



Super Scout[®]
Web Filter

Installation and User Guide

For Check Point™ FireWall-1®

NOTICES

Copyright © 1998-2001 SurfControl plc. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owner.

SurfControl USA

100 Enterprise Way, Suite A-110
Scotts Valley
CA 95066
USA Telephone: +1 831 431 1400
Fax: +1 831 431 1800

SurfControl Europe

Riverside
Mountbatten Way
Congleton
Cheshire
CW12 1DY
England

Telephone: +44 (0) 1 260 296259
Fax: +44 (0) 1260 296251

SurfControl is a registered trademark and SuperScout and the SurfControl logo are trademarks of SurfControl plc. All other trademarks are property of their respective owners.

Version 2.1-A published September 2001.

TABLE OF CONTENTS

Notices	ii
Table of Contents	iii
Product Overview	1
Chapter 1. SuperScout UFP Server Installation	2
Installation Considerations	2
System Requirements	3
Installing the UFP Server	6
Customizing the Default Configuration.....	12
On Solaris or Linux	14
Uninstalling the product.....	14
On Windows NT or Windows 2000	15
Registering the UFP Server.....	16
Registering on Solaris or Linux.....	17
Registering on Windows NT or Windows 2000	18
The SuperScout UFP Server Directory Structure	20
Chapter 2. Configuring the SuperScout UFP Server	25
Accessing the Administrator	26
Scheduling FastUpdates	29
Modifying the Cache Lifetime Setting	32
Setting the Redirection URL	33
Changing Authentication Status	34
Creating an Authentication Key	35
Working with the URL Exception List	37

Chapter 3. Configuring Check Point FireWall-1	39
Creating a Network Object.....	40
Creating a UFP Server.....	41
Creating a URI Resource	42
Inserting a URI Resource into a FireWall-1 Access Policy.....	46
Chapter 4. Installing the SuperScout Monitor and Reporter	47
System Requirements	47
Placement and Configuration Options.....	48
Installing the SuperScout Monitor and Reporter	54
Chapter 5. Configuring the Monitor and Reporter	56
Defining IP Ranges to Monitor	56
Selecting Monitor Settings.....	59
Database Tools.....	60
Upgrading from Access to SQL Server	63
Chapter 6. Using the SuperScout Monitor	66
Displaying the Monitor Window.....	67
About The Monitor Window	68
Accessing User and Site Activity Details.....	71
Displaying User Options.....	74
Displaying Site Options.....	74
Using the Real-Time Monitor.....	76
Managing the Monitor Database	78
Scheduling LiveUpdate of the URL Category List	81
Chapter 7. Reporting with SuperScout.....	83
Generating Reports.....	84
Selecting Report Criteria	85

Publishing Reports	86
Blocked Report Information.....	87
Using Web Reporting	88
Appendix A. SuperScout Categories	96
Appendix B. SuperScout Standard Reports.....	101
Quick Reports	101
Summary Reports.....	103
Comparison Reports.....	104
Detailed Reports.....	105

Product Overview

SuperScout Web Filter for Check Point FireWall-1 provides the ability to easily define and control user access to objectionable or non-business-related content. The product is comprised of two components:

- The SuperScout UFP Server component works as a plug-in to the FireWall-1 product, providing the SurfControl URL Category List of classified web sites to use in controlling access to the Internet
- SuperScout Monitor and Reporter, an optional component, is installed on a separate machine from the SuperScout on FireWall-1 inside the Intranet firewall to monitor users on a more granular basis

SuperScout Web Filter has been certified by Check Point as an OPSEC Compliant product. It was developed using the URL Filtering Protocol (UFP), which defines a Client/Server interface to categorize and control communication, based on a specific URL address.

UFP Caching

When FireWall-1 asks the SuperScout UFP Server to categorize a URL, it caches the reply, thereby reducing the number of UFP categorization requests made by FireWall-1 and improving throughput. SuperScout also informs FireWall-1 if all other URLs within the site have the same categorization. This can dramatically reduce the number of requests FireWall-1 will make to SuperScout.

You can use the SuperScout Administrator to configure how long FireWall-1 will hold a cached URL categorization.

Redirection URL

When a user requests a blocked site, the user is redirected to a URL you specify in the Administrator. Typically, this redirection URL points to a Web page explaining your company's Acceptable Usage Policy for Internet access.

Scheduling URL Category List Updates

The URL Category List categorizes over 1.8 million Web sites, with new sites added daily. You can use the SuperScout Fast Update to set up regular updates to the URL Category List at your convenience.

Enhanced Custom URL Support

User-defined URLs can be added to any of the standard SuperScout categories.

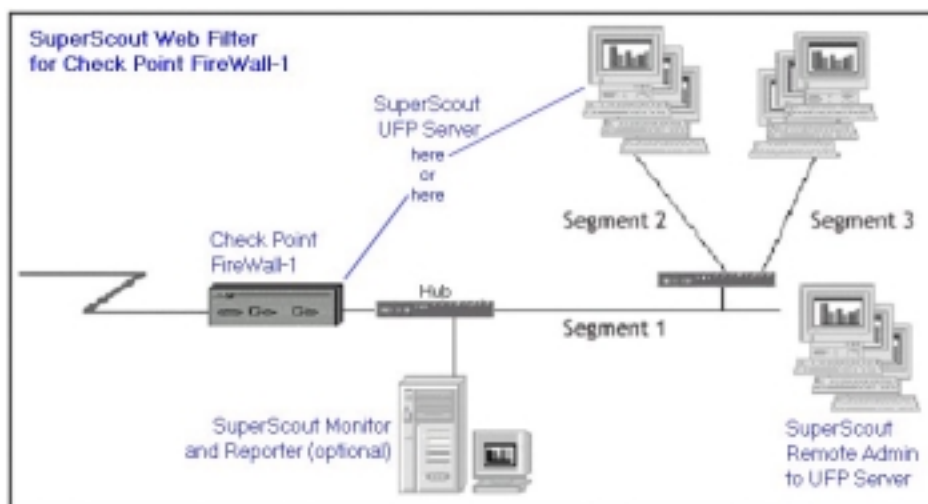
Chapter 1. SuperScout UFP Server Installation

This chapter explains how to install the SuperScout UFP Server component. Topics include:

- Installation Considerations
- System Requirements
- Installing the UFP Server
- Registering the UFP Server
- The SuperScout UFP Directory Structure

Installation Considerations

SuperScout UFP Server is position-independent on your network. It can be installed on the same computer as Check Point FireWall-1 or it can be installed on a separate computer. The only consideration is that any network devices between the two machines must not block communication between FireWall-1 and the SuperScout UFP Server. By default, the UFP Server listens on port 18182.



System Requirements

Before installing the product, check the table below to make sure that the system meets the system requirements for the product.

Installing on Solaris

For installations of SuperScout UFP Server on the FireWall-1 machine:

Operating System	Sun Solaris v2.6, Solaris V7 (32bit mode)
Applications	Check Point FireWall-1 v 4.1 or later with SP2 or higher
Processor	100MHz SPARC-class processor or higher
Memory	At least 256 MB, more recommended
Disk Space	Minimum 200MB free disk space
Web Administrator	MS Internet Explorer 5.0 or higher or Netscape Communicator 6.0 for Solaris 7 only

For installations of SuperScout UFP Server as a standalone on its own machine:

Operating System	Sun Solaris v2.6, Solaris V7 (32bit mode)
Applications	Check Point FireWall-1 v 4.1 or later with SP2 or higher
Processor	100MHz SPARC-class processor or higher
Memory	At least 128 MB, more recommended
Disk Space	Minimum 200MB free disk space
Web Administrator	MS Internet Explorer 5.0 or higher or Netscape Communicator 6.0 for Solaris 7 only

Installing on Linux

For installations of SuperScout UFP Server on the FireWall-1 machine:

Operating System	Linux kernel 2.2.12-20 or later and glibc 2.1.3-6 or later
Applications	Check Point FireWall-1 v 4.1 or later with SP2 or higher
Processor	Pentium II Processor or 333MHz or higher
Memory	At least 256 MB, more recommended
Disk Space	Minimum 200MB free disk space
Web Administrator	MS Internet Explorer 5.0 or higher or Netscape Communicator 6.0

For installations of SuperScout UFP Server as a standalone on its own machine:

Operating System	Linux kernel 2.2.12-20 or later and glibc 2.1.3-6 or later
Applications	Check Point FireWall-1 v 4.1 or later with SP2 or higher
Processor	Pentium II Processor or 333MHz or higher
Memory	At least 128 MB, more recommended
Disk Space	Minimum 200MB free disk space
Web Administrator	MS Internet Explorer 5.0 or higher or Netscape Communicator 6.0

Installing on Windows NT or Windows 2000

Operating System	Windows NT v4.0 Server with SP 6a or Microsoft Windows 2000 Server with SP 1 or Microsoft Windows 2000 Advanced Server with SP 1
Applications	Check Point FireWall-1v4.1 or later with SP2 or higher
Processor	Pentium II Processor 400MHz; Pentium III recommended
Memory	At least 256 Mb, more recommended
Disk Space	Minimum 200Mb free disk space
Web Administrator	MS Internet Explorer 5.0 or higher

For installations of SuperScout UFP Server as a standalone on its own machine:

Operating System	Windows NT v 4.0 Server with SP 6a or Microsoft Windows 2000 Server with SP1 or Microsoft Windows 2000 Advanced Server with SP 1
Applications	Check Point FireWall-1 v 4.1 or later with SP2 or higher
Processor	Pentium II Processor 400Mhz; Pentium III recommended
Memory	At least 128Mb more recommended
Disk Space	Minimum 200Mb free disk space
Web Administrator	MS Internet Explorer 5.0 or higher

Installing the UFP Server

The following is relevant to installations either downloaded from www.surfcontrol.com or from the SuperScout Web Filter CD.

Installing on Solaris or Linux

Creating the Directory

Before you install SuperScout UFP Server, you need to do the following:

1. Log in with `root` permission.
2. Create a new directory on a partition with enough space.

Uncompressing the SuperScout UFP Server file

1. Download the SuperScout UFP Server product from the SurfControl website into this new directory. If you have already downloaded SuperScout, then copy the archive to this new location making sure that you use binary mode if you are using an ftp transfer mechanism.
2. Change directory to this newly created one. If you now list the contents of this current directory you will see the SuperScout UFP Server installation archive.
3. Uncompress this archive (`tar.Z`) file by using one of two commands, either `compress -d <filename>` or `uncompress <filename>`
4. Next use the `tar -xvf <filename>` command to extract the complete directory structure.

Starting the Configure Script

After the extraction is complete, you are ready to start the Configure script. At the prompt type:

```
./Configure
```

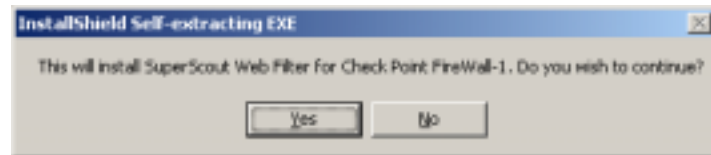
When the Configure script is run initially, it will set up the product as an evaluation copy with a remote admin port of 9999 for the Administrator (the Web interface of the product). Also, it will create a configuration database system and initialize all the default settings. This script only needs to be run once, at setup.

Installing on Windows NT or Windows 2000

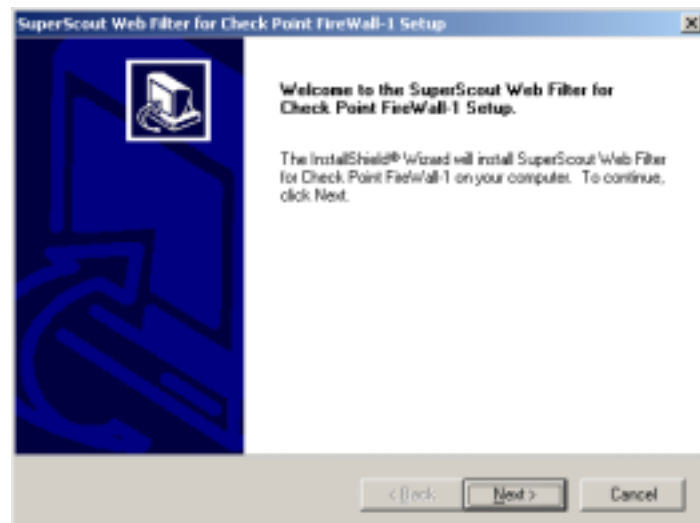
To install the SuperScout UFP Server product on to Windows NT or Windows 2000 place your CD in the CD drive to launch the Installation Wizard. This should start automatically, if it does not then use Explorer to navigate to your CD drive then select `Setup` from the SuperScout UFP Server folder.

If you have downloaded the product from the Web, navigate to the location of the downloaded file then double-click `setup.exe`.

When you start to install a message box will appear as follows:

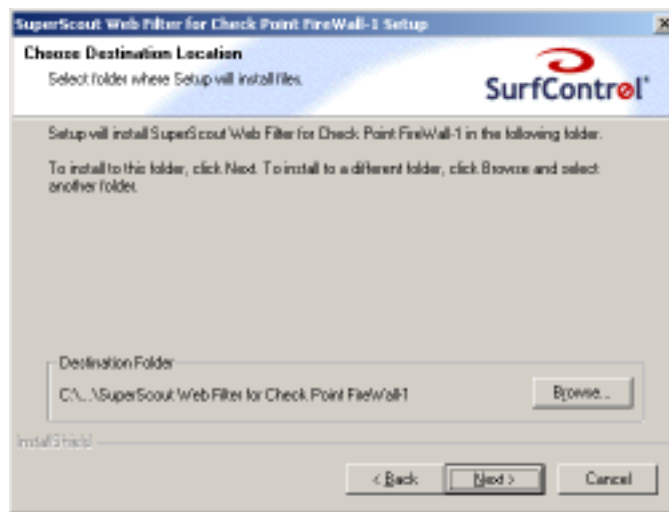


1. Click **Yes**. This will start the extraction of the files which in turn will start the installation. Once this is done, the first screen that you will see is the SuperScout UFP Server Welcome screen:



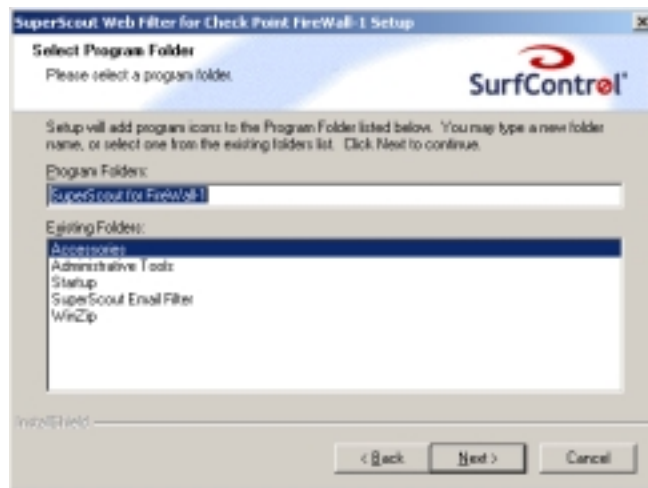
2. Click **Next**.

3. You will now see the SuperScout Web Filter for Check Point FireWall-1 License Agreement Dialog.
4. Click **Yes** if you agree to it's terms.
5. You will now be asked to choose a destination folder for the program:



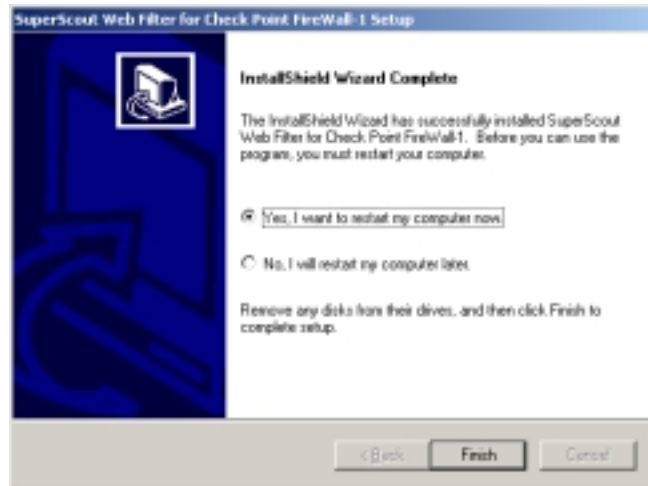
If you wish to install into a folder other than the default location of C:\Program Files\SuperScout Web Filter for Check Point FireWall-1 use the **Browse** button to navigate to another location. Click **Next** to continue.

6. You will then be asked which program folder you wish to install into:



7. The default program folder is SuperScout Web Filter for FireWall-1. If you are happy with this program folder then click **Next** to finish the installation.

8. You will then see a set up status box followed by an Install Wizard Complete dialog where you will be asked if you wish to restart your computer. This screen indicates that the installation of your SuperScout Web Filter for Check Point FireWall-1 is complete:



The installation procedure will install the product as an evaluation copy with a remote admin port of 9999 for the Administrator (the Web interface of the product). Also, it will create a configuration database system and initialize all the default settings

After Installation

On all platforms a default user account is created initially with admin/admin as the username/password for the Administrator. You should change this by creating a new user as soon as possible to avoid breaches in security. The default configuration for this product is:

- The UFP Server is running
- The port number is 18182
- The connection is unauthenticated

This default configuration can be altered at any time after installation.

Customizing the Default Configuration

In the Windows environment go to the command prompt and execute the radmin commands from the bin directory. In the Linux and Solaris environments go to the product installation directory and execute the radmin commands as follows:

To change the SuperScout Administrator port number

Type: `bin/radmin -l <port_number>`

Note: Restart the `stfw1` service for changes to take effect.

