SurfControl®

Version 2.5

SurfControl Report Central

Administrator's Guide

NOTICES

jTDS JDBC Driver for Microsoft SQL Server and Sybase

jRegistryKey - A JNI wrapper of the Windows Registry functions

November 2006

Comments on this Guide?

You can view updated documentation and support information at
http://www.surfcontrol.com

Was this guide helpful? E-mail us at documentation@surfcontrol.com to suggest changes or make a correction.

TECHNICAL SUPPORT

For the latest support information on SurfControl products, visit
http://www.surfcontrol.com/support

You can find the following information on the Technical Support Web pages:

- Read the Top Issues – This page has a quick list that covers the most common support issues encountered with SurfControl products.
- Search our Knowledge Base – Our constantly updated Knowledge Base contains articles, FAQs and glossary items to answer your questions about all SurfControl products.
  http://kb.surfcontrol.com
- If your question or problem cannot be answered by the Top Issues or is not in the Knowledge Base, complete an Online Support Request Form.
- Telephone Support numbers – If you would like to speak with a Technical Support Representative, our excellent SurfControl Technical Support is just a phone call away.

SURFCONTROL SALES

For product and pricing information, or to place an order, contact SurfControl. To find your nearest SurfControl office, please visit our Website.

http://www.surfcontrol.com

SurfControl Sales

CONTENTS

1

Introduction

WELCOME TO SURFCONTROL REPORT CENTRAL

This chapter explains how SurfControl Report Central works, and introduces you to the various reporting and configuration options.

Before you can use Report Central effectively, you need to:

- Create accounts for users.
- Set permission levels for users.
- Specify the types of reports that users can access.

See Chapter 2 for details of these options.

GETTING STARTED

Before opening SurfControl Report Central (SRC), you need to configure your browser to allow pop-ups and cookies from the SRC server. If you will be connecting using HTTPS, the default security certificate that is generated by SRC enables secure, encrypted communication. However, you may want to consider using a self-signed or Certificate Authority (CA) signed security certificate.

POP-UP BLOCKERS

You need to configure your pop-up blocker to allow pop-ups from the Report Central server. If you are using Internet Explorer 6.0:

1. Select **Tools** > **Pop-up Blocker** > **Pop-up Blocker Settings**.
2. Enter the URL of the SRC server
3. Click **Add**.

COOKIES

You need to set your browser to allow cookies from the Report Central server. If you are using Internet Explorer 6.0:

1. Select **Tools** > **Internet Options** > **Privacy** tab > **Sites**.
2. Enter the URL of the SRC server.
3. Click **Allow**.

CERTIFICATE MANAGEMENT

When a client attempts to access SurfControl Report Central (SRC) using HTTPS, the server sends a default digital security certificate to the browser. This enables secure, encrypted communication, but the browser displays a Security Alert.

Figure 1-1 Security Alert

- If you click **Yes**, SRC uses the default certificate for the duration of the SRC session. The Security Alert is displayed at the start of each SRC session.
- If you click **View Certificate**, you can view and install the default certificate. The Security Alert will not be displayed until the certificate expires after 90 days.

For both instances above, after 90 days the Security Alert is displayed at the start of each session and the second item is

"The security certificate has expired or is not yet valid."

If you use the default certificate, communications will continue to be secure. However, to avoid triggering the Security Alert, you can do one of the following:

- Create and install a self-signed certificate, which you can renew regularly, usually yearly.
- Buy or obtain a valid, signed digital certificate from a Certificate Authority (CA).

  If you have your own CA server, you can use it to validate server and Virtual Private Network (VPN) certificates within your own network.

SRC certificates are located in the .sckeystore file.

Creating and Installing a Self-Signed Certificate

Prior to creating a self-signed certificate, ensure that the network is protected and the client and server are in the same domain.

