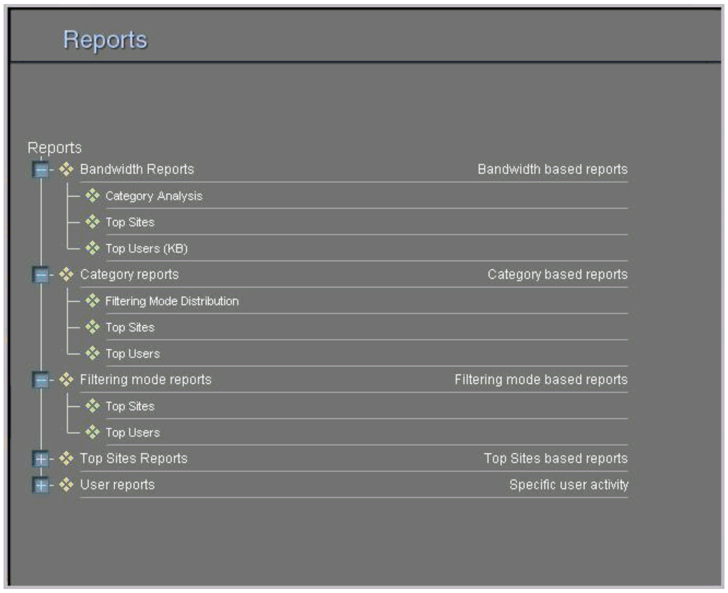
NOTE:

If the PureSight Log Server has not been installed or the Log Server storage type is set to None, logging is disabled and reports cannot be generated. Similarly, all log activity is stopped if the PureSight system is temporarily stopped or disabled.

PureSight provides a number of different types of reports. The definable parameters for each report enable you to generate and view data according to your specific requirements. For example, you can generate reports for a specific user or for a defined time period.

Reports Pane

The main *Reports* pane, shown below, is accessed from the menu in the Administration side bar by clicking **Reports**.



Reports

Reports

⊟ Bandwidth Reports	Bandwidth based reports
Category Analysis	
Top Sites	
Top Users (KB)	
⊟ Category reports	Category based reports
Filtering Mode Distribution	
Top Sites	
Top Users	
⊟ Filtering mode reports	Filtering mode based reports
Top Sites	
Top Users	
⊞ Top Sites Reports	Top Sites based reports
⊞ User reports	Specific user activity

The *Reports* pane contains the **Reports** tree, which when expanded, displays available reports arranged according to type. Clicking a specific report name displays definable parameters for that report. Refer to *Report Descriptions*, page 8-6, for an explanation of the available report types.

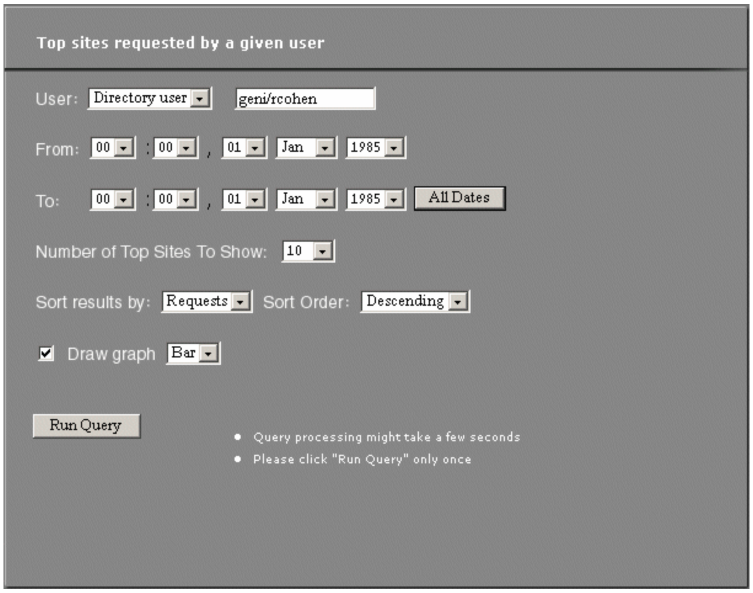
Generating a Report

For each report, you can specify parameters to focus the report on your particular area of interest. You can also define the format of the generated report data. There are default settings for all report parameters.