To add users and passwords

Type: `bin/radmin -a -n <uname> -p <pwd> [-i <ip_address>]`

Where `ip_address` is the IP address of the Client that requires access to the Administrator.

To remove a user

Type: `bin/radmin -d -n <uname>`

To display a list of users

Type: `bin/radmin -u`

Options for the radmin Command

Command	Description
<code>radmin -h</code>	Displays a syntax description (help screen).
<code>radmin -l port</code>	Sets the listening port for the Administrator.
<code>radmin -H path</code>	Sets the path to the html-files.
<code>radmin -v</code>	Displays version information.
<code>radmin -u</code>	Displays a user list.
<code>radmin -a -n name -p pass [-i IP]</code>	Adds a user where: name is the username pass is the password for this user IP is the allowed IP address for user; this is optional. If this option is not specified, the default value of 0.0.0.0 will be assumed. This default value will allow the user to access the Administrator from any machine.
<code>radmin -d -n name</code>	Deletes a user.

On Solaris or Linux

To start the UFP Server

On Solaris, the start and stop scripts are created in `/etc/rc2.d`. On Linux the start and stop scripts are created for run levels 2, 3, 4 and 5 in the respective subdirectories under `/etc/rc.d`. The start script will start the `cfgservd` daemon and the UFP daemon `stfw1d` automatically upon a reboot. Hence, a manual start after rebooting is not necessary.

To start the UFP Server manually

Type: `./stfw1 start`

If another instance of either daemon is running you will see a message stating that this is the case.

To stop the UFP Server daemon

Type: `./stfw1 stop`

Uninstalling the product

To remove the product installation type:

`./Uninstall`

On Windows NT or Windows 2000

The program is loaded as a service and is started automatically after installation.

To start the UFP Server manually

To start the UFP Server service:

1. Use the **Settings** option in the **Start** menu to navigate to the **Windows Control Panel**
2. Click on **Services** then highlight **SuperScout for Check Point FireWall-1**
3. Click the **Start** button

To stop the UFP Server manually

To stop the UFP Server service:

1. Use the **Settings** option in the **Start** menu to navigate to the **Windows Control Panel**
2. Click on **Services** then highlight **SuperScout for Check Point FireWall-1**
3. Click the **Stop** button

Note: An entry will be made into your active log file each time the service is started or stopped.

Registering the UFP Server

After you purchase the software, you will receive a license key file that enables you to register the software. As a registered user, you will be able to receive updates to the URL Category List.

Registering on Solaris or Linux

To register the software on Solaris or Linux go to the product installation directory and type:

```
bin/register -f <filename>
```

Options for the register Command

Command	Description
register -help	Displays a syntax description (help screen)
register -p	Displays valid product IDs
register -u user:company	Sets update user and company information
register -f filename	Imports a registration file

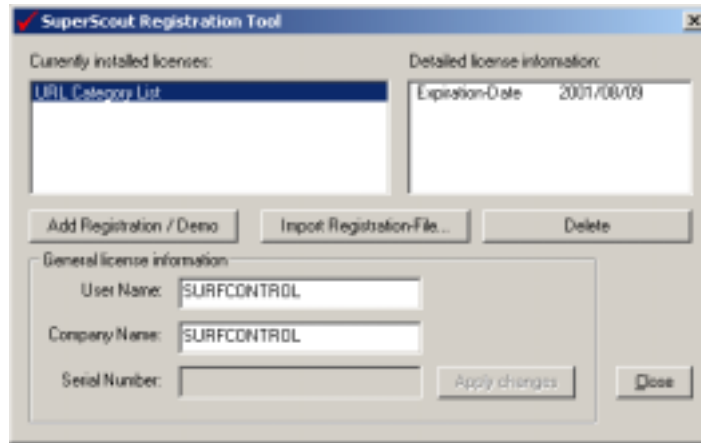
Note : If you wish to change/add user details using the `register -u` command and if the user or company names contain spaces, you should enclose the names in single or double quotes.

e.g. `register -u "Bob Smith"`

Registering on Windows NT or Windows 2000

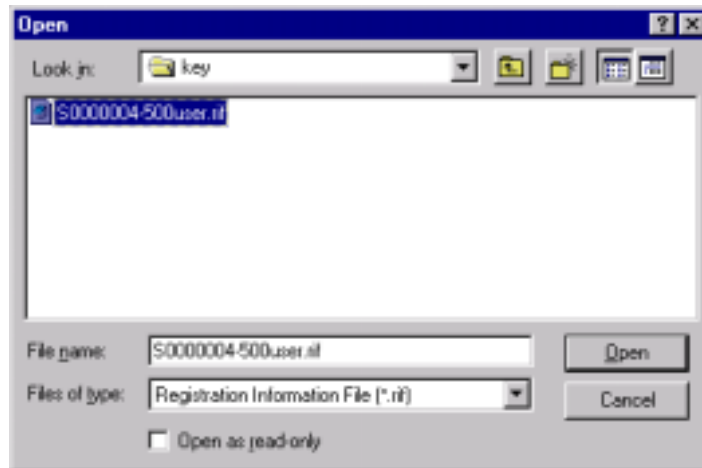
To register the software on Windows NT or Windows 2000:

1. Click on **Start > Programs > SuperScout for FireWall-1 then Registration**. This will launch the Registration tool:

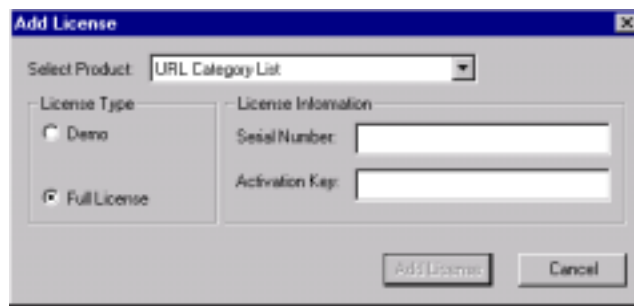


2. Ensure that your user name and company details are correct in the General license information edit fields. If you wish to change either of these details enter the new details into the edit fields. The **Apply changes** button will then become enabled.
3. Click the **Apply changes** if you have edited these details.
4. Click **Import Registration** file.

- Using Explorer browse to the location of your file. Double-click this file:



- Click **Open**. You should now see a message saying; 'Registration file successfully imported'.
- Alternatively, in the Registration Tool click **Add Registration / Demo** to type in your registration information. The Add License dialog will appear:



- Click on the **Full License** option to enter your information. This will enable the **License Information** section.
- Click **Add License** to save this information and return to the Registration Tool dialog.
- Click **Close** to save.

The SuperScout UFP Server Directory Structure

When installing on Solaris or Linux

Once you have extracted the directory structure from the `tar.z` file, you will see a list of subdirectories within your new directory. This section lists the directories and their contents.

Directory	File	Purpose
bin		Contains the files needed to run the actual product.
	<code>cfgservd</code>	Daemon that manages access to the configuration database. It is the only entity that is allowed to read from and write to this database. It must be started prior to the SuperScout UFP Server daemon and must be the last thing to be stopped.
	<code>cfgservd.pid</code>	Stores process ID of the <code>cfgservd</code> daemon.
	<code>confdb</code>	Holds the configuration settings. Only <code>cfgservd</code> can read or write to this file. In the event of unwanted changes being made to the set up of the product, it is possible to delete this file and then re-run Configure. This will return the configuration to its default settings. It is recommended however, that this is done only as last resort and caution must be exercised at all times.
	<code>init.tpl</code>	File that holds the initial configuration template.
	<code>initreg</code>	Tool that imports the <code>init.tpl</code> and using the <code>cfgservd</code> daemon, writes the information from this file to the <code>confdb</code> .
	<code>opsec_putkey</code>	Creates authentication keys. You will need to use this if you wish to create an authenticated connection.
	<code>register</code>	Used to register the product. It is invoked by Configure to register a demo license during initial setup. The user has to use this tool to fully register the product.
	<code>stfw1d</code>	UFP Server daemon that handles the FireWall-1 requests and also runs the web user interface. It must be started after <code>cfgservd</code> and stopped before it.
	<code>stfw1d.pid</code>	This file stores the process ID of the <code>stfw1</code> daemon.
	<code>radmin</code>	Enables the user to configure the Administrator

		settings.
data		Holds two files, which contain information about the category lists that SuperScout UFP Server supplies to FireWall-1.
	aura.csf	Contains the actual database for the category list. It is this file that is updated by FastUpdate when you have a registered version of the product.
	urllist.pri	There is an option to create additions or exceptions to the main category database. If you use this facility, any requirements you may have contrary to standard categorization are stored in this file. Note: urllist.pri is totally controlled by the user and is independent of the aura.csf file. Any alterations/additions made to this file will not change the aura.csf file.
doc		Contains files relating to information about this version of SuperScout UFP Server.
	License.txt	Contains the License agreement as a text file.
	ST Web UFP Server Install Guide.pdf	Installation and User guide for the product.
	release.txt	Information about this release such as release notes and known issues.
html		Sources for the Web based Administrator of SuperScout UFP Server.
logs		Any log files created when Logging is enabled.
scripts		Original templates for the scripts that were created when the Configure script is run. The scripts stfw1 and Uninstall are stored in the installation directory. The stfw1 script sets up the environment and calls the necessary binaries from the bin directory in the required sequence. Note: Do not try to run the binaries directly as it can lead to unexpected results. On Solaris, for automatic startup of the product at boot time, a start script (S90stfw1) is created in the directory /etc/rc2.d. This is a symbolic link to the stfw1 script in the installation directory. On Linux, the start script is created in each of the sub-directories under /etc/rc.d for run levels 2, 3, 4 and 5. Similarly kill scripts (k90stfw1) are created in these directories which are also symbolic links to the stfw1

		script. Use the Uninstall script to remove the installed product.
update		Once the product is registered, the Update directory becomes active. FastUpdate uses this as a working directory and as a place in which to store header information. The header information is in turn used by the FastUpdate Server to ascertain whether SuperScout UFP Server has the most recent aura.csf

When installing on Windows NT or Windows 2000

Once you have installed SuperScout UFP Server the installation directories will contain the following:

Directory	File	Purpose
bin		Contains the files needed to run the actual product.
	cfgservd.exe	This is the service that manages access to the configuration database and is the only
	opsec_putkey.exe	Creates authentication keys. You will need to use this if you wish to create an authenticated connection
	registerw.exe	This is used to fully register the product. It is invoked during the initial set up to register a demo license.
	stfw1d.exe	This is the service which implements the UFP Server that handles the FireWall-1 requests and also runs the web user interface.
	radmin.exe	This enables the user to configure the administrator settings.
data		Holds two files, which contain information about the category lists that SuperScout UFP Server supplies to FireWall-1.
	aura.csf	Contains the actual database for the category list. It is this file that is updated by FastUpdate when you have a registered version of the product.
	urllist.pri	There is an option to create additions or exceptions to the main category database. If you use this facility, any requirements you may have contrary to standard categorization are stored in this file. Note: urllist.pri is totally controlled by the user and is independent of the aura.csf file. Any alterations/additions made to this file will not change the aura.csf file.
doc		Contains files relating to information about this version of SuperScout UFP Server.
	License.txt	Contains the License agreement as a text file.
	ST Web UFP Server Install Guide.pdf	Installation and User guide for the product.
	release.txt	Information about this release such as release notes and known issues.

html		Sources for the Web based Administrator of SuperScout UFP Server.
logs		Any log files created when Logging is enabled.
update		Once the product is registered, the Update directory becomes active. FastUpdate uses this as a working directory and as a place in which to store header information. The header information is in turn used by the FastUpdate Server to ascertain whether SuperScout UFP Server has the most recent aura.csf

Chapter 2. Configuring the SuperScout UFP Server

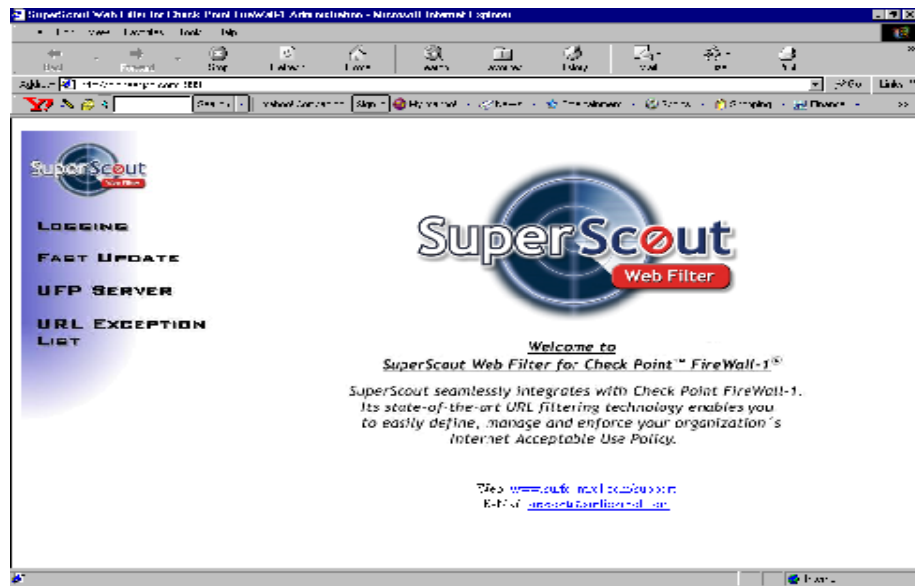
To make the SuperScout UFP Server services available to Check Point FireWall-1, both SuperScout UFP Server and FireWall-1 must be configured. This chapter provides the necessary configuration procedures for:

- Logging
- Scheduling FastUpdate for the URL Category List
- Changing Authentication Status
- Configuring the Redirection URL
- Working with the URL Exception List
- Modifying the Cache Lifetime Setting

Accessing the Administrator

SuperScout UFP Server includes a web-based Administrator that you can use to make day-to-day changes in SuperScout. Once you have installed SuperScout UFP Server and run the Configure script, the Administrator will be available at the default port of 9999.

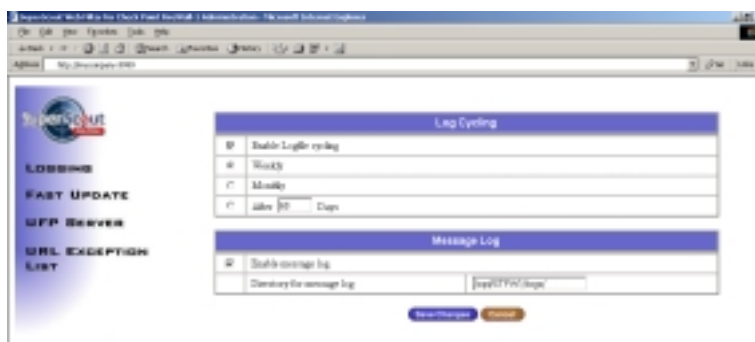
1. In a Web browser enter the URL, `http://host:9999`, where host is either the hostname or the IP address of the machine on which SuperScout UFP Server is installed.
2. A user authentication dialog will appear. Enter the default username as 'admin' and the password as 'admin'. You should change this username and password as soon as possible to prevent breaches in security.
3. You should now see the initial screen of the SuperScout Administrator:



Note: If you have installed SuperScout UFP Server and FireWall-1 on the same machine, you must install a suitable policy on the FireWall-1 to enable incoming connections on the SuperScout Administrator port. This policy should also allow outgoing HTTP connections to allow FastUpdate to function.

To enable Message Log File cycling

1. Click **Logging** on the Administrator menu. You now see the logging screen.
2. Click the check box to enable log file cycling:



3. Select the frequency of the cycling by choosing one of the time settings:
 - **Weekly:** Produces one log file per day to a maximum of 7 files. Starting on day 8, each day's file will be overwritten by new data. Log file format: MM_W_0X.LOG where x stands for the number of the weekday (0..Sunday to 6..Saturday)
 - **Monthly:** Produces one log file per month
Log file format: MM_M_mm.LOG where mm stands for the number of the month (1..12)
 - **After * days:** Produces one log file and overwrites it on the first day after the number specified.
Log file format: MM.LOG

Cycled log files are renamed and saved to the log directory
Log file format: MM_mmd.LOG

4. Once you have set your Logging Cycle, click **Save Changes**.

To disable Message Logging

1. Uncheck the Enable message log check box on the Logging screen.
2. Click **Save Changes**.

To change the directory for Message Log files

By default, log files are stored in the logs subdirectory, which is created in the directory where you installed the product. To change the default location of this directory:

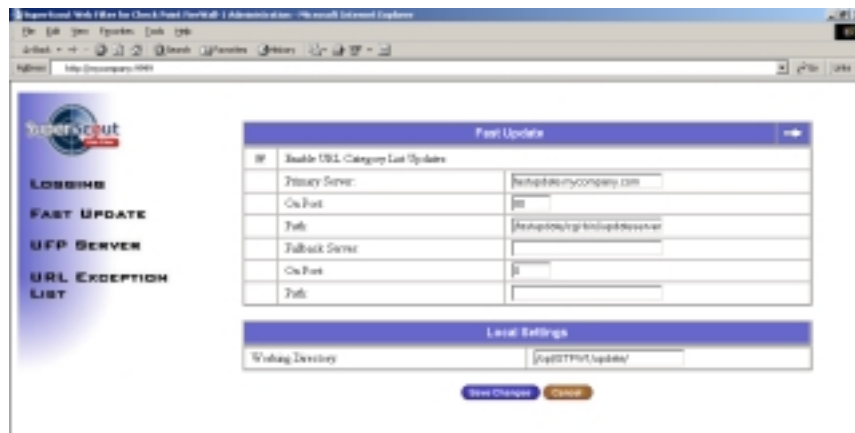
1. Enter the path in the “directory for message log” text box.
2. Click **Save Changes**.