Creating a Self-Signed Certificate. To create a self-signed certificate:

1 Stop SurfControl Report Central service.

2 Go to a command prompt, and then enter:

```
cd <SRC installation path>\Report Central\Tomcat
```

3 To generate the self signed certificate that will be valid for a period of 365 days, enter:

```
..\jre\bin\keytool -selfcert -alias tomcat -storepass changeit -validity 365 -
keystore .sckeystore
```

4 Re-start SurfControl Report Central.

Installing a Self-Signed Certificate. To install a self-signed certificate:

1 Access SRC using HTTPS.

2 In the Security Alert, click **View Certificate**.

3 Click **Install Certificate**.

4 Follow the instructions in the Install Certificate Wizard.

5 In the Security Alert, click **Yes**.

You must repeat this procedure for each client.

Obtaining and Importing a Signed Certificate from a CA

To use a signed certificate from a CA, you need to:

1 Generate a Certificate Signing Request (CSR).

2 Import the signed certificate.

Generating a Certificate Signing Request (CSR). To generate a CSR:

1 Go to the .sckeystore directory:

```
cd <SRC installation path>\Report Central\tomcat
```

2 Enter the command below to create a file called SRC.txt:

```
..\jre\bin\keytool.exe -certreq -keystore .sckeystore -file SRC.txt -alias tomcat
```

3 You will be prompted for a password (‘changeit’ by default).

4 Send the newly created CSR file(SRC.txt) to a CA.

Importing a Signed Certificate. To import a signed certificate:

1 The response from the CA will contain a file with a .p7b extension. Before importing the newly signed certificate, stop SurfControl Report Central service.
2 Go to a command prompt. Assuming the p7b file is called <filename>.p7b, enter:

```
..\jre\bin\keytool.exe -import -trustcacerts -keystore .sckeystore -alias tomcat
-file <filename>.p7b
```

3 You will be prompted for a password ("changeit" by default).
4 You are prompted with a warning similar to "This certificate is not trusted. Install anyway?". Enter `Yes`.
5 Re-start the SurfControl Report Central service.

Additional Security - Passwords

The passwords for the keystore and the private key are defaults and are not secure. SurfControl recommends changing these passwords. See **http://mindprod.com/jgloss/keytoolexe.html#PASSWORDS** for details of changing the passwords. If the keystore password is changed, you must edit the Tomcat server.xml file to tell Tomcat the new password.

OPENING SRC

You can use two methods of opening Report Central for either E-mail Filter reports or Web Filter reports through the **Start** menu:

- To connect using HTTP, select

  All Programs > SurfControl Report Central > Web Filter Reports

  All Programs > SurfControl Report Central > E-mail Filter Reports
- To connect using a secure connection with HTTPS, select

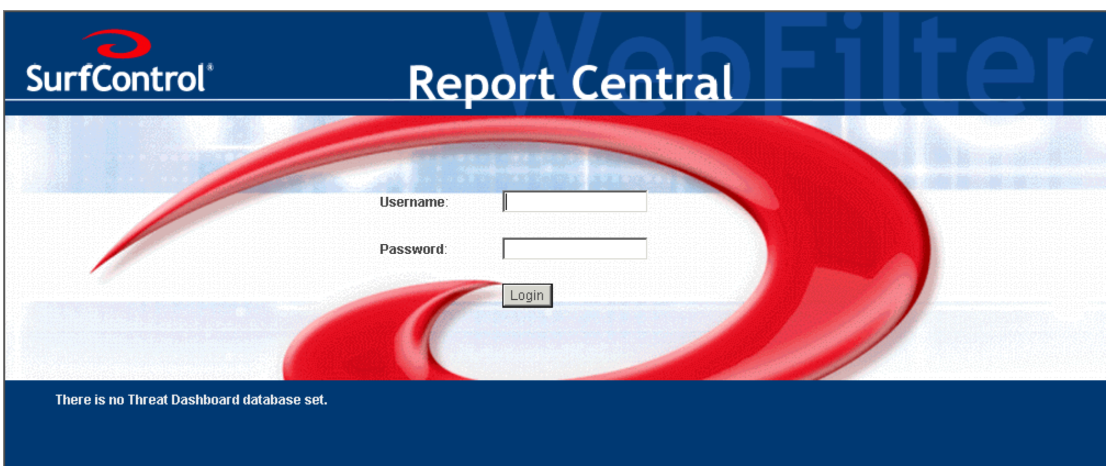
  All Programs > SurfControl Report Central > Web Filter Reports - Secure Connection