The following procedure describes the configuration process for one report example. Other possible report parameters that are not included in the example are listed at the end of the procedure on page 8-6.

➢ **To generate a report:**

1 Click the required report in the main *Reports* pane. The parameters for the selected report are displayed in the workspace. The example below displays parameters for **Top sites requested by a given user**, for a directory user.



Top sites requested by a given user

User: Directory user geni/rcohen

From: 00 : 00 , 01 Jan 1985

To: 00 : 00 , 01 Jan 1985

Number of Top Sites To Show: 10

Sort results by: Requests Sort Order: Descending

☑ Draw graph Bar

- Query processing might take a few seconds
- Please click "Run Query" only once

2 From the drop down list, select **All Users** to include all users in the report,

1 or

2 Select **IP Address** and enter the relevant IP address to focus the report,

3 or

4 Select **Directory User** and enter the relevant directory username to generate a report on a specific user.

3 In the **From** and **To** fields, define the time range of the report by selecting the required time (in hours and minutes), day, month and year from the dropdown lists. In order to present all data available in the PureSight logs, select the All Dates button.

4 In the **Number of Top Sites to Show** field, select a value from the dropdown list to limit the number of sites included in the report. If the number is greater than 20, a graph will not be created.

5 In the **Sort results by** field, select from the dropdown list the parameter on which the report is to be based. The options available depend on the report.

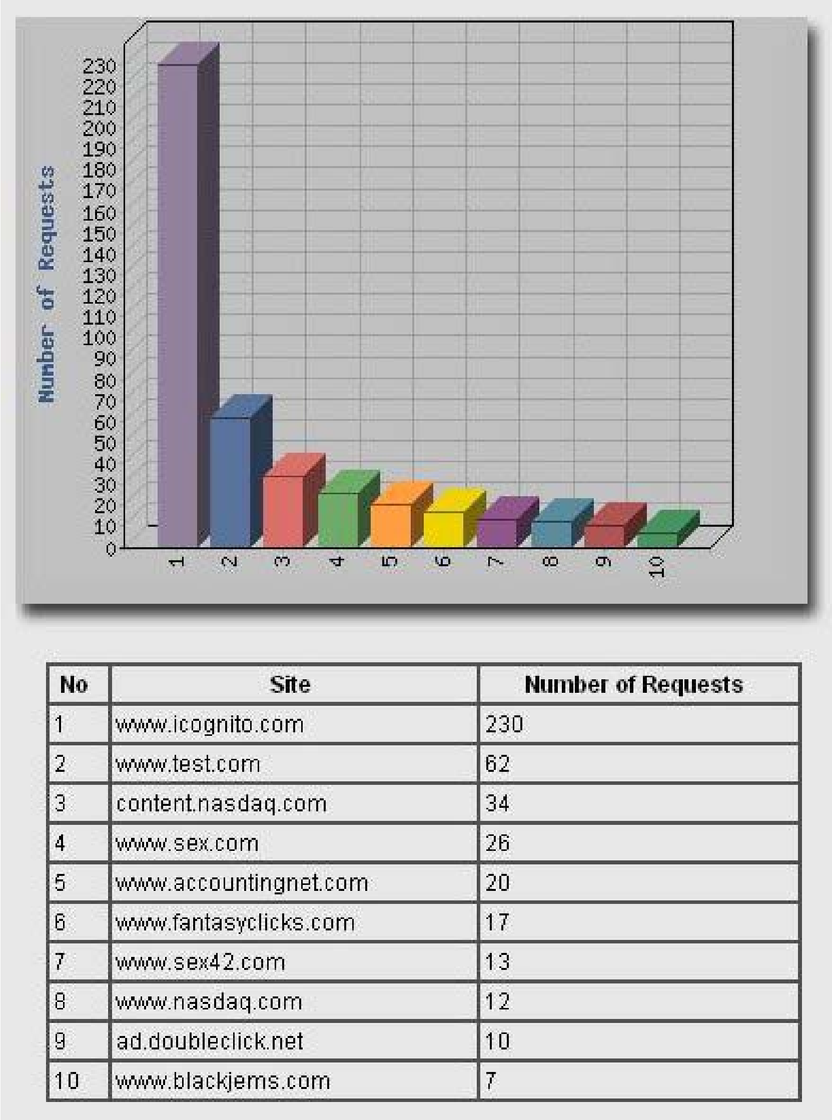
6 In the **Sort Order** field, select **Ascending** or **Descending** from the dropdown list to specify the order in which data is displayed in the report.