Scheduling FastUpdates

It is advisable for your own Internet security (and that of your users) to regularly update your Category Lists. This ensures that new Web sites and those that have changed recently are still categorized correctly. We advise you to do this on a daily basis, however you can make less frequent updates should this be preferable. The Scheduler enables you to configure an update that occurs automatically at a time to suit you and your network. Once you have set your required update time, click **Save Changes** to immediately update the Category List. After this the Category List will be updated according to the settings that you have entered in to the Scheduler.

To Schedule a FastUpdate

1. Click **FastUpdate** on the Administrator menu. This displays the scheduler screen. Tick the **Enable URL Category List Updates** check box to show a detailed list:



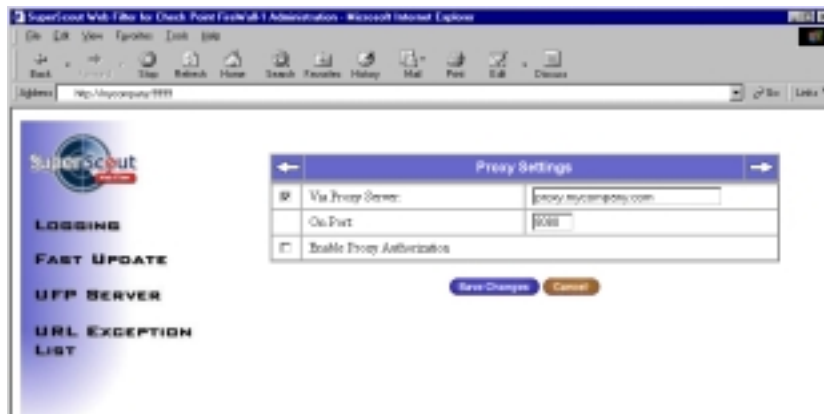
The screenshot shows the 'Fast Update' configuration screen in the SuperScout Web Filter for FireWall-1 administrator interface. The interface includes a sidebar with navigation options: LOGGING, FAST UPDATE, UFP SERVER, and URL EXCEPTION LIST. The main content area is titled 'Fast Update' and contains a table with the following settings:

IF	Enable URL Category List Updates
	<input checked="" type="checkbox"/>
Primary Server:	http://www.comcast.com
On Port:	80
Fails:	http://www.comcast.com
Fallback Server:	
On Port:	
Fails:	

Below the table is a 'Local Settings' section with a 'Working Directory' field set to 'http://www.comcast.com'. At the bottom of the form are 'Save Changes' and 'Cancel' buttons.

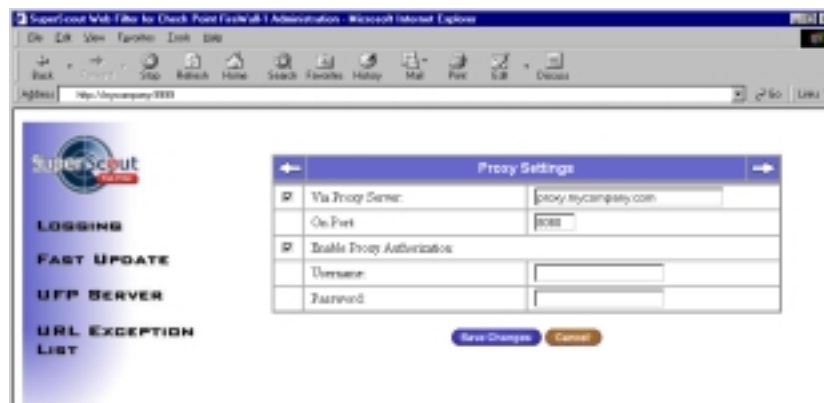
2. The default settings for the FastUpdate Server should not need to be changed at any time.
3. Click the right arrow link to go to the Proxy Settings screen.

If you are connecting to the Fast Update Server via a Proxy Server you can enter the relevant information in the Proxy Settings screen:



To set up a connection via a Proxy Server:

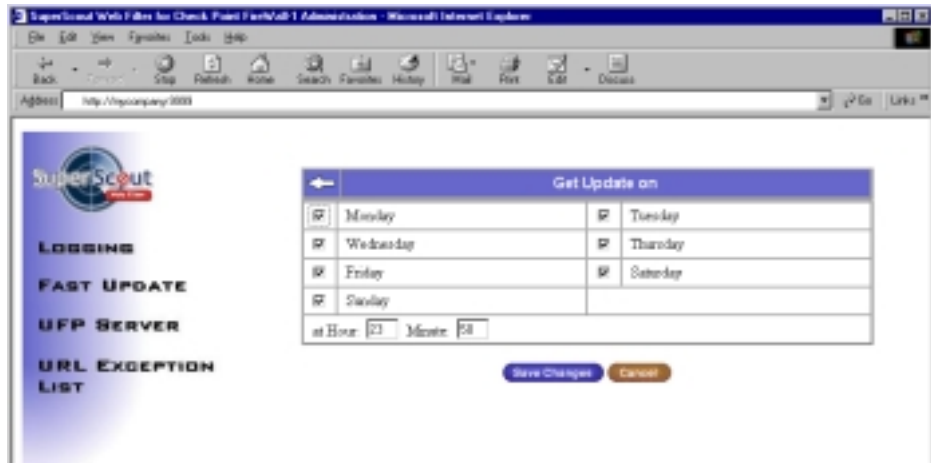
1. In the Proxy Settings screen check the **Via Proxy** check box.
2. Enter your Proxy Server address in the edit field provided.
3. Change the port number to your Proxy Server's port number.
4. If authorization is necessary check the **Enable Proxy Authentication** check box. This will enable extra edit fields where you can enter the Username and Password needed for your Proxy Server:



5. Enter this Username and Password.
6. Click the right arrow link to go to the next screen which enables you to configure the days and time for FastUpdate.

7. Enter the days and times on which you wish to schedule Fast Updates by checking the check boxes (for days) and entering the required time schedules in the **Hour** and **Minute** edit fields:

Note: All times use a 24 hour format



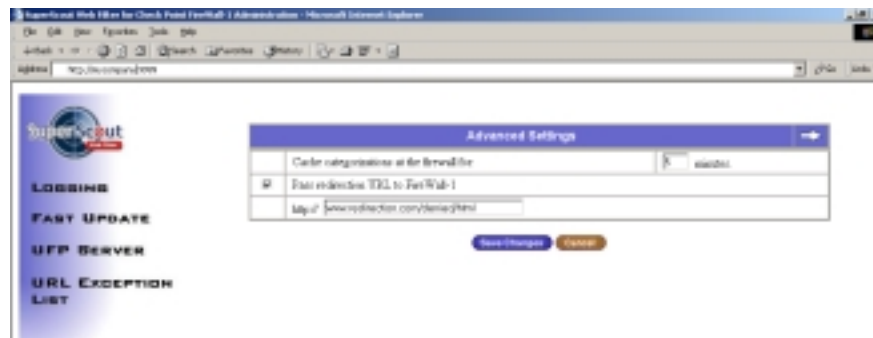
8. Click **Save Changes** to save your settings.

Modifying the Cache Lifetime Setting

When SuperScout UFP Server categorizes a URL, FireWall-1 can cache the categorization, reducing the number of categorization requests that FireWall-1 makes to the SuperScout UFP Server. You can set the length of time that FireWall-1 will keep a cached categorization; the default value is 5 minutes.

To Modify the UFP Caching Value

1. Click **UFP Server** on the Administrator menu.
2. This will take you to the **Advanced Settings** screen where you will see a table containing an entry called **Cache categorizations at the firewall for**. Next to this an edit field allows you to enter your required cache lifetime in minutes:



3. Enter the required number of minutes in this edit field.
4. Click **Save Changes** to save these settings.

Setting the Redirection URL

FireWall-1 v.4.1 SP2 has the ability to redirect a blocked connection to a URL specified by a UFP Server. Typically, the Redirection URL could explain your company's Acceptable Usage Policy.

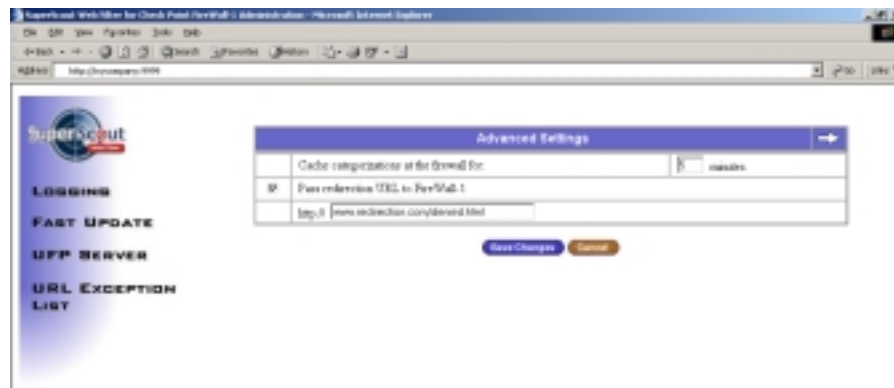
When users try to access a denied site, they will be redirected to the specified Redirection URL, a page where you can explain that access to the site has been blocked. The SuperScout UFP Server does not provide this page; it can be any URL hosted by any web server.

Note: You should ensure that the Redirection URL does not belong to one of the blocked categories.

If you wish to setup the Redirection URL, you can do that via the Administrator.

To Set the Redirection URL

1. Click **UFP Server** on the Administrator menu. Click the right arrow to go to the Advanced Settings screen:



2. Select the **Pass redirection URL to FireWall-1** check box. You now see an http:// edit field beneath the check box.
3. Enter the location of your preferred URL in here.
4. Click the **Save Changes** button.

Note: Always take care when altering the settings on this page as incorrect information can interfere with the functioning of SuperScout.

Changing Authentication Status

FireWall-1 will communicate with SuperScout UFP Server in one of two modes:

- Normal / unauthenticated — Data is transferred without any restrictions
- Authenticated — SuperScout UFP Server and FireWall-1 must verify each other's identities before any data can be transferred

Creating an Authentication Key

If you wish to use an authenticated connection you will need to create a key that will be used by SuperScout UFP Server and Firewall-1 to verify each other's identity. Creating a key involves running commands on both the FireWall-1 machine and the SuperScout UFP Server machine. Host name refers to the actual machine name, and not the name of a workstation object defined inside of the Check Point FireWall-1 software. To create an authentication key and configure an authenticated connection:

1. On the FireWall-1 machine find the FireWall-1 subdirectory, `conf`. In this directory you will find a file called `fwopsec.conf`. Edit this file by adding the following line:

```
server <ufp-server-ip> <ufp-service-port> auth_opsec
```

An example of this would be:

```
Server 1.2.3.4 18182 auth_opsec
```

2. Restart the FireWall-1 service for the changes to take effect.
3. Next, in the `bin` directory, run the command:

```
fw putkey -opsec <ufp-server-ip>
```

An example of this, using the settings above, would be:

```
fw putkey -opsec 1.2.3.4
```

4. The system will ask you to enter a key. Decide what pass phrase you will use as a key; this can be any combination of numbers and/or alphabetic characters, usually four characters in length.
5. On the SuperScout UFP Server machine, find the SuperScout `bin` subdirectory and run the command:

On Linux and Solaris

```
./opsec_putkey <firewall-1-ip>
```

On Windows NT or Windows 2000

```
opsec_putkey <firewall-1-ip>
```

An example of this on Solaris or Linux, using the settings above, would be:

```
./opsec_putkey 1.2.3.4
```

6. The system will ask you to enter a key. Enter the same key that you entered on the FireWall-1 machine. You should then see a message that authentication was successfully initialized.
7. Once you have configured your machines to use an authenticated connection, you then need to enable authenticated mode in the Administrator. Click **UFP Server** on the Administrator menu to go to the **Advanced Settings**. Then click the right arrow link to go to **UFP Server Settings**. Check the **Authenticated Connection** check box



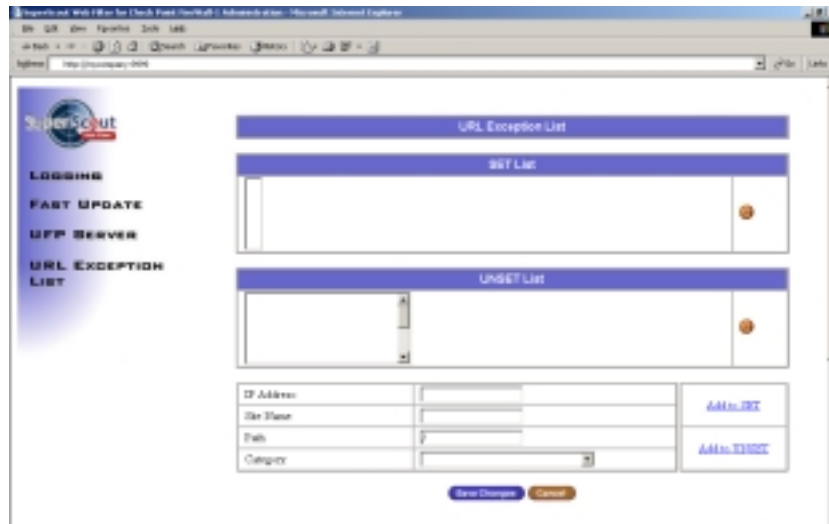
8. Click **Save Changes**
9. Restart the UFP Server for changes to take effect.
10. The UFP Server listens on port 18182 by default. If you need to change this port you can also do this at the bottom of this screen.

Note: The field 'IP Address' specifies the IP Address on which the listening port for the UFP Server will be established. The default value of 0.0.0.0 will establish a listening port for all available IP addresses on the UFP Server host.

Working with the URL Exception List

SuperScout UFP Server provides categorizing by site using the SurfControl URL Category List, which classifies over 1.8 million URLs into a variety of categories.

You can use the URL Exception List page in the SuperScout Administrator to change, add or remove sites from the URL Category List or to change the category of an existing list:



- Use the SET list to specify a new site to be added to an existing category or to change the category of an existing site in the URL Category List
- Use the UNSET list to specify sites as "None". These sites will be either blocked or allowed, based on rules you have set up on the FireWall-1 machine

To add a site to the SET List:

1. Click **URL Exception List** on the Administrator menu.
2. Type the URL information into the boxes at the bottom of the screen and select a category from the drop-down box.
3. Click **Add to SET** to add the URL to the exception list.
4. Click **Save Changes**.

To add a site to the UNSET List

1. Click **URL Exception List** on the Administrator menu.
2. Type the URL information into the boxes at the bottom of the screen and leave the category field blank.
3. Click **Add to UNSET**.
4. This will add the URL to the UNSET list and set the category as "None".
5. Click **Save Changes**.

Note: While the URL is included in this Unset list, no category can be assigned to it.

To remove a site from the SET or UNSET List:

1. Select the URL you want to remove.
2. Click on the trash can icon on the right side of the list.
3. Click **Save Changes**.

Chapter 3. Configuring Check Point FireWall-1

After installing SuperScout UFP Server, the FireWall-1 product needs to be configured to use the SuperScout URL Filtering protocol. FireWall-1 is configured using the Check Point FireWall-1 Policy Editor. The procedures in this subsection illustrate how to complete this configuration.

In the Check Point FireWall-1 Policy Editor:

1. Create a Network Object to represent the machine on which SuperScout UFP Server is installed.
2. Create a UFP Server object for the SuperScout service.
3. Create a URI Resource containing categories from the SuperScout list of URLs.
4. Insert the URI Resource into FireWall-1 access rules. The following example's Internet Acceptable Use Policy contains only two rules, which FireWall-1 enforces in descending order as follows:
 - Reject and log access to Web sites defined in the URI Resource named 'Block'
 - Allow access to all destinations not covered by the previous rule

Optionally, you can configure Authentication Connection between the FireWall-1 machine and the SuperScout UFP Server machine.

Creating a Network Object

FireWall-1 must have a network object defined for the machine on which SuperScout UFP Server is installed. If one does not already exist, perform the following procedure.

Note: If you have installed SuperScout UFP Server on the same machine as FireWall-1, you can skip this step.

To Create a Network Object

1. Start the Check Point Policy Editor and navigate through the interface until you see the initial rule base policy.
2. From the menu bar select **Manage** and then **Network Objects** to display the **Network Objects** dialog.
3. Once you can see the **Network Objects** dialog, click the **New** button and choose **Workstation** from the pull-down list. You will now see the Workstation Properties dialog.
4. Select the **General** tab in order to enter the details of the Workstation on which you have installed SuperScout.
5. In the **Name** edit field enter the name of your SuperScout UFP Server (this is the name of the workstation on which you have installed SuperScout).
6. In the IP Address edit field enter the IP address of this workstation. Alternatively, click the **Get address** button, which will automatically insert the IP Address of the workstation that you have already named.
7. Click **OK**.

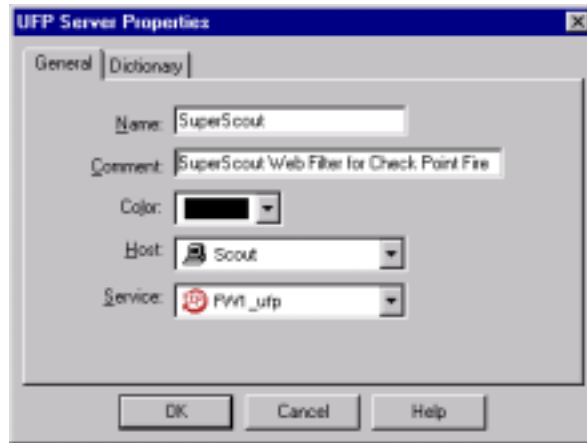
Note: This is the only tab from this dialog that you need to edit.