  All Programs > SurfControl Report Central > E-mail Filter Reports - Secure Connection

  For details of the default security certificate and self-signed or CA signed certificates, please see Certificate Management on page 3. See SurfControl Knowledge Base article 1788 for more information.

For both connections, the Logon screen is displayed.

Figure 1-2 First time SRC Logon screen



To configure Report Central to display a Threat Dashboard at the bottom of this Logon screen, see Databases - E-mail Filter on page 23.

The Threat Dashboard is described in the next section, The Threat Dashboard on page 8.

LOGGING ON TO REPORT CENTRAL

Note: SurfControl advise you to add the URL of the SRC server as a trusted site. If you are using Internet Explorer:
1. Select **Internet Explorer** > **Tools** > **Internet Options...** > **Security**
2. Select **Trusted Sites**, and then click **Sites**.
3. Enter the URL of the SRC server, and then click **Add**.

For your first log on, you need the Username and Password of the user that you set up during installation. This user has Reports Administrator privileges.

If needed, you can then set up other users. See Configuring User Accounts on page 15.

THE THREAT DASHBOARD

The Threat Dashboard displays an overview of the Internet traffic (for Web Filter) or e-mail traffic (E-mail Filter), as monitored in your current database. The name of the database connection is shown at the top of the dashboard.

Figure 1-3 Logon screen showing Threat Dashboard - example (Web Filter)

FORMATTING THE THREAT DASHBOARD

There are two drop-down list boxes at the top of the dashboard that enable you to change the data that is shown and how it is displayed:

- **Date** – Select to show data from either the previous 7 (default) or 28 days.
- **Format** – Select a format for the dashboard display:
  - **.swf** (Macromedia Flash). This is the default view. You might need to install the free Flash viewer to be able to view the dashboard in this format.
  - **.png** (Portable Network Graphic).
  - **.jpg** (Joint Photographic Experts Group).

With the png and jpg formats, you can save, e-mail or print the image from a right-click menu. This enables you to include the graphs in reports or send them to an e-mail distribution list if needed.

THREAT DASHBOARD – SRC FOR WEB FILTER

The SRC for Web Filter dashboard shows the following sets of graphs:

- **Total Traffic** – shows the number of times users have accessed Internet sites (Web site hits) and the bandwidth use.
- **Traffic Stats** – shows the number of Web site requests that have been allowed, blocked, overridden and blocked by AVA (Anti-Virus Agent).

  Overridden and Blocked by AVA requests are only displayed for ISA Server. Also, Blocked by AVA requests are only displayed for users who have a valid AVA license.
- **Top 10** – shows the top ten Web Filter categories or protocols by either hits or bandwidth.

THREAT DASHBOARD – SRC FOR E-MAIL FILTER

The SRC for E-mail Filter dashboard shows the following sets of graphs:

- **Connection Trend** – shows the trend for the types of connection received at the gateway (such as Accepted, DHA, SPF, DOS, and so on).
- **Message Trend** – shows the combined inbound and outbound trend for the types of e-mail, as categorized by E-mail Filter (such as, Legitimate, Compliance, Spam, Virus, and so on).
- **Policy Type** – shows the combined inbound and outbound total of the types of e-mail processed by E-mail Filter (such as, Legitimate, Compliance, Spam, Virus, and so on).