7 Select the **Draw graph** checkbox to include a graphical display of the report data, and select a graph type (**Bar** or **Pie**) from the dropdown list.

NOTE:

Note: Not all reports include both pie and bar graphs.

8 Click the **Run Query** button to generate the report. In the example below, the **Top Sites Requested by User** report is displayed as a bar graph and table.



No	Site	Number of Requests
1	www.icognito.com	230
2	www.test.com	62
3	content.nasdaq.com	34
4	www.sex.com	26
5	www.accountingnet.com	20
6	www.fantasyclicks.com	17
7	www.sex42.com	13
8	www.nasdaq.com	12
9	ad.doubleclick.net	10
10	www.blackjems.com	7

5 The following report parameters are not included in the previous example, but may appear for other reports:

All Categories/**Category**: Enables you to include all categories in the report, or a single specified category, for example, **Gambling** or **Adult**.

Filtering mode: Enables you to select the filtering mode that the report is based on, for example, **Block** or **Warn**.

Number of Top Users to Show: Enables you to limit the number of users included in the report.

Report Descriptions

There are five categories of reports that can be generated: Bandwidth, Category, Filtering Mode, Top Sites, and User. The various reports included in each of these categories are described in this section.

The table in each category contains for each report the report **Name** (as displayed in the *Reports* pane), the report **Title** (as displayed at the top of the relevant report parameter page) and a short **Description** of the report. All reports can be generated to show data over a defined time period.

Bandwidth Reports

Bandwidth reports enable you to view data on bandwidth consumption in your organization, broken down by factors such as subject category, requested sites and users.

Name	Title	Description
Category Analysis (KB)	Bandwidth consumption (KB) in each category	Displays the bandwidth consumption broken down by category.
Top Sites (KB)	Top bandwidth sites (KB)	Displays the sites consuming the most bandwidth.
Top Users (KB)	Top bandwidth users (KB)	Displays the users consuming the most bandwidth.

Category Reports

Category reports enable you to view data for the filtering categories, for example, gambling and sports, broken down by factors such as filtering mode, top users and top requested sites.

Name	Title	Description
Filtering Mode Distribution	Distribution of filtering modes for a given category	Displays category information broken down by filtering mode.
Top Sites	Top sites requested for a given category	Displays the most frequently requested sites in a category.
Top Users	Top users for a given category, based on number of requests	Displays the users most frequently requesting sites in a category.

Filtering Mode Reports

Filtering Mode reports enable you to view data showing activity in a filtering mode, for example, block or allow, broken down by factors such as top users and top requested sites.

Name	Title	Description
Top Sites	Top sites requested for a given filtering mode	Displays the most frequently requested sites in a filtering mode.
Top Users	Top users for a given filtering mode, based on the number of requests	Displays the users most frequently requesting sites in a filtering mode.

Top Sites Reports

Top Sites reports enable you to view data on the most frequently requested sites. Descriptions for the following Top Sites reports can be found in the previous categories, as follows:

Top Bandwidth Sites, refer to *Bandwidth Reports*, page 8-6.

Top Category Sites, refer to *Category Reports*, page 8-7.

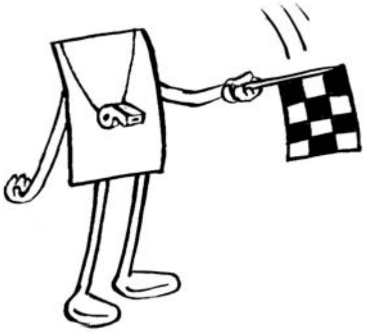
Top Filtering Mode Sites, refer to *Filtering Mode Reports*, page 8-8.

Name	Title	Description
Top Sites	Top sites requested by users	Displays the most frequently requested sites.

User Reports

User reports enable you to view data on individual users in your organization.

Name	Title	Description
Bandwidth Consumption by Category	Amount of bytes downloaded in each category	Displays the bandwidth consumption in each category for the user.
Top Sites	Top sites requested by a given user	Displays the sites most requested by the user.
Category Analysis	Number and proportion of requests made to each category	Displays the number and percentage of requests made by the user in each category.
Distribution by Filtering Mode	Number and proportion of requests that were blocked, warned or permitted	Displays the number and percentage of requests by the user that fall under each filtering mode.