Creating a UFP Server

A UFP Server object represents a Network Object that provides URL categorization services. Once you have added the SuperScout network object, you need to create a new Server object.

To create a UFP Server Object

1. From the menu bar of the Check Point Policy Editor select **Manage** and then **Servers**.
2. In the Servers dialog that follows, select **New** then choose **UFP** from the drop-down menu to display the following dialog:



3. In the Name edit field of this UFP Server Properties dialog enter the name of the SuperScout Server. There is a Comment edit field available if you wish to enter any more details.
4. Next select your SuperScout Server from the list box entitled Host.
5. Click the **Dictionary** tab and then click **Get Dictionary** to retrieve the SuperScout URL Category List and details.
6. Click **OK** to exit and save the object.

Note: If you do not see the list of categories then this is an indication that there is a problem in the communication between FireWall-1 and the UFP Server. Common causes of this are that the UFP Server is not running or that the wrong host has been defined.

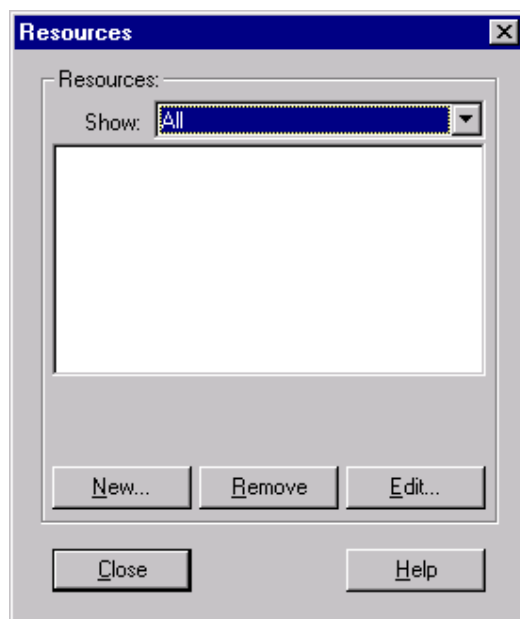
Creating a URI Resource

A URI is a Uniform Resource Identifier, of which the familiar URL (Uniform Resource Locator) is a specific class. A URI Resource is a collection of URIs. In the following example, the URI Resource contains the URLs within specified SuperScout categories.

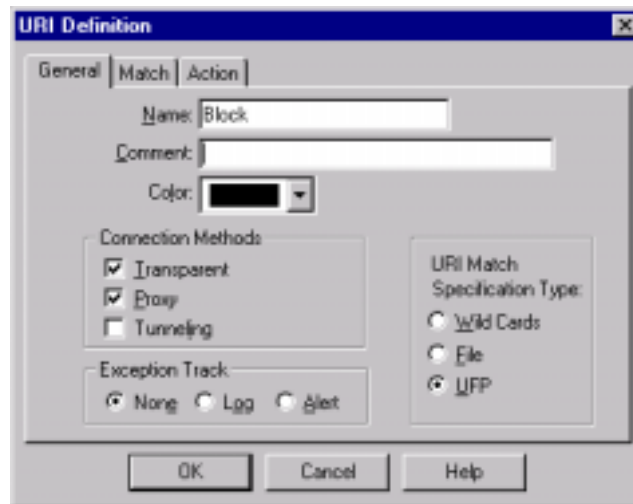
In the following procedure, a single URI resource is created for the SuperScout UFP Server.

To create a URI Resource

1. From the menu bar of the Check Point initial rule base policy select **Manage** and then **Resources** to display the following dialog:



2. Click **New** and select **URI** from the drop-down menu. This will display the following dialog:

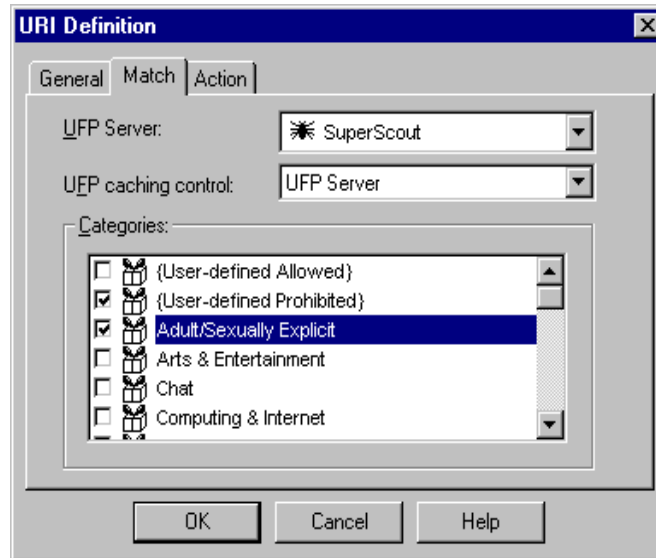


3. In the above example, the URI Resource is named 'Block' as we will be using it as an example of a common object contained in Drop or Reject rules.

Note: The name cannot have any spaces.

4. Fill in the details on the **General** tab.
5. In the section titled URI Match Specification Type, click the radio button for UFP.

- Next select the **Match** tab to display the following dialog:



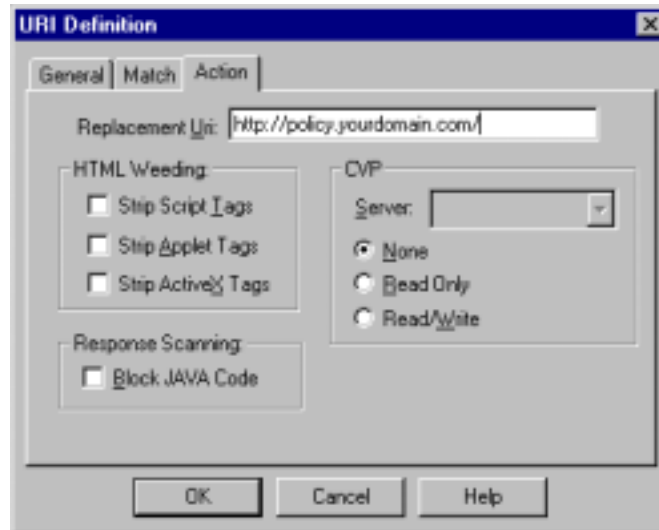
- Choose your UFP Server from the drop-down list. The category list associated with this Server will be displayed.
- For UFP caching control select **UFP Server**. By setting the UFP Caching Control to **UFP Server** the categorizations returned from SuperScout will be cached by FireWall-1 for a time period specified in the SuperScout Administrator UI.

Note: The ability to set the UFP caching control is only available in the Check Point FireWall-1 V4.1 SP2 or later. If you have an earlier version, you will not see this option.

- Check all categories associated with this resource, i.e. any URL categories that you would like to have blocked. These include specific categories such as Arts & Entertainment or non specific ones such as {User-defined Prohibited} and {User-defined Allowed}. You define the contents of these two User-defined categories by using the URL Exception List in the Administrator.

Note: Once you have done this, all URLs that fit into these categories will be grouped into a single resource bearing the name that you entered in the Name edit field of the General tab.

10. Finally select the **Action** tab in the URI Definition dialog:



11. If you want to specify a Replacement URI, type the URL to which the user will be redirected if they try to connect to a forbidden site. This would normally be the URL containing a message that explains your company's Acceptable Usage Policy. The next time that you access the **Resources** tab, you will see this resource already listed.

The Replacement URI field here is similar to the Redirection URL field in the SuperScout Administrator. The only difference is that the Redirection URL works on a global level, while the Replacement URI can be different for each URI resource. If both the Replacement URI and the Redirection URL are specified, then the Redirection URL will override the Replacement URI.

12. Click **OK**.

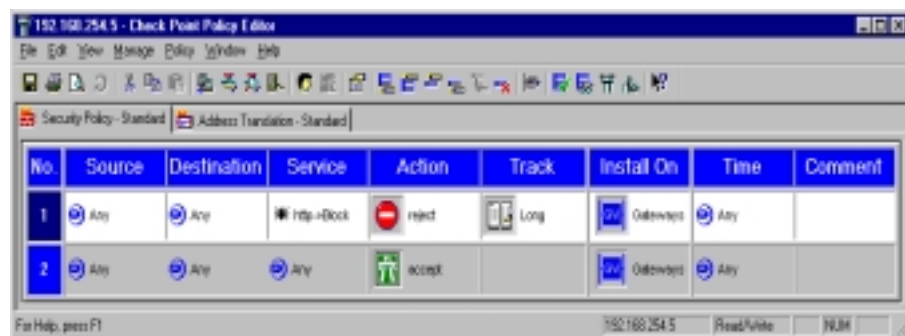
Inserting a URI Resource into a FireWall-1 Access Policy

You next need to define a rule for the HTTP traffic that should be checked by SuperScout. Go back to the rule base policy and add a new Accept rule (a rule that allows anyone access to anywhere at any time. Above this rule insert a new one that defines how you wish HTTP traffic to be blocked.

URI Resources are added to the FireWall-1 access policy by clicking the right mouse button over a rule's **Service** column. Place the URI Resource in the proper sequence to support your Internet Acceptable Use Policy.

To insert the SuperScout URI Resource into the FireWall-1 access policy

1. Access the **Check Point Policy Editor**:



2. Place the mouse cursor over the **Service** column and right click.
3. In the popup menu select **Add With Resource** to display a dialog that allows you to enter the URI Resource that you configured earlier.
4. In the **Action** column right-click and choose how you wish FireWall-1 to respond to any requests for access to the URLs grouped together under this URI resource.
5. Right-click in the **Track** column and choose the level of logging required.
6. Click the **Install Policies** button to install the policy.
7. Click **OK** to exit.

Chapter 4. Installing the SuperScout Monitor and Reporter

SuperScout includes the SuperScout Monitor and Reporter component. Once installed, SuperScout Monitor and Reporter will allow you to generate reports in real time or schedule them in a variety of formats. The Reporter service includes over 60 standard reports that can be easily customized to meet your needs.

This chapter explains the following topics:

- System Requirements
- Placement and Configuration Options
- Installing the SuperScout Monitor and Reporter

System Requirements

The table below lists the system requirements for the SuperScout Monitor and Reporter.

Operating System	Microsoft Windows NT 4 with Service Pack 6a or Windows 2000 Server with SP1 or Windows 2000 Advanced Server with SP1
Processor	Pentium II 400MHz processor; or higher; Pentium III recommended
Memory	128 MB; 256 MB recommended
Disk space	1 GB disk space
Network	Promiscuous mode Ethernet Card
Other	Microsoft Internet Explorer 5.01 with SP1 or higher

If you have a very high volume of network traffic, you may require a more powerful PC. Monitoring Internet access over a large, busy enterprise can cause your database to grow very quickly, so you should ensure that the machine you will be using has adequate disk space. For further information, see the Support pages on the SurfControl web site: <http://www.surfcontrol.com/support/>

Placement and Configuration Options

The efficiency and effectiveness of SuperScout Monitor and Reporter is dependent upon where it is installed in your network.

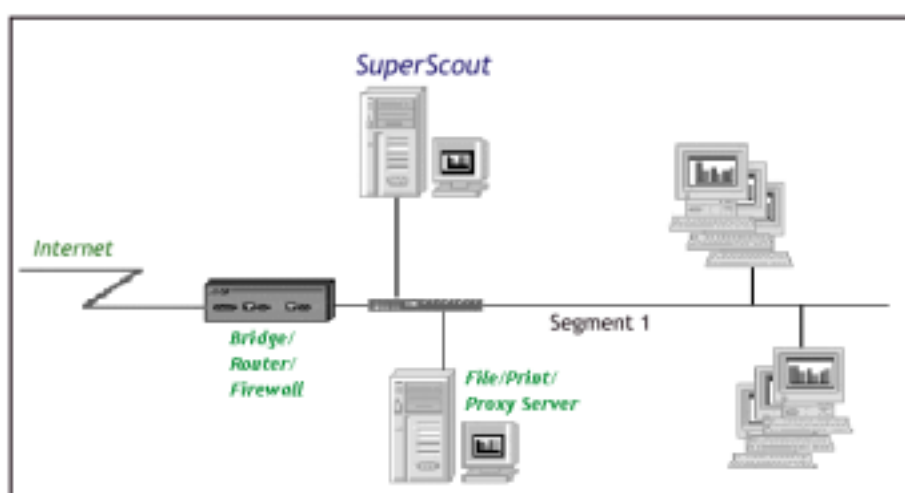
SuperScout Monitor and Reporter can be installed on any node and you can perform duplicate installations on other nodes throughout your network.

Note: For every copy of SuperScout Monitor and Reporter you will need to schedule individual LiveUpdates of the URL Category List.

Single-segment Network Placement

All of the machines in this network are connected to a simple hub. In this scenario, you may install SuperScout Monitor and Reporter on any suitable machine and you will be able to monitor Internet access across the network.

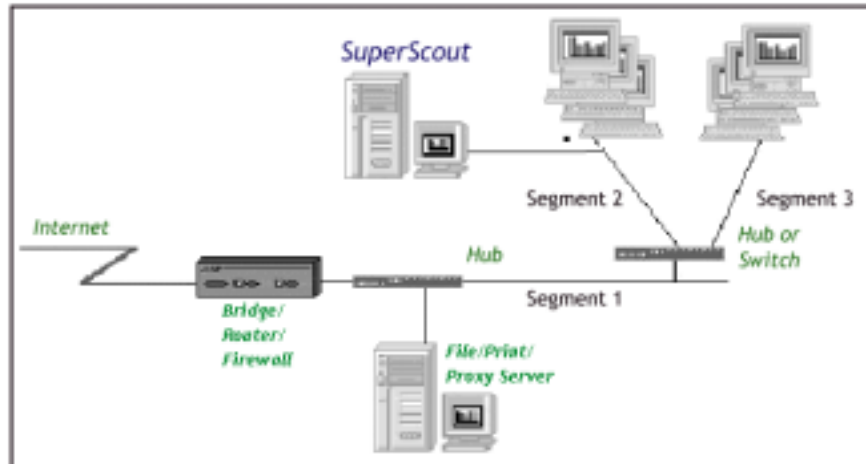
Note: SuperScout Monitor and Reporter should be installed on the same hub as FireWall-1 if multiple hubs are in use.



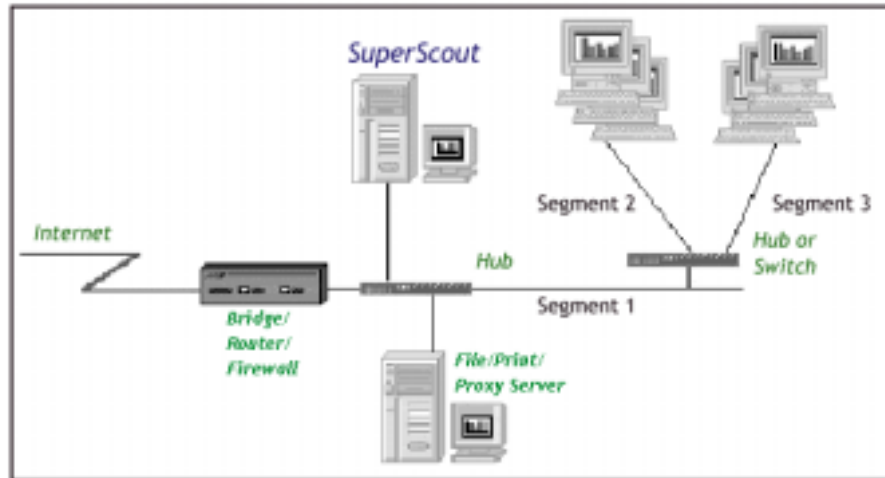
Multi-segment Network Placement

To ensure monitoring of all traffic in a multi-segmented network, you may need to install more than one copy of SuperScout Monitor and Reporter or strategically install it just before the firewall and external to all network segments.

For example: if the SuperScout Monitor and Reporter product is only installed on a machine in segment 2, it will not be able to see any traffic in segments 1 or 3. Clearly, if you wish to monitor only one segment, this will not present a problem. If, however, you wish to monitor activity on all of the segments you will need to install SuperScout Monitor and Reporter in a different location.



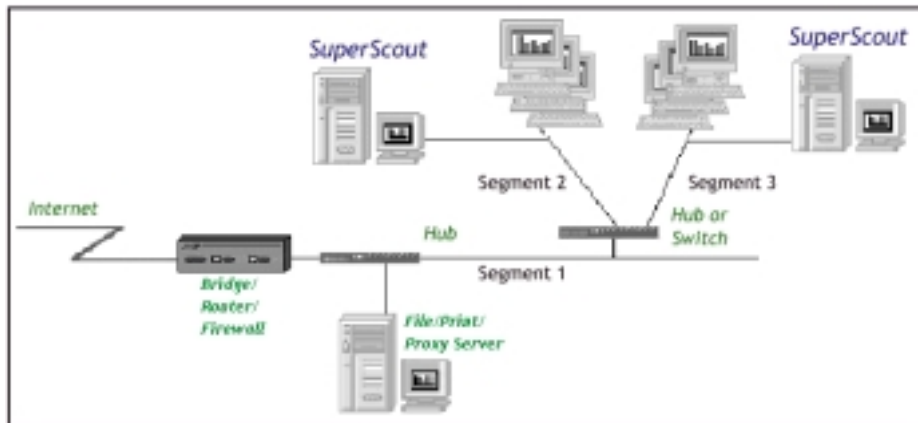
Below, the SuperScout Monitor and Reporter Server has been moved to segment 1. In this location, it will be able to see all of the traffic to and from the Internet because all Internet traffic will pass through the segment where SuperScout Monitor and Reporter component is installed.