You can use the drop-down lists to specify that the message and policy graphs are shown by either volume or size.

The **Domains:** drop-down list contains only protected domains.

The **Scale:** drop-down enables you to select Hits or Bandwith.

REPORT CENTRAL FUNCTIONS

Report Central has three functions, which are displayed in the bottom-left corner of the window:

- Configuration
- Drill-Down Manager
- Report Manager.

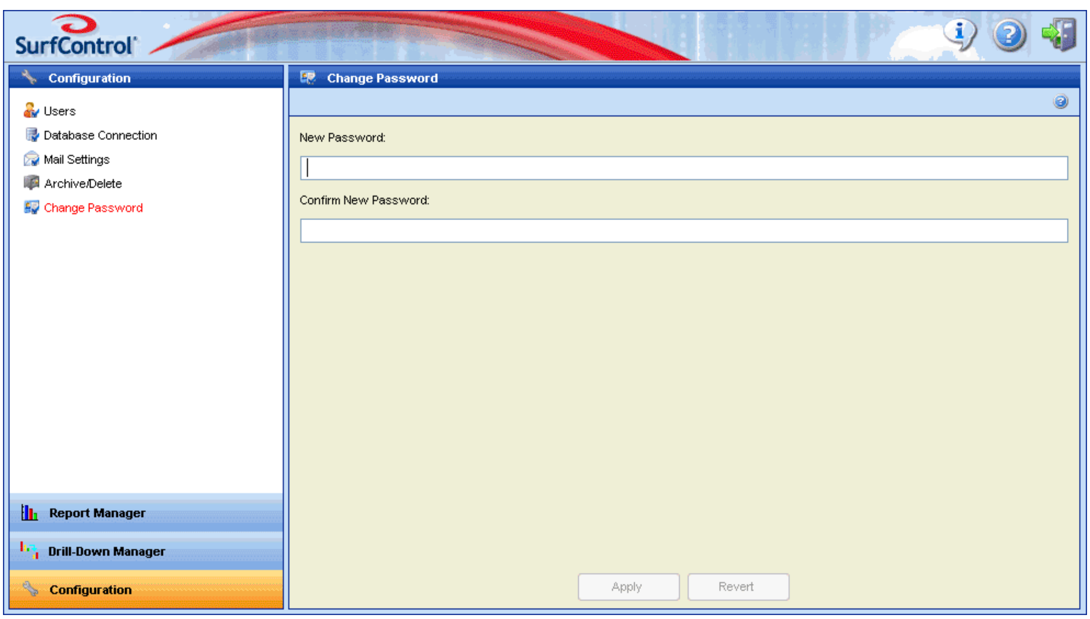
The number of functions displayed depends on the privileges of the user.

In addition, Report Central is supplied with context-sensitive Help, which includes a full-text search facility and an index.

CONFIGURATION

Use the Configuration function to set up users and database connections. See Chapter 2.