Chapter 9

System Diagnostics

About This Chapter

This chapter describes the System Diagnostics provided in PureSight, which examine all of the PureSight components and modules connected to the PureSight Management Server.

- ✦ **Overview**, page 9-2, provides an overview of the System Diagnostics provided in PureSight.
- ✦ **Alerts**, page 9-3, describes the Diagnostics Alert section and provides detailed information on the possible alerts that may appear.
- ✦ **Filtering Server Diagnostics**, page 9-7, describes the diagnostics tests performed on each of the PureSight Content Filtering Servers connected to the Management Server.
- ✦ **Log Server Diagnostics**, page 9-8, describes the diagnostics tests performed on the PureSight Log Server connected to the Management Server.

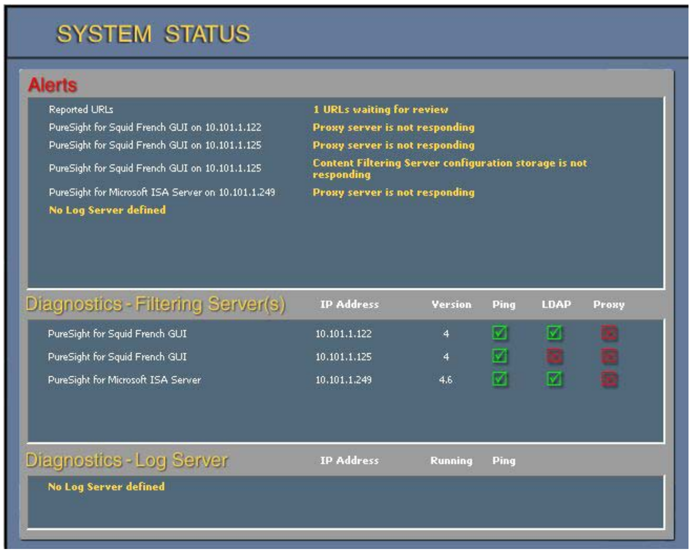
Overview

PureSight Diagnostics provides detailed analysis of all installed modules including PureSight Content Filtering Servers and PureSight Log Server. The PureSight Content Filtering Servers are checked for network access, configuration storage integrity and licensing. The PureSight Log Server is checked for network access MySQL access (if defined as the log storage).

The System Diagnostics pane contains the following sections:

- **Alerts** – contains important notifications regarding system malfunctions or other issues requiring immediate attention.
- **Filtering Server Diagnostics** – contains test results for each of the PureSight Content Filtering Servers connected to the Management Server.
- **Log Server Diagnostics** – contains test results of the PureSight Log Server connected to the Management Server.

The *System Diagnostics* pane is accessed from the menu in the Administration side bar by clicking **Diagnostics.**



SYSTEM STATUS

Alerts

Reported URLs	1 URLs waiting for review
PureSight for Squid French GUI on 10.101.1.122	Proxy server is not responding
PureSight for Squid French GUI on 10.101.1.125	Proxy server is not responding
PureSight for Squid French GUI on 10.101.1.125	Content Filtering Server configuration storage is not responding
PureSight for Microsoft ISA Server on 10.101.1.249	Proxy server is not responding
No Log Server defined	

Diagnostics - Filtering Server(s)	IP Address	Version	Ping	LDAP	Proxy
PureSight for Squid French GUI	10.101.1.122	4	☑	☑	☒
PureSight for Squid French GUI	10.101.1.125	4	☑	☒	☒
PureSight for Microsoft ISA Server	10.101.1.249	4.6	☑	☑	☒

Diagnostics - Log Server	IP Address	Running	Ping
No Log Server defined			

Alerts

The Alerts section displays system warning messages for all components installed on the Content Filtering Servers machines and Log Server machine.

Messages appearing in the Alerts section require Administrator attention, since they reflect an error state in the system.

The following tables include all possible alert messages and the suggested manner to address each given alert message.