Although this installation will monitor Internet traffic for the whole network, some local traffic will not be seen. If, for instance, you have an intranet Server installed on a machine in segment 2 being accessed by a machine on segment 3, the communication will not be seen by the SuperScout Monitor and Reporter. Again, this may or may not be important, depending on your Internet Use Policy.

To ensure monitoring of all of the traffic of a segmented network you may need to install more than one copy of the SuperScout Monitor and Reporter component.

In the figure below, two copies have been installed, one in Segment 2 and one in Segment 3. Segment 1 has been left unmonitored because it just has the File/Print Server.



Performance Considerations

There are a number of factors to take into account when deploying SuperScout Monitor and Reporter on your network.

The first thing to understand is the components within a Server that affect performance:

- CPU: A faster CPU or multiple CPUs will improve processing throughput.
- RAM: Larger amount of memory will improve performance through better buffering.
- Disk Subsystem: Probably the most important, a faster disk system (SCSI, SCSI II etc) will improve throughput.
- Virus Checkers and Services: Disable any that are not needed.

Database Options

There are other factors that come into play, and other options you can deploy in tuning the system. The size of the monitored database can also impact performance; not just recording to it but also accessing it for reports can severely impact system performance.

By default, SuperScout Monitor and Reporter will install and use a Microsoft Access database. If your configuration involves several collectors writing to a single database or if you will have large amounts of monitored data and frequent reports, you may wish to configure SuperScout to use a Microsoft SQL Server database.

Monitoring Options

What size and strength of system your monitoring requires depends on the amount of traffic (packets per second) that you need to monitor since the biggest impact on performance is the recording of monitored packets to the SuperScout Monitor database. Understanding the volume of network traffic, the mix of protocols, and the level of detail you want to monitor will help in sizing the correct system. For example, if you are not interested in monitoring FTP or telnet, you can disable these protocols in the SuperScout Monitor. Doing this reduces the monitoring workload.

You can further reduce the workload by deciding to not monitor certain workstations. This can be done through the Monitor User interface, for instance if you have a web Server inside your firewall you may not wish to see all the traffic associated with that system.

You can also reduce the amount of monitoring for each connection by recording only the top-level domain and not individual graphics that typically get accessed.

Distributing Services and Multiple Collectors

Your network may have such a large volume of traffic that no one system can handle it. In this instance you can deploy multiple Servers. These Servers can be physically deployed on different segments if you have a switched network, or they can be configured to only monitor certain sub nets. This will allow you to balance the load across several Servers, giving control to departments or groups so they will be able to monitor and control their own Internet Acceptable Use Policy. Separate monitor databases will be needed at each Server.

However, if you wish to use a single database to view and produce reports, you will need to consolidate the information. This can be done using flat files at each of the SuperScout Monitor and Reporter Servers (in this case known as collectors). Then use the database 'update' process to write the flat files from each of the 'collectors' to a single database.

Flat File Recording

Recording the monitored data into the relational database tables can consume resources your system may not have, so you can choose to configure SuperScout Monitor and Reporter to record data into a flat file, this is considerably faster than writing to the database.

However, data in the flat files cannot be seen by the Monitor and is not available for reports until you load the flat files into the SuperScout Monitor and Reporter database. You can automate this process somewhat, by setting a size limit on the flat files used, and opening a new temporary file when this limit is reached. A background update process can then periodically check when system resources are available to see if there is a closed temporary file and update the SuperScout Monitor database.

Installing the SuperScout Monitor and Reporter

When installing the SuperScout Monitor and Reporter component, you have the option to perform one of the following:

- **Complete Install** - Installs all of the components
- **Client Install** - Installs the administrative tools only

You must perform at least one Complete Install on your network. You may, for example, perform a Complete Install on a Server located in a computer room while installing only the Clients at administration points, such as managers' PCs.

Note on File Permissions: If you install the Client and Server components on different machines, it is essential that the Client have the appropriate file permissions to access the database resident on the Server.

To ensure smooth installation and configuration, a list of frequently asked questions and their answers are provided and kept updated on the SurfControl web site <http://www.surfcontrol.com>

To install the Monitor and Reporter component:

1. If you are installing from a CD, place the SuperScout CD in the drive and select `setup.exe`. If you downloaded the product from the SurfControl web site, find the location where you saved the download file, unzip it and run the `setup.exe` file. The Install Wizard will now start.
2. You will see the Installation Screen followed by the Welcome and then the License Agreement screen. Navigate through these screens clicking **Next** until you see the User Information screen. Here you will be asked for the following information:
 - Your name
 - Your company's name
 - Your serial number. Enter your serial number in the edit field if you are installing the full, purchased product. Alternatively click **Next** to install an Evaluation version.
3. Once you have entered this information you will be asked for a destination directory for the SuperScout files. Enter your desired location here or click **Next** for a default location.
4. The next screen that you will see will ask whether you wish to install a Complete or a Client version of SuperScout. To install the complete product, choose **Complete Installation**. If you only want to install the Client component, choose the **Client Only** installation. Click **Next**.
5. A Multiple NIC Option screen will appear. If you are installing on a Proxy Server select the external interface. Other multi-homed machines select the interface for the network you want to monitor. Only one interface can be monitored at a time. **Click Next**.
6. A screen will then appear informing you that Set-up is complete. Click **Finish**. You may be asked you to re-boot to complete the installation.
7. After you have installed SuperScout Monitor and Reporter and restarted the machine, the monitoring service will immediately begin tracking Internet traffic on the network. Each time the Monitor detects a request from a workstation it has not seen before, it will add the workstation's details to the Monitor's database and attempt to identify the real name of the PC and the name of the user logged in to that PC.

Chapter 5. Configuring the Monitor and Reporter

You can configure the Monitor services to:

- Define IP ranges to monitor
- Select **Monitor Settings** for categorization and username support
- Use the SuperScout database tools.

Note: You should change the advanced settings only if instructed to do so by SurfControl Support.

All these configuration options are available on the SuperScout Service Settings Property tab.

Defining IP Ranges to Monitor

Use the Subnet tab to define which IP ranges the software will use to either monitor or ignore. Check the **Monitor everything except...** box to make the list exclude the specified IP ranges.

To add a network address to the list

1. Right-click on the SuperScout Monitor and Reporter icon in the Windows taskbar (lower right of window).
2. Select **Configure SuperScout Service** from the popup menu.
3. Click the **Add** button.
4. In the following dialog, type in the network address and mask.



5. Click **OK** to close the dialog.

To remove a network address from the list

Note: There is no Undo or Confirm on this function, so be sure of the network address you want to remove before proceeding.

1. Right-click on the SuperScout Monitor and Reporter icon in the Windows taskbar (lower right of window).
2. Select **Configure SuperScout Service** from the popup menu.
3. Click on the network address you want to remove.
4. Click the **Remove** button.

To change a network address on the list

1. Right-click on the SuperScout Monitor and Reporter icon in the Windows taskbar (lower right of window).
2. Select **Configure SuperScout Service** from the popup menu.
3. Click on the network address you want to change.
4. Click the **Change** button.
5. In the dialog, change the information as needed.
6. Click **OK**

Selecting Monitor Settings

Use the Monitor Settings on the SuperScout Service Settings property sheet to define categorization and username support options.

To open the Settings property sheet

1. Right-click on the SuperScout Monitor and Reporter icon in the Windows taskbar (lower right of window).
2. Select **Configure SuperScout Service** on the popup menu.

To choose categorization settings

1. Click the option you want to use:
 - **No auto-categorization** disables all categorization
 - **SmartScan Only** disables categorization for all installed lists. Enables keyword categorization and is only user defined
 - **Auto-categorization on** enables all categorization
2. When finished, click **OK** to close the property sheet to close the dialog.

To select username support

1. Deselect **Enable username support** to disable all username discovery and use.
2. Select **Delay** before checking for a new user: (seconds) only if you have enabled username support. This specifies how often SuperScout should query each workstation to check for active users.

To specify TCP/IP name resolution options

The Monitor uses packet-sniffing technology to locate DNS packets, providing that SuperScout is located where DNS traffic can be seen.

1. Select **Enable Workstation name resolution** to enable resolution for workstation names, which can be either DNS or WINS.
2. Select **Enable Site name resolution** to enable DNS resolution for site names.

If DNS Packets are not seen and the settings are not selected, SuperScout will log IP addresses rather than site names.

Database Tools

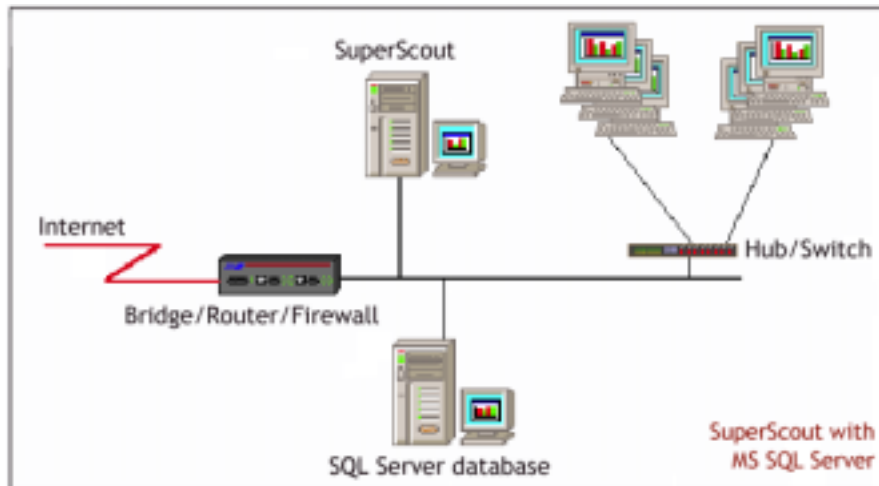
The Monitor database is configured, updated, and maintained using the SuperScout database tools. You can use these tools to:

- Create a Microsoft SQL Server database with the schema required by SuperScout
- Upgrade a Microsoft Access database to a Microsoft SQL Server database
- Select a Microsoft Access or Microsoft SQL Server database that you can use with SuperScout in place of the default Microsoft Access database. You should only select databases created via the SuperScout Create SQL Database command or known SuperScout-compliant databases
- Perform database purges
- Update the database from outside sources

Create a SQL Server Database

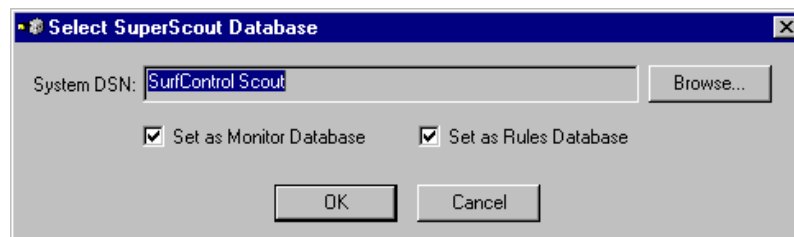
You can create a Microsoft SQL Server database to use in place of the default Microsoft Access database. After the database has been created, use the **Select Database** command to configure SuperScout to use the new Database.

Note: In order to run **Create SQL Database**, you must first install the **Microsoft SQL Client Connectivity** components. You must also have previously purchased **MS SQL Server** and have it installed on the **Server** where you will create the new database.



Using SQL Server with SuperScout Monitor and Reporter

1. With SuperScout Monitor and Reporter installed and running, select **Create SQL Database** from the **Database Tools** folder of the SuperScout Program menu.
2. Enter the following information into the SQL Server Setup dialog:
 - **Name** of the DSN entry that will be created referencing the SQL Database
 - **Database Name** that will be created on the SQL Server
 - **Server** where the database will be created
 - **Use Trusted Connection** indicating whether or not trusted authentication should be used to connect to the database
 - **Username** is the SQL username to use to connect to the database
 - **Password** is the SQL password to use to connect to the database
3. Execute the **Select Database** command on the **Database Tools** area of the SuperScout Start menu. The following dialog box appears.



4. Stop the SuperScout service.
5. Select **Browse**, then click **Machine Data Source** and select the name of the database you created earlier. SuperScout will now use the Microsoft SQL Server database rather than the default Microsoft Access database.
6. Start the SuperScout service.

Upgrading from Access to SQL Server

If you started using SuperScout with the default Microsoft Access database, you may want to move to SQL Server for improved performance or scalability. SuperScout provides the ability to move all the data in an SuperScout Access database to a SuperScout SQL Server database.

Before Upgrading

Before you begin, make sure that you have:

- Installed Microsoft SQL Server on your network and that there is a network connection between the machine where you are installing SuperScout and the machine where SQL Server is installed
- Installed SQL Server Client Connectivity pack on the SuperScout machine

To upgrade from Access to SQL Server

1. Select **Database Tools/Upgrade Access Database to SQL Server Database** on the SuperScout Start menu.

This starts the Database Creation Wizard that will guide you through the steps involved in creating a SQL Server database schema and moving your Access data and rules into the new SQL Server database.

2. After you finish this process, use the **Select Database** command to change the database that SuperScout uses to store data.

Select a Different Database

Use this command to specify the DSN entry of the database that you would like to use for the SuperScout Monitor and Reporter Service. This tool would normally be used in conjunction with Create SQL database to configure SuperScout Monitor and Reporter to use the database created by that command.

To select a database

1. Select **Database Tools** followed by **Select Database** on the SuperScout Start menu.
2. Choose any of the following options:
 - **Browse** selects the ODBC entry to use as the default database
 - **Set as Monitor Database** sets the selected System DSN as the default database to be used by SuperScout Monitor

Purging the Database

The purge command streamlines the data stored in the SuperScout database by removing detailed information while retaining key information about workstations, sites and groups. This process can make the database considerably smaller.

Note: Purging only removes connection details. All sites and users will remain in the database.

To purge a database

1. Select **Database Tools** followed by **Database Management** on the SuperScout Start menu. You now see the Database Management property sheet.
2. Select the **Purge** tab.
3. Select the database to purge.
4. Choose one of the following time options:
 - **Purge All** removes all connection details
 - **Save Today's Data** removes all but today's connection details
 - **Save data from the last <N> days** preserves data, where 'n' is the number of days to retain connection details
 - **Save data from DD/MM/YY** removes all connections details before the specified date
 - **Purge Range** removes all connections for the specified range
5. Click the **Purge** button to start the purge operation.
6. When the operation is completed, click **Close** to close the property sheet.

Chapter 6. Using the SuperScout Monitor

This chapter explains the following topics:

- Displaying the Monitor Window
- About the Monitor Window
- Accessing User and Site Activity Details
- Displaying User Options
- Displaying Site Options
- Using the Real-Time Monitor
- Managing the Monitor Database

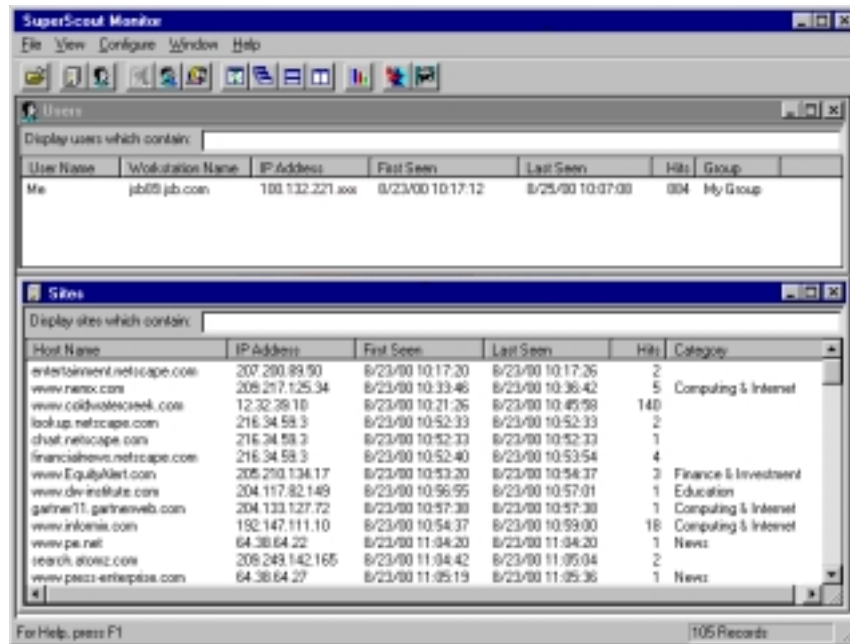
The SuperScout Monitor provides a view of activity by user and sites requested. As traffic is generated on the network, information about user activity is recorded in the SuperScout database and then displayed by the Monitor.

Displaying the Monitor Window

As SuperScout records information as it is seen, it may take some time for data to appear in the Monitor. To get an updated view of activity, click the **Refresh** button on the toolbar or press the F5 key.

To display the SuperScout Monitor

1. Select **SuperScout Monitor** on the **SuperScout Start Menu**. The following window will appear:



2. As SuperScout records information as it is seen, it may take some time for data to appear in the Monitor. To get an updated view of activity, click the **Refresh** button on the toolbar or press the F5 key.

If you have just started monitoring users, you may not see much data displayed, because the Monitor database does not yet contain a lot of monitoring information.

About The Monitor Window

This section explains the toolbar and menus available in the SuperScout Monitor.

The Toolbar

The tool bar is a short cut to the commands available in the menus. An explanation of each is provided below along with its associated menu.



Note: The Rules Administrator and the VCA are not available in this Edition of the SuperScout Monitor and Reporter component.