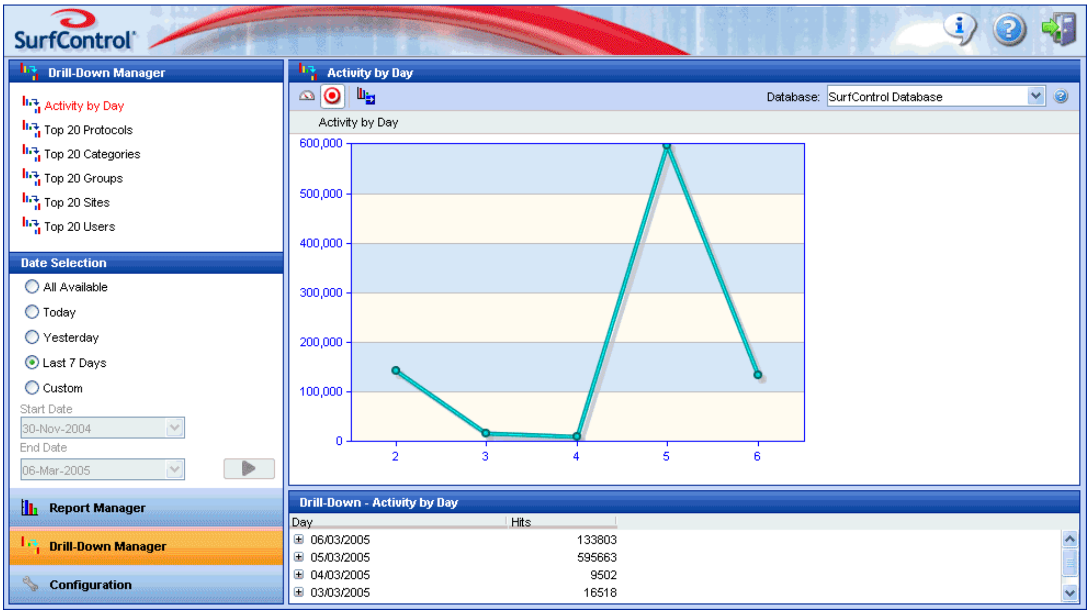
Figure 1-4 Configuration function



DRILL-DOWN MANAGER

Use the Drill-Down Manager to examine data for a particular day or range of days. See Chapter 3.

Figure 1-5 Drill-Down Manager



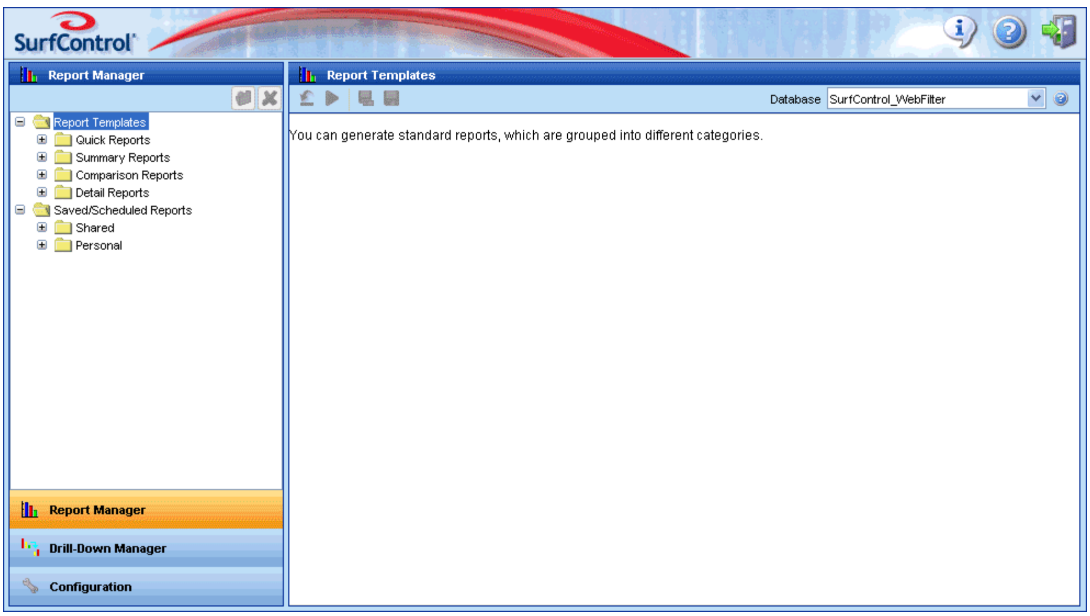
REPORT MANAGER

Use Report Manager templates to create and save reports for the data that you need. You can also schedule when the reports are to run.

For details of Report Manager for:

- Web Filter reports, see Chapter 4.
- E-mail Filter reports, see Chapter 5.

Figure 1-6 Report Manager - example Web Filter display



2

Configuration

INTRODUCTION