Content Filtering Server Alerts

Alert	Suggested action
HTTP server does not seem to be running	Start the HTTP server
Filter configuration storage is not responding	The local configuration storage (OpenLDAP server) running on the PureSight Content Filtering Server machine is not responding. On Linux, start the slapd process. On Windows, start the PureSight Management Server service.
No License key	There is no license key assigned to the PureSight Content Filtering Server. Receive a license key from your vendor, and set the license key for the Content Filtering Server by editing the server. Refer to chapter 3, *Servers*, for detailed information.
Trial License will expire in less than 3 days	The PureSight Content Filtering Servers license key will be invalid in less than 3 days. Contact your vendor to receive a permanent license key and set the new license for the Content Filtering Server by editing the server. Refer to chapter 3, *Servers*, for detailed information.
Trial License has expired.	The PureSight Content Filtering Servers license key has expired. Contact your vendor to receive a permanent license key and set the new license for the Content Filtering Server by editing the server. Refer to chapter 3, *Servers*, for detailed information.

License error	The PureSight Content Filtering Servers license key is invalid. Contact your vendor to receive a valid license key and set the new license for the Content Filtering Server by editing the server. Refer to chapter 3, *Servers*, for detailed information.
No filtering server installed	Install a PureSight Content Filtering Server and initialize it in order to begin filtering Internet access.
Not responding to Ping request	The PureSight Content Filtering Server machine is not responding to a ping test. Ping test will fail if either the machine is down or ping is not enabled on that machine. Make sure that the machine is up and running and can be accessed from the Management Server
Uninitialized	The PureSight Content Filtering Server was installed but not initialized yet. Go to the Servers pane and click on the appropriate server to initialize it.
Disconnected from Management Server	The PureSight Content Filtering Server was disconnected from the Management Server and therefore does not receive configuration changes conducted on the Management Server. You should uninstall the PureSight Content Filtering Server.
Uninstalled	The PureSight Content Filtering Server was uninstalled and therefore should be disconnected from the Management Server. On the Servers pane, mark the server’s checkbox and click on **Delete Checked Items**.

Log Server Alerts

Alert	Suggested action
No Log Server defined	To enable logging and reporting, install PureSight Log Server.
Log Server does not seem to be running	Start the PureSight Log Server. On Windows, start the PureSight Log Server service. On Linux, run the pslogsrvd daemon.
Not responding to Pint request	The PureSight Log Server machine is not responding to a ping test. Ping test will fail if either the machine is down or ping is not enabled on that machine. Make sure that the machine is up and running and can be access from the Management Server
MySQL server does not seem to be running	PureSight Log Server is configured to log data to a MySQL database, which is not responding. Start the MySQL database and make sure the Management Server can connect to the database.
MySQL not responding to Ping test	The MySQL machine is not responding to a ping test. Ping test will fail if either the machine is down or ping is not enabled on that machine. Make sure that the machine is up and running and can be access from the Management Server

Filtering Server Diagnostics

The Filtering Server Diagnostics section provides detailed information regarding the result of each test conducted on each of the PureSight Content Filtering Servers defined on the Management Server.

Tests conducted on each of the PureSight Content Filtering Servers:

✦ **Ping** – tests responsiveness of the machine. Ping test will fail if either the machine is down or ping is not enabled on that machine.

✦ **LDAP** – tests the local configuration storage of the PureSight Content Filtering Server. If the LDAP test fails, then the LDAP server is not running and the PureSight Content Filtering Server is not filtering properly.

✦ **HTTP** – tests the responsiveness of the HTTP server with which PureSight Content Filtering Server integrates. If the HTTP test fails, then the HTTP server is not running and HTTP traffic is not enabled.

NOTE:

If any of the tests fail, an appropriate Alert message will appear in the Alert section of the System Diagnostics pane. Refer to the appropriate message documentation in order to address the problem.

Log Server Diagnostics

The Log Server Diagnostics section provides detailed information regarding the result of each test conducted on the PureSight Log Filtering Server.

Tests conducted on the PureSight Log Server:

- Running – tests the ability to connect to the PureSight Log Server. If the Running test fails, then the PureSight Log Server is not running and not logging any data.
- Ping - tests responsiveness of the machine. Ping test will fail if either the machine is down or ping is not enabled on that machine.

NOTE:

If any of the tests fail, an appropriate Alert message will appear in the Alert section of the System Diagnostics pane. Refer to the appropriate message documentation in order to address the problem.