File Menu

Open Database — displays a dialog where you can select an alternative database to load into the Monitor

Exit — closes the Monitor

View Menu

Sites — displays the Sites pane

Users — displays the Monitored Users window

Site Detail — shows details for the selected window

User Detail — shows details for the selected user

Reports — opens the Reports dialog

Refresh — refreshes the display of monitored data

Configure Menu

Unmonitored Sites — displays which sites are omitted from the Monitor database. You can add a site to this list by clicking the **Add New Item** button (left button) and typing in the site name. Names or numbers are allowed as well as wild cards; for example; *.net for all workstations with .net at the end of their name.

The data for any site already stored prior to manual entry into the unmonitored site list will still exist and be reported on. If you want to specifically remove existing data, then use the **Don't Monitor** command when the site is selected in the Site window.

Unmonitored Users — prevents a user from being monitored. Any data collected so far is maintained in the database. You can add a user to this list by clicking the **Add New Item** button (left button) and typing in the username. Wild cards are allowed; for example; *.net for all user with .net at the end of their name.

Monitored Users — configures the users to be monitored. If you selected **Automatically monitor new users** during installation, new users detected by SuperScout will be added to this list automatically.

- Highlight the users you wish to monitor from the left box and press **Add**. All users selected, up to the maximum user count enabled by your product license, will be added to the Monitored Users list
- The Automatically monitor new users box will auto-detect new users and add them to the Monitored Users list, until the maximum user count is attained. Turn this option off if you want to maintain direct control of which users are monitored

Audit Levels — allows more information to be captured for users that are exhibiting abusive or prohibited behavior, as defined by your company's Internet Access Policy. You can monitor all HTTP traffic or only page-level traffic, which ignores images and other items contained on a page.

User Audit Level — sets audit levels for the selected user. Default Audit Level sets the default audit level for all users.

Monitored Protocols — defines which protocols (ports) to monitor. The default is to monitor only TELNET, HTTP, FTP and NNTP protocols.

- The Monitor all protocols option monitors everything. If you remove any protocols from the list, this option is automatically disabled
- The Configure Protocols option display a list of defined protocols and you can insert, delete, and configure a protocol name. For each new protocol, you must define the port numbers to be monitored

User Groups — enables you to add, rename, and delete configured groups. This group category would normally be used for 'departments' but could be used for any grouping required. Click the **Add** button to add a new group. To delete a group, select it and click the **Delete** button.

Screen Refresh — specifies how often the Monitor data display will be automatically updated.

User Menu

This menu is only displayed when the User window is active. Menu items are grayed out if a user is not selected.

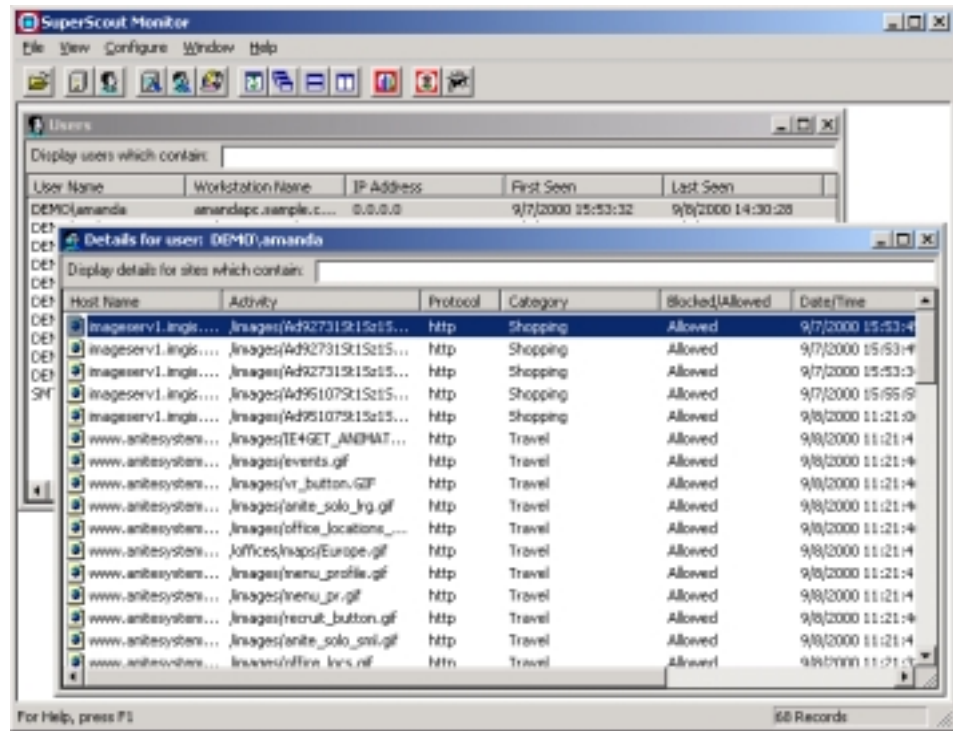
- **Rename** — displays detail for the selected user and allows you to change the label of the object as listed in the Monitor
- **Change Group** — moves the selected group of objects into a different group. By default, users are assigned to the default group *Everybody*
- **Don't Monitor** — stops tracking the user and removes their activity data from the SuperScout database
- **Delete** — removes the user from the database and removes their activity data from the SuperScout database

Accessing User and Site Activity Details

You can use the Monitor to see details of specific users and sites and sort on different columns in each window.

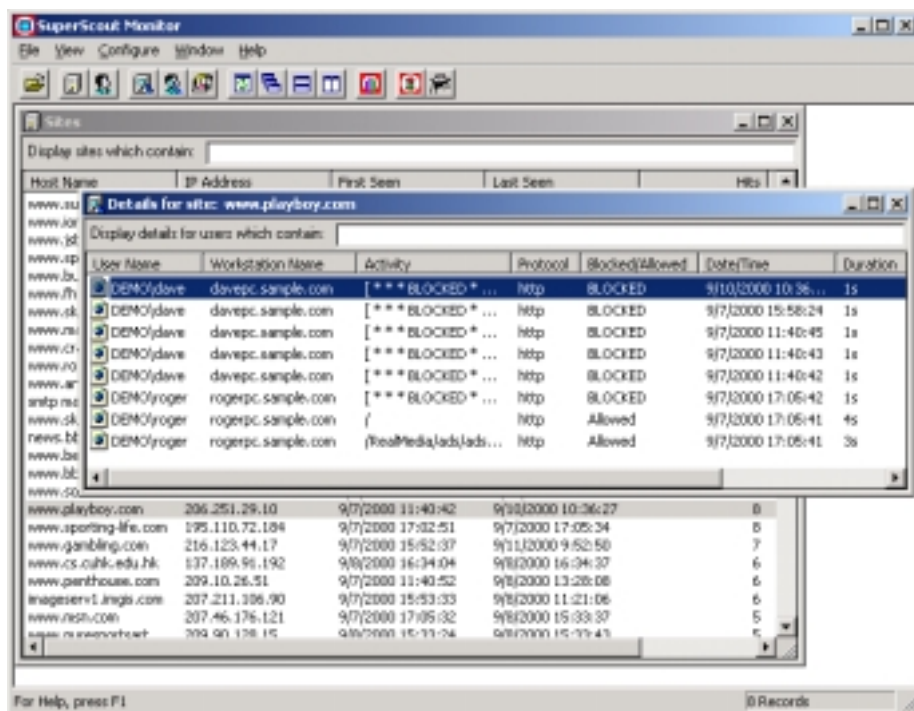
To view User Activity details

1. Double-click the relevant user.
2. A new window appears, displaying all activity for the selected user:



To view Site Activity details

1. Double-click the relevant site name.
2. A new window appears, displaying all activity for the selected site:

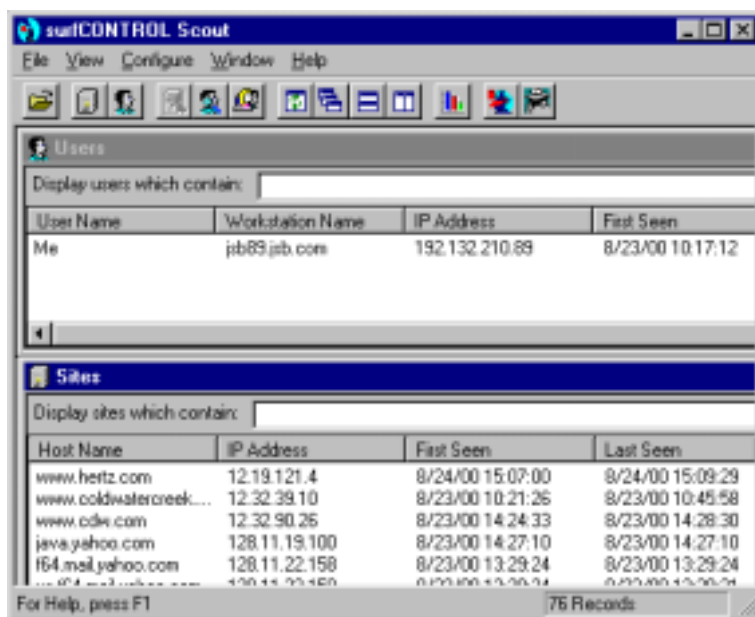


To sort by activities

Click on the label at the top of the pane that matches what you want to sort by. For example, click on IP Address in the Sites pane to sort all sites by their IP addresses.

To search for specific users or sites

1. Type the text you want to locate in the “Display...” box for either Users or Sites. The following window is displayed:



2. The Monitor displays all objects from the listing that contain the specified text string.

Displaying User Options

To display User options

Right-click on a user entry. You see the five commands explained here:

- **User Detail** displays detailed activity for the selected user. To see more detail for an entry, double-click it. This command has its own set of subcommands:
 - To jump to a site, right-click and select **Go to: http://<Site>**
 - To jump to a page, right-click and select **Go to: http://<Site...page>**
- **Rename...** changes the label for the selected user
- **Change Group...** moves the selected group of objects into a different group. By default, users are assigned to the default group *Everybody*
- **Don't Monitor** stops tracking the user and removes their activity data from the SuperScout database
- **Delete** removes the user from the database and removes their activity data from the SuperScout database

Displaying Site Options

To display Site options

Right-click on a site entry. You see the four commands explained here:

- **Site Detail** display detailed activity for the selected site. This command has its own set of subcommands:
 - To see other requests by the same user, double-click on the entry or select **User Detail** on the popup menu
 - To display all HTTP activity, including image files like .jpg and .gif files, select **Show All HTTP activity** on the popup menu
 - To jump to a site, right-click and select **Go to: http://<Site>**
 - To jump to a page, right-click and select **Go to: http://<Site...page>**
- **Don't Monitor** stops tracking the selected site and removes all previous connection details from the SuperScout database

- **Delete** removes the site from the database and removes all connection details from the SuperScout database
- **Go to: http://<Site>** displays the highlighted site

Tips for Monitoring Protocols

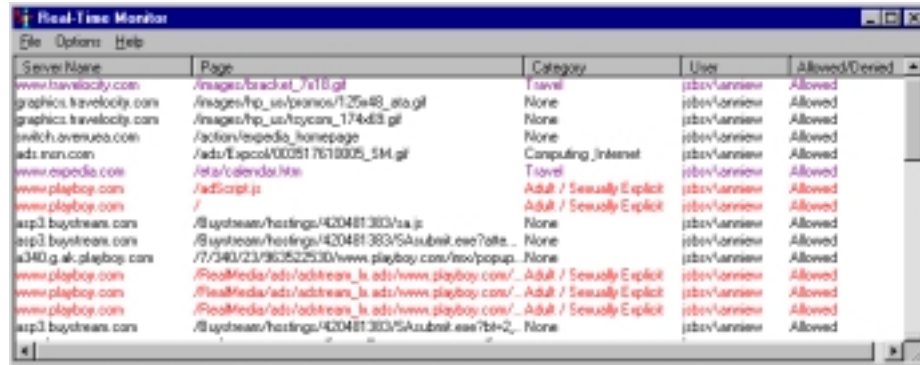
When analyzing SMTP (e-mail) traffic, depending on your Server configuration, outgoing mail may appear to have been sent from your mail Server rather than a particular workstation and vice versa. It is therefore important to look at the listing description to see who sent the mail and where they sent it. The monitor also records the contents of the subject line (this feature is disabled when evaluating the software).

Using the Real-Time Monitor

The SuperScout Real-Time Monitor shows activity on the network as it is happening in real time.

To display the Real-Time Monitor

1. Select **Real-Time Monitor** on the SuperScout Start menu. You now see the Real-Time Monitor:

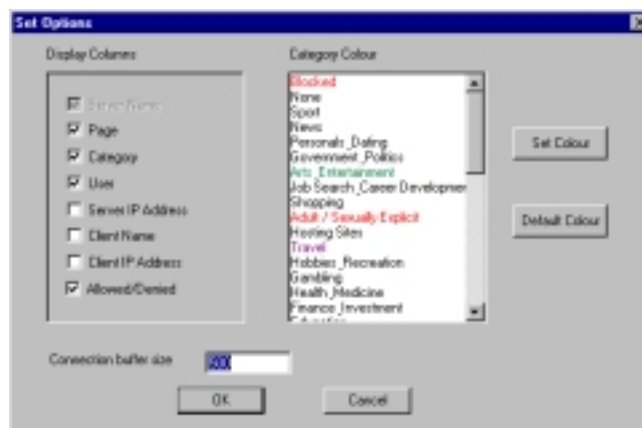


Server Name	Page	Category	User	Allowed/Denied
www.travelocity.com	/images/track_at_7x18.gif	Travel	jstev\jannsew	Allowed
graphics.travelocity.com	/images/hp_us/pranos/125e48_8to.gif	None	jstev\jannsew	Allowed
graphics.travelocity.com	/images/hp_us/toycars_174d83.gif	None	jstev\jannsew	Allowed
switch.oversueo.com	/action/expedia_homepage	None	jstev\jannsew	Allowed
ads.msn.com	/ads/Expcol/000517618005_5M.gif	Computing_Internet	jstev\jannsew	Allowed
www.expedia.com	/etc/calendar.htm	Travel	jstev\jannsew	Allowed
www.playboy.com	/adScript.js	Adult / Sexually Explicit	jstev\jannsew	Allowed
www.playboy.com	/	Adult / Sexually Explicit	jstev\jannsew	Allowed
asp3.buystream.com	/8uystream/hastings/420481383/va.js	None	jstev\jannsew	Allowed
asp3.buystream.com	/8uystream/hastings/420481383/5Asubmit.exe?offe...	None	jstev\jannsew	Allowed
u340.g.ak.playboy.com	/7/340/23/363522530/www.playboy.com/mo/popup...	None	jstev\jannsew	Allowed
www.playboy.com	/RealMedia/ads/adstream_hk_ads/www.playboy.com/...	Adult / Sexually Explicit	jstev\jannsew	Allowed
www.playboy.com	/RealMedia/ads/adstream_hk_ads/www.playboy.com/...	Adult / Sexually Explicit	jstev\jannsew	Allowed
www.playboy.com	/RealMedia/ads/adstream_hk_ads/www.playboy.com/...	Adult / Sexually Explicit	jstev\jannsew	Allowed
asp3.buystream.com	/8uystream/hastings/420481383/5Asubmit.exe?bl=2...	None	jstev\jannsew	Allowed

2. As traffic is generated on the network, information is shown in the Real-Time Monitor. To jump to a site listed in the Real-Time Monitor, double-click the site name.

To change options on the Real-Time Monitor

1. Select **Set** on the **Options** menu.
2. You now see a dialog where you can set the information displayed and set colors for any of the categories available:



The Display Columns section contains the information you can choose to display in columns of the Real-Time Monitor.

- **Server** — displays the site being visited. You cannot edit this setting
- **Page** — displays the page being visited
- **Category** — displays the category for sites that have been classified. If the site has not been classified, then “Unknown” is displayed
- **User** — displays the username of the person connecting the site
- **Server IP Address** — displays the IP address for the site
- **Client Name** and **Client IP Address** — display information about the Client

Connection Buffer Size — specifies the maximum number of lines to display in the Real-Time Monitor

- The **Category Color** section shows the current color settings for the SuperScout categories. You can edit the settings so you can more easily spot useful categories in the Real-Time Monitor
- **Set Color** — opens a dialog where you can set the color for the selected category
- **Default Color** — restores the default color (black) for the selected category

Managing the Monitor Database

As soon as you start SuperScout, it begins building a database of all of the Internet traffic it sees. On a busy network, this can cause the database to grow quickly so you should perform database maintenance tasks regularly.

You can use the Database Management command on the Database Tools menu to:

- Purge the database of detail-level data
- Archive a Microsoft Access database used with SuperScout
- Compact the Microsoft Access database used with SuperScout

Note: When performing database tasks, the SuperScout service is stopped. When the tasks are completed, the service is restarted.

The **purge command** streamlines the data stored in the SuperScout database by removing detailed information while retaining key information about workstations, sites and groups. This process can make the database considerably smaller.

Note: Purging only removes connection details. All sites and users will remain in the database.

To purge a database

1. Select **Database Tools** followed by **Database Management** on the SuperScout Start menu. You now see the Database Management property sheet.
2. Select the **Purge** tab.
3. Select the database to purge.
4. Choose one of the following time options:
 - **Purge All** removes all connection details
 - **Save Today's Data** removes all but today's connection details
 - **Save data from the last <N> days** preserves data, where 'N' is the number of days to retain connection details
 - **Save data from DD/MM/YY** removes all connection details before the specified date
 - **Purge Range** removes all connections for the specified range
5. Click the **Purge** button to start the purge operation
6. When the operation is completed, click **Close** to close the property sheet

To archive a database

1. Select **Database Tools** followed by **Database Management** on the SuperScout Start menu. You now see the Database Management property sheet.
2. Select the **Archive** tab.
3. Select the database to archive.
4. Choose any of the following options:
 - **Archive to** specifies the file name or directory where you wish to create the archived database. If you select **Unique database filename** you should select a directory. If not select a directory and provide a filename
 - **Unique database filename** specifies whether you want to create a unique file-name. If selected, the date that the archive was created will be used as part of the filename
 - **Purge Archive Database** specifies that once the archive has been created; the connection details of the source should be purged
 - **Create a DSN to the archive as named below** enables you to create a DSN entry that will reference the archived database
5. Click the **Archive** button to start the archive operation.
6. When the operation is completed, click **Close** to close the property sheet.

Note: This command can only be used with Microsoft Access databases. You cannot use this command if your SuperScout database is Microsoft SQL Server.

Compacting a database reduces its size by eliminating redundant space without removing any of its contents.

Note: This command can only be used with Microsoft Access databases. You cannot use this command if your SuperScout database is Microsoft SQL Server.

To compact a database

1. Select **Database Tools** followed by **Database Management** on the SuperScout Start menu. You now see the Database Management property sheet.
2. Select the **Compact** tab.
3. Select the database to archive.
4. Click the **Compact Now** button to start the compacting operation.
5. When the operation is completed, click **Close** to close the property sheet.

Each purchase of SuperScout includes a one-year subscription to the URL Category List that contains over 1.6 million URLs classified into over 35 Adult and Productivity categories. To keep your list updated with the newest URLs found and classified by the SuperScout filtering team, you should schedule regular updates at a time when your system/network load is low.

The URL Category List is updated nightly, so you can schedule nightly updates to take full advantage of the latest version of the list. Or you can schedule weekly or monthly updates, whatever fits your needs.

Scheduling LiveUpdate of the URL Category List

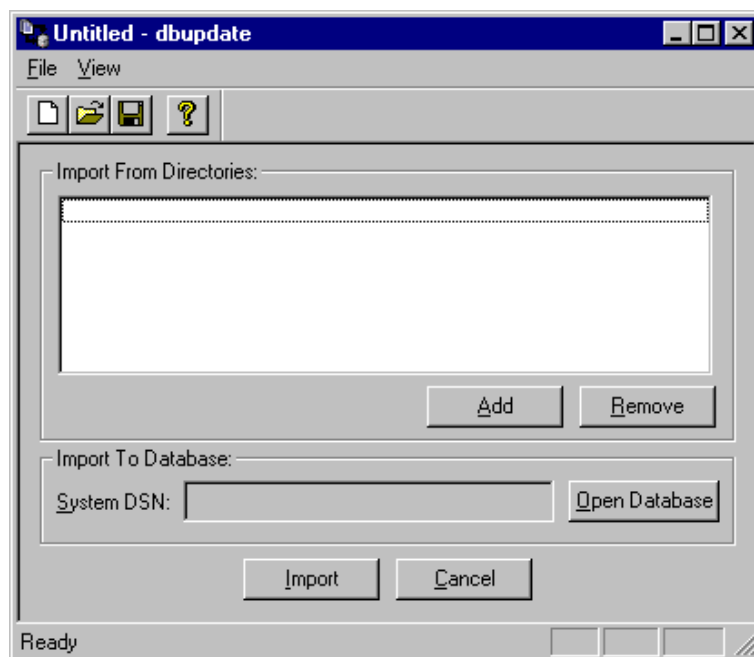
To schedule an update to the URL Category database

1. Select **Scheduler** on the SuperScout Start menu. You now see the SuperScout Scheduler dialog.
2. Click **Add Item** to open a new dialog where you can specify the details of the new event.
3. Choose **Category Database Update** as the item to configure, and then click on **Configure**.
4. Since this option is only available for registered users, you may be asked to provide registration details.
5. When finished with the configuration options, select the day, time, and frequency when you want the reports to be generated.
6. Check the box if you wish for SuperScout to retry if there is a failure.
7. Enter a description for the item. This is the name that will appear in the Scheduler dialog, so choose a name that represents the item clearly.
8. Click **OK** to finish configuring the item.

To update a database

If you are writing to a flat file, this option allows you to update the database with the flat files.

1. Select **Database Tools** followed by **Database Updater** on the SuperScout Start menu. You now see the **dbupdate** dialog:



2. Select **Add** and locate the flat file directory, usually c:\program files\SurfControl SuperScout\tmp.
3. Select the DSN entry of the SuperScout database that you would like to write the flat files written to.
4. Click the **Import** button to start the updating operation.

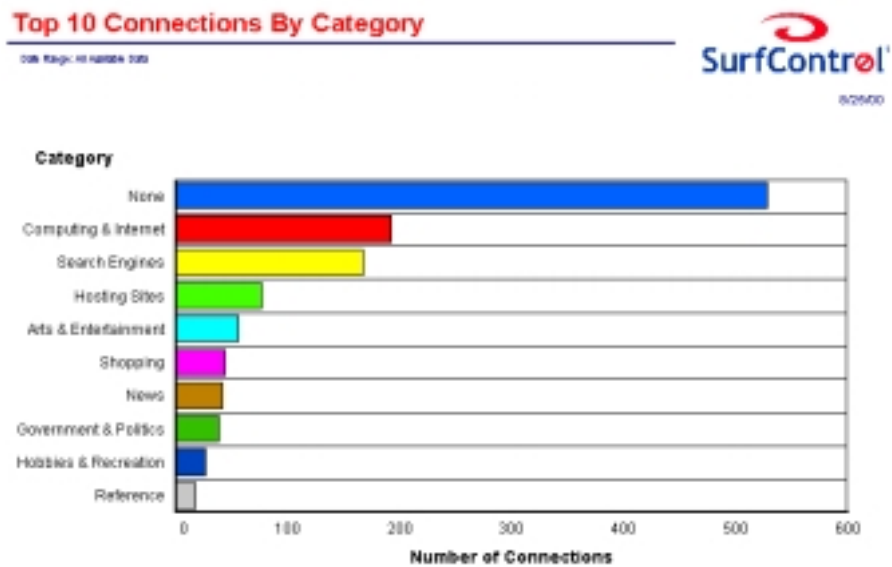
Chapter 7. Reporting with SuperScout

This chapter covers the following topics:

- Generating Reports
- Selecting Report Criteria
- Publishing Reports
- Blocked Report Information

SuperScout includes a range of quick, summary, comparative and detailed reports, which are available to assess your Internet and Intranet access.

For example, you can generate a report that shows the most requested connection by SuperScout category:



Generating Reports

You can generate over 60 standard reports from the SuperScout Monitor window. These reports are grouped into 4 categories:

- **Quick** reports, which use information in the entire database
- **Summary** reports, where you can specify criteria
- **Comparison** reports, where you can also specify criteria
- **Detail** reports, where you can specify several criteria to produce detailed analyses

When creating a report, you must decide the following criteria:

- The type of report to be run
- The criteria for the report if you have selected anything other than a quick report

After the report is run, you can then choose distribution options for it, such as email or a folder.

To generate a report

1. Click **Reports...** on the **View** menu or click the **Reports** button on the toolbar.
2. Click the report you want to run.
3. If you have selected any report other than a Quick report, you may specify report criteria and advanced criteria (see below). The defaults are to report on all data, all users, all sites, and so on.
4. Click **OK** to generate the report.

Selecting Report Criteria

The Time/Date section of the Report dialog enables you to specify the time period for the report. Use the **Exclude Time Range** button to run the report on all data collected except for the specified time range. This is useful if you want the report to exclude a weekend or holiday week.

The Advanced Criteria section enables you to select specific details in these areas:

- Users
- Groups
- Sites
- Categories
- Protocols

Selecting one of these items displays a dialog where you can specify the objects to include in the report. After you select criteria for an area, the button for that area appears with an asterisk to indicate that restrictions exist.

Use the **Reset** button to clear all criteria you have previously selected.

Publishing Reports

The completed report is always displayed on your screen, but you can also choose to print it, save it, or publish it to one of the following destinations:

- **Disk File.** Choose this option to save the report to a file, either locally or on the network
- **Exchange Folder.** Choose this option to store the report in a Microsoft Exchange folder. You must have your email program open to use this option
- **Microsoft Mail (MAPI).** Choose this option to send the report via email. You must have your email program open to use this option

For best results, choose either Word for Windows format. All reports—pie chart, bar chart, or table format—display well in Word format.

To print a report

Click the Printer icon in the toolbar of the Report window.

To publish a report

1. Click the **Envelope** icon in the toolbar of the Report window.
2. Select the format and destination for the report.
3. Click **OK**.

If the format and destination you have selected require additional information, you see one or more dialogs where you can select the values requested. For example, if you choose a Disk File as the destination, you see a dialog where you can specify the name and location of the file to be created.

Blocked Report Information

With the SuperScout and FireWall-1 product integration, FireWall-1 makes the decision to block HTTP traffic based on the URL filtering rules that are put in place at the firewall. Therefore, the SuperScout's blocked reports are not a feature that is available in this product bundle. Additionally, any field marked **Allowed/Denied** is not operational and will default to Allowed.

In order to obtain information on blocked site activity, reports should be run based on the categories set to be blocked by the firewall.

In the Summary Reports tab, both the **TOP N USERS** and **TOP N DEPARTMENTS** reports enable you to run reports by category and with user detail.

The **Report Criteria** section features Time/Date information, which allows you to define the date of usage and time of usage for the report through the following choices: All Available, Today, Last 7 Days, or Custom.

In the **Advanced Criteria** section the relevant fields for blocked site activity are: Users, Groups, Categories and Options.

- **Users** can be added or removed simply by selecting the appropriate criteria and pressing the **Add** or **Remove** selector button
- **Groups** can be added or removed simply by selecting the appropriate criteria and pressing the **Add** or **Remove** selector button
- **Categories** enables you to select various categories based on the blocked categories set in the Firewall-1 rule policy

Note: This information can be obtained in Check Point FireWall-1 by reviewing which categories have been selected to be blocked under the Policy Editor's URI panel

- **Options** opens into the General Options tab. The selectable criterion changes the N variable, which relates to the number of Departments or Users. By changing this variable, you can easily get the total (top) number of users against departments based on number of connections and site categories or top number of users based on number of connections and categories

Once the **Report Criteria** and **Advanced Criteria** are set, the resulting report will display the departments and users who have accessed sites that have been set to be blocked according to the company's Internet Acceptable Use Policy.

Using Web Reporting

This release of SuperScout includes the ability to remote execute reports through the Microsoft Internet Explorer 5.0 (and higher) web browser.

Note: Your browser must be Java-enabled to use web reporting.

To access Web reporting

1. Open a Web browser and type:
<IP address>:8888/surf/ WebReport.dll/StartPage
where IP address specifies the machine where SuperScout is running. For example, if you are running web reports on the machine where SuperScout is installed, you should type:
http://localhost:8888/WebReport.dll/StartPage
2. The default login for web reporting users is username **admin** and password **admin**.
3. SuperScout will then check to make sure the local machine you are using has the correct components installed. When you see the message " Installation OK" displayed, you can continue.
4. Click **Web Reporting** to access reports
or
Click **User Manager** to handle administrative tasks.

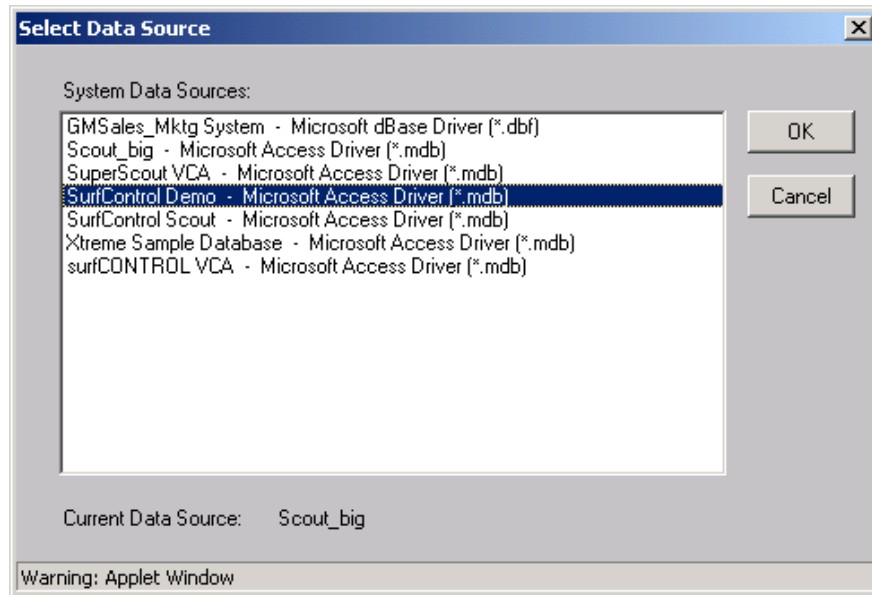
Note: For security purposes, you should change the default password for the admin account as soon as possible.

Selecting a Database

By default, Web Reporting uses the current SuperScout Monitor database, but you can select a different database to use when generating web reports

To select a database

1. Click the **Change Database** button at the bottom of the Web Reporting window. This will display a dialog where you can select a data source. (This dialog may take a short time to display, depending on the number of data sources and network locations):



2. Click the data source you want to use for Web Reporting.
3. Click **OK**.

The Web Reporting program will display the word “Ready” in the Report Description area when the new database has been loaded and is ready to query for reports.

Managing Access to Web Reporting

Only the administrator can add, delete, and change user accounts for SuperScout Web Reporting. The following procedures assume that you have accessed Web Reporting, selected **User Manager**, and logged in as the Administrator. The User Manager page looks like this:

To add an account

1. Click **Add User** on the Web Reporting User Manager page.
2. On the Add User page, enter a username and password.
Note: Each of these must be between 5 and 50 characters in length.
3. Click the **Add** button. You are now returned to the User Manager page, where you can see the new username displayed in the User List field.

To delete an account

1. Select the username you want to delete from the User List on the Web Reporting User Manager page.
2. Click **Delete User**. You now see a dialog asking you to confirm the deletion.
3. Click **OK** to delete the user.

To change the password for an account

1. Select the username you want to edit from the User List on the Web Reporting User Manager page.
2. Click **Change User**.
3. On the Change User Password page, enter the new password you want to assign to that user.
4. Click **Change** to change the password.

To change the Administrator password

1. Select **Change Admin** on the Web Reporting User Manager page.
2. On the Change Administrator page, enter the new password for the admin account.
3. Click **Change** to execute the change.

Note: For security purposes, you should change the default password for the admin account as soon as possible

Working with Databases

To reload the database

Click the **Reload Database** button to pick up the latest version of the database.

To select a different database

Click the **Change Database** button to select a different database.

Generating Web Reports

To generate reports, select the Web Reporting option when you access the Web Reporting feature via the correct URL for the SuperScout machine. The main page for Web Reports looks very similar to the dialog for standard reports.

To select a report to generate

1. Select the report you want to generate. To jump between types of reports (Quick, Summary, Comparison, and Detail) click on the desired tab.
2. Select the Report Criteria and Advanced Criteria for the report you want to generate. See below for more information on these criteria:
 - To select more than one item in a list, hold down the Shift key while clicking the desired items
 - If the **Options** button is available, you can click on it to select additional report-specific options, such as Browse Time and Workstation Cost per Hour
 - Click **Run Report** to generate the report and display it in the Web browser. Depending on the size of the database, the results may take a few minutes to be displayed
 - To display more than one report at a time, check the **New Window for each Report** box on the Reporting page

Selecting Date/Time Criteria

The Time/Date section of the Report dialog enables you to specify the time period for the report. Use the **Exclude Time Range** button to run the report on all data collected except for the specified time range. This is useful if you want the report to exclude a weekend or holiday week.

The screenshot shows a dialog box titled "Time/Date". It contains five radio buttons: "All Available" (selected), "Today", "Last 7 Days", "Last Full Month", and "Custom". To the right of the radio buttons are two columns of date and time selection fields: "Start Date:" and "End Date:" (with dropdown arrows), and "Start Time:" and "End Time:" (with dropdown arrows). Below these fields are two checkboxes: "Use same start and end times per day" (checked) and "Exclude Time Range" (unchecked).

Selecting Advanced Criteria

The Advanced Criteria section enables you to select specific details in these areas:

The screenshot shows a dialog box titled "Advanced Criteria". It contains six buttons arranged in two rows: "Users...", "Groups...", "Sites..." in the first row, and "Categories...", "Protocols...", "Options..." in the second row. Below these buttons is a checkbox labeled "Display selected criteria on report" and a "Reset" button.

Selecting one of these items displays a dialog where you can specify the objects to include in the report. After you select criteria for an area, the button for that area appears with an asterisk to indicate that restrictions exist.

Click the **Display selected criteria on report** option to show the settings you have selected on the report.

Use the **Reset** button to clear any of the criteria you have previously selected.

Selecting Options

The **Options** button in the Advanced Criteria section provides additional options for specific reports. If a report does not allow you to select **Options**, the button is grayed out and unavailable when you select that report.

The available options are

- **Top N Value:** used to specify the value of N in reports named “Top N”. The default value is 10
- **Browse Sensitivity.** The default is 3 minutes. If a request has been made by the user and no subsequent request is made by that user, SuperScout assigns the specified value as the time the user browsed the requested page
- **Browse Duration Threshold Alert.** The default is 10 minutes
- **Workstation Cost Per Hour.** The default is 10. SuperScout uses the PC’s regional settings, so the value is 10 dollars for PCs using US settings and 10 pounds for PCs with UK settings

Note: The Reset button does not clear Options settings. You must open the Options dialog and edit values manually.

Viewing Web Reports

Web reports display in modified browser window. You can use the icons in the window tool bar to print the report or email the report to someone.

The example below shows a web report for Top N Sites, where N has been specified as 12:



The screenshot shows a browser window titled 'SuperScout Web Reporting - Microsoft Internet Explorer'. The page content includes the title 'Top 12 Sites', the SuperScout logo, and a date range of '11/20/00 00:00:00 to 11/27/2000 23:59:59'. Below this is a table with two columns: 'No of Connections' and 'Site'.

No of Connections	Site
2240	www.1stn.com
987	contexts.sandient.com
928	apps.vickets-systems.com
668	www.rstbc.com
611	go.1stn.com
727	www.af.com
578	www.1stn.com
452	www.google.com
382	www.microsoft.com
278	home.microsoft.com
253	www.page3.com
253	rstbc.com

To print a web report

1. Click the Printer icon in the toolbar.
2. The report is sent to the default printer for your machine.

Note: There is no mechanism for specifying a printer for Web Reporting in this release. You must change the default printer instead.

To email a web report

1. Click the email icon in the toolbar.
2. Choose **Send Page** on the pull-down menu. This displays a new email message with the report shown as an HTML attachment.
3. Enter the To: information and click **Send**.

Note: The recipient may not see some reports correctly if they have never run SuperScout Web Reporting. This is because the charts in Web Reporting require a Java applet that is installed when you first access Web Reporting.

Appendix A. SuperScout Categories

This appendix lists the categories used by the SuperScout UFP Server and SuperScout Monitor and Reporter components, along with examples of the material in each category.

The SuperScout Monitor and Reporter component features the complete URL Category List of 39 categories.

The SuperScout UFP Server provides 30 subject categories though the UFP protocol, so 9 of the 39 categories on the Monitor and Reporter are mapped to other categories as shown below:

The mapping is as follows in the SuperScout UFP Server URL Category List:

- Advertisements maps to Shopping
- Education maps to Lifestyle & Culture
- Games maps to Hobbies & Recreation
- Hacking maps to Criminal Skills
- Kids' Sites maps to Arts & Entertainment
- Motor Vehicles maps to Shopping
- Religion maps to Lifestyle & Culture
- Streaming Media maps to Arts & Entertainment
- Weapons maps to Violence

(The UFP protocol supports 32 categories, but SuperScout uses two category slots for “{User-defined Prohibited}” and “{User-defined Allowed}”, leaving only 30 available slots for categories).

Category	Defined Criteria
Adult/Sexually Explicit	Sexually-oriented or erotic full or partial nudity Depictions or images of sexual acts, including animals or inanimate objects used in a sexual manner Erotic stories and textual descriptions of sexual acts Sexually expletive or sexually violent text or graphics Bondage, fetishes, genital piercing Adult products including sex toys, CD-ROMs, and videos Adult services including videoconferencing, escort services, and strip clubs Explicit cartoons and animation Note: SuperScout does not block on the basis of sexual preference, nor does it block sites regarding sexual health, breast cancer, or sexually transmitted diseases (except in graphic examples).
Advertisements*	Banner Ad Servers

Arts & Entertainment	<p>Television, movies, music and video programming guides Comics, jokes, movie, video or sound clips Discussion forums on television, movies, music and videos Online magazines and reviews on the entertainment industry Circuses, theatre, variety magazines, and radio Broadcasting firms and technologies (satellite, cable, etc.) Book reviews and promotions, publishing houses, comic books, and poetry Jokes, comedians, any site designed to be funny or satirical Online museums, galleries, artist sites (included sculpture, photography, etc.) Celebrity fan sites Horoscopes City Guides</p>
Chat	Web-based chat
Computing & Internet	<p>Reviews, information, buyer's guides of computers, computer parts and accessories, and software — Computer/software/Internet companies, industry news and magazines — Sites that design and/or maintain web pages including individual web designers</p>
Criminal Skills	<p>Advocating, instructing, giving advice on performing illegal acts such as phone, service theft, evading law enforcement, lock-picking, fraud, plagiarism/cheating, and burglary techniques</p>
Drugs, Alcohol & Tobacco	<p>Recipes, instructions or kits for manufacturing or growing illicit substances, including alcohol, for purposes other than industrial usage Glamorizing, encouraging, or instructing on the use of or masking the use of alcohol, tobacco, illegal drugs, or other substances that are illegal to minors Alcohol and tobacco manufacturers' commercial Web sites Information on "legal highs": glue sniffing, misuse of prescription drugs or abuse of other legal substances Distributing alcohol, illegal drugs, or tobacco free or for a charge Displaying, selling, or detailing use of drug paraphernalia Note: SurfControl does not block sites discussing medicinal drug use, industrial hemp use, or public debate on the issue of legalizing certain drugs. Nor does it block sites sponsored by a public or private agency that provides educational information on drug use.</p>
Education*	<p>.edu sites: pre-, elementary, secondary, and high schools; universities. Distance education and trade schools Online teacher resources (lesson plans, etc.) Topic-specific search engines (anthropology, medicine, etc.)</p>
Finance & Investment	<p>Stock quotes, stock tickers, and fund rates Online stock or equity trading Investing advice or contacts for trading securities Money management/investment services or firms General finances and companies that advise thereof Accountancy, actuaries, banks, mortgages, and general insurance companies</p>

Food & Drink	Recipes, cooking instruction and tips, food products, and wine advisors Restaurants, cafes, eateries, pubs, and bars Food/drink magazines, reviews
Gambling	Online gambling or lottery web sites that invite the use of real money Information or advice for placing wagers, participating in lotteries, or gambling real money, or running numbers Virtual casinos and offshore gambling ventures Virtual sports leagues and sports picks and betting pools
Games*	Game playing or downloading; game hosting or contest hosting Tips and advice on games or obtaining cheat codes (“cheatz”) Journals and magazines dedicated to game playing
Glamour & Intimate Apparel	Lingerie, negligee or swimwear modeling Model fan pages; fitness models/sports celebrities Fashion or glamour magazines online; clothing catalogs Beauty and cosmetics Modeling information and agencies
Government & Politics	Government services such as taxation, armed forces, customs bureaus, emergency services. Local government sites Political debate, canvassing, election information and results Local, national, and international political sites
Hacking*	Promotion, instruction, or advice on the questionable or illegal use of equipment and/or software for purpose of hacking passwords, creating viruses, gaining access to other computers and/or computerized communication systems. Anonymous surfing sites and/or sites that provide “work-arounds” for our filtering software. Cracked software
Hate Speech	Advocating or inciting degradation or attack of specified populations or institutions based on associations such as religion, race, nationality, gender, age, disability, or sexual orientation Promoting a political or social agenda that is supremacist in nature and exclusionary of others based on their race, religion, nationality, gender, age, disability, or sexual orientation Holocaust revisionist/denial sites Militancy Coercion or recruitment for membership in a gang* or cult** Note: SurfControl does not block news, historical, or press incidents that may include the above criteria (except in graphic examples).
Health & Medicine	General health such as fitness and well-being Alternative and complementary therapies Medical information about ailments, conditions, and drugs Medical reference Hospital or medical insurance Dentistry, optometry, and other medical-related sites General psychiatry and mental well-being sites Promoting self-healing of physical and mental abuses, ailments, and addictions Psychology, self-help books, and organizations
Hobbies & Recreation	Recreational pastimes such as collecting, gardening, kit airplanes

	Outdoor recreational activities such as hiking, camping, rock climbing Tips or trends focused on a specific art, craft, or technique Online publications on a specific pastime or recreational activity Online clubs, associations or forums dedicated to a hobby
Hosting Sites	Web sites that host business and individuals' web pages (i.e. GeoCities, earthlink.net, AOL)
Job Search & Career Development	Employment agencies, contractors, job listings, career information Career searches, career-networking groups
Kids' Sites*	Sites specifically aimed at children or published by children
Lifestyle & Culture	Homelife and family-related topics, including parenting tips, gay/lesbian/bisexual (non-pornographic sites), weddings, births, and funerals Foreign cultures, socio-cultural information
Motor Vehicles*	Car reviews, vehicle purchasing or sales tips, parts catalogs Auto trading, photos, discussion of vehicles including motorcycles, boats, cars, trucks and RVs Journals and magazines on vehicle modification, repair, and customization Online automotive enthusiast clubs
News	Newspapers online Headline news sites, newswire services, and personalized news services Weather sites
Personals and Dating	Singles listings, matchmaking and dating services Advice for dating or relationships; romance tips and suggestions
Photo Searches	Sites that provide resources for photo and image searches
Real Estate	Home, apartment, and land listings Rental or relocation services Tips on buying or selling a home Home loan and mortgage information Real estate agents Home improvement
Reference	Personal, professional, or educational reference Online dictionaries, maps, and language translation sites Census, almanacs, and library catalogues Topic-specific search engines
Religion*	Churches, synagogues, and other houses of worship Any faith or religious beliefs, including "alternative" religions such as wicca and witchcraft
Remote Proxies	Remote proxies or anonymous surfing
Search Engines	General search engines (Yahoo, AltaVista, Google)
Shopping	Internet malls and online auctions Department stores, retail stores, company catalogs online Online downloadable product warehouses; specialty items for sale Freebies or merchandise giveaways

Sports	Team or conference web sites National, international, college, professional scores and schedules Sports-related online magazines or newsletters
Streaming Media*	Streaming media files or events (any live or archived audio or video file)
Travel	Airlines and flight booking agencies Accommodation information Travel package listings City guides and tourist information Weather bureaus Car rentals
Usenet News	All newsgroups accessed through the HTTP protocol
Violence	Sites portraying, describing or advocating physical assault against humans, animals, or institutions Depictions of torture, mutilation, gore, or horrific death Sites advocating suicide or self-mutilation Instructions, recipes or kits for making bombs or other harmful or destructive devices Excessive use of profanity or obscene gesticulation Note: SurfControl does not block news, historical, or press incidents that may include the above criteria (except in graphic examples).
Weapons*	Sites that allow online purchasing or ordering information, including lists of prices and dealer locations Any page or site predominantly containing, or providing links to, content related to the sale of guns, weapons, ammunition or poisonous substances Sites displaying or detailing the use of guns, weapons, ammunition or poisonous substances.
Web-based Email	Sites that provide web-based email accounts

Appendix B. SuperScout Standard Reports

This release of SuperScout contains over 60 standard reports you can generate and publish. This appendix describes those reports by category:

- Quick
- Summary
- Comparison
- Detailed

Quick Reports

Name	Type	Description
Blocked Category Detail (This report is not operational with this product)	Table	Sites that have been blocked, the user attempting the connection and the number of hits the user has made to the blocked site. Sites are sorted by category.
Blocked Category Summary (This report is not operational with this product)	Table	Number of blocked attempts made to each category.
Category Analysis	Pie Chart	Based on the number of connections made to each category, displays percentages by category. Also includes a table showing the actual number of connections to each category.
Departmental Analysis	Pie Chart	Based on the number of hits made by each department, displays percentages by department. Also includes a table showing the actual number of connections made by each department.
Site Access	Table	Each site, its relevant IP address, total number of connections made to the site, and when it was first and last accessed. Sorted by total number of connections.
Top 10 Browse Times	Bar Chart	Based on total browse time.
Top 10 Categories	Bar Chart	Based on number of connections made
Top 10 Departments	Bar Chart	Based on number of connections made.
Top 10 Departments by Cost	Bar Chart	Based on total cost incurred while browsing.
Top 10 Protocols	Bar Chart	Based on number of connections made
Top 10 Sites	Bar Chart	Based on number of connections made

Top 10 SMTP Email Receivers, by Quantity	Table	By number of emails received.
Top 10 SMTP Email Receivers, by Size	Table	By bytes received.
Top 10 SMTP Email Senders, by Quantity	Table	By number of emails sent.
Top 10 SMTP Email Senders by Size,	Table	By bytes sent.
Top 10 Users	Bar Chart	Based on number of connections made
Top 10 Users by Cost	Bar Chart	Based on total cost incurred while browsing, calculated using Browse Time Sensitivity* and workstation cost per hour.
Top 10 Users showing Categories	Bar Chart	Based on number of connections made to each category. <i>Not available in Web Reporting.</i>
Top 10 Users showing Protocols	Bar Chart	Based on number of connections made on each protocol. <i>Not available in Web Reporting.</i>
Top 10 Workstations	Bar Chart	Based on number of connections made

* Browse time sensitivity by default is 3 minutes; if a connection is made within 3 minutes it is presumed the user is continuously browsing.

Summary Reports

Name	Type	Description
Daily Access	Bar Chart	Number of connections made each day.
Top Days	Bar Chart	Number of connections made for each day of the week.
Top N Browse Times	Table	Based on total browser time, based on Browse Time Sensitivity*.
Top N Categories	Table	Based on number of connections made.
Top N Departments	Table	Based on number of connections made.
Top N Departments by Cost	Table	Based on total cost incurred while browsing, calculated using Browse Time Sensitivity* and workstation cost per hour.
Top N Departments showing Categories	Table	Based on number of connections mad, sorted by category within department.
Top N Protocols	Table	Based on number of connections made.
Top N Sites	Table	Based on number of connections made.
Top N SMTP Email Receivers, by Quantity	Table	By number of emails received.
Top N SMTP Email Receivers, by Size	Table	By bytes received.
Top N SMTP Email Senders, by Quantity	Table	By number of emails sent.
Top N SMTP Email Senders, by Size	Table	By bytes sent.
Top N Users	Table	Based on number of connections made.
Top N Users by Cost	Table	Based on total cost incurred while browsing, calculated using Browse Time Sensitivity* and workstation cost per hour.
Top N Users showing Categories	Table	Based on number of connections made to each category.
Top N Users showing protocols	Table	Based on number of connections made on each protocol.
Top N Workstations	Table	Based on number of connections made.
Top Times	Bar Chart	Number of connections made for each hour of the day.

** Browse time sensitivity by default is 3 minutes; if a connection is made within 3 minutes it is presumed the user is continuously browsing.*

Comparison Reports

Name	Type	Description
Category Analysis	Pie Chart	Categories by percentage, based on the number of connections made to each category. Also includes a table showing the actual number of connections to each category.
Category Connection Analysis	Pie Chart	Categories by department, based on the number of connections made.
Category Data Analysis	Pie Chart	Amount of bytes sent and received to each category, based on the amount of data.
Category Time Analysis	Line Graph	Connections made over time, based on the number of connections to each category.
Departmental Analysis	Pie Chart	Number of hits by department. Also includes a table showing actual number of connections by department.
Departmental Connection Analysis	Pie Chart	Connections made to each category by department.
Departmental Data Analysis	Pie Chart	Bytes sent and received by each category.
Departmental Time Analysis	Line Graph	Connections over time by department.
Protocol Analysis	Pie Chart	Number of connections by protocol.
Protocol Data Analysis	Pie Chart	Bytes sent and received by protocol.
Protocol Time Analysis	Line Graph	Connections made over time by protocol.
Site Connection Analysis	Pie Chart	Top 10 sites accessed.
Site Data Analysis	Pie Chart	Bytes sent and received for top 10 sites.
User Connection Analyses	Pie Chart	Top 10 users by number of connections made.
User Data Analysis	Pie Chart	Bytes sent and received by each user.

Detailed Reports

The *Browse Time Activity Summary* report from previous versions of SuperScout has been renamed *Top N Users* and is located on the Summary Reports tab.

Name	Type	Description
Blocked Category Detail (This report is not operational with this product)	Table	Blocked sites, user attempting the connection, and number of hits user made to the blocked site. Sites are sorted by category.
Blocked Category Summary (This report is not operational with this product)	Table	Total number of blocked attempts made to each category.
Blocked User Activity (This report is not operational with this product)	Table	Sites that have been blocked, the site category and the time each site was blocked. Sorted by user.
Browse Time Activity Detail	Table	For each user, displays browsing per day. This report asks for a browse duration threshold, if 10 minutes is entered, then any time duration that exceeds 10 minutes will be highlighted. Total browse time is calculated using the browse time sensitivity, which by default is 3 minutes. Using this setting if a connection is made within 3 minutes it is presumed that the user is continuously browsing.
Newsgroup Analysis		Requests for newsgroup connections. <i>Not available in Web Reporting.</i>
Protocol Data Analysis		Bytes sent and received by protocol.
Security Analysis	Table	Connections made from external Clients to internal Servers, displayed as user sites visited, site activity, bytes sent, received, and date/time connection was made. Sorted by user. You are prompted for an IP range to exclude; you would normally exclude your internal IP range so that report displays only external Clients.
Site Access	Table	Each site, its relevant IP address, total number of connections made to the site, and when it was first and last accessed, sorted by total number of connections.
Site Activity	Table	Site activity, port, user name, bytes sent and received, and date/time of connection, sorted by site name. You can add a filter to list only certain types of activity.
Site Categorization Details	Table	Categorized sites and total number of hits

		made to each site, sorted by category.
SMTP Email Analysis	Table	Sender, recipient, subject and time/date for each email, sorted by sender. <i>Not available in Web Reporting.</i>
User Access	Table	Access details for all users or specified users.
User Activity	Table	First and last access times by user, either for all users or for specified users. <i>Not available in Web Reporting.</i>
User Activity Detail	Table	All activity by user, for all users or specified users.
User Cost Analysis	Table	Cost information for users, for all users or specified users, based on browse times.
User Data Analysis Detail	Table	Total bytes sent and received for all or specified users.

User Access	Table	User's last IP address, total number of connections made, first access, and last access, sorted by user.
User Activity	Table	First and last access made to each site and whether the connection was allowed or disallowed, sorted by user.
User Activity Detail	Table	Site visited, the site activity, port, user name, bytes sent and received, and date/time of connection, sorted by user. You can also add a filter to list only certain types of activity.
User Cost Analysis	Table	Total browse time by user, calculated using Browse Time Sensitivity and workstation cost per hour.

** Browse time sensitivity by default is 3 minutes; if a connection is made within 3 minutes it is presumed the user is continuously browsing.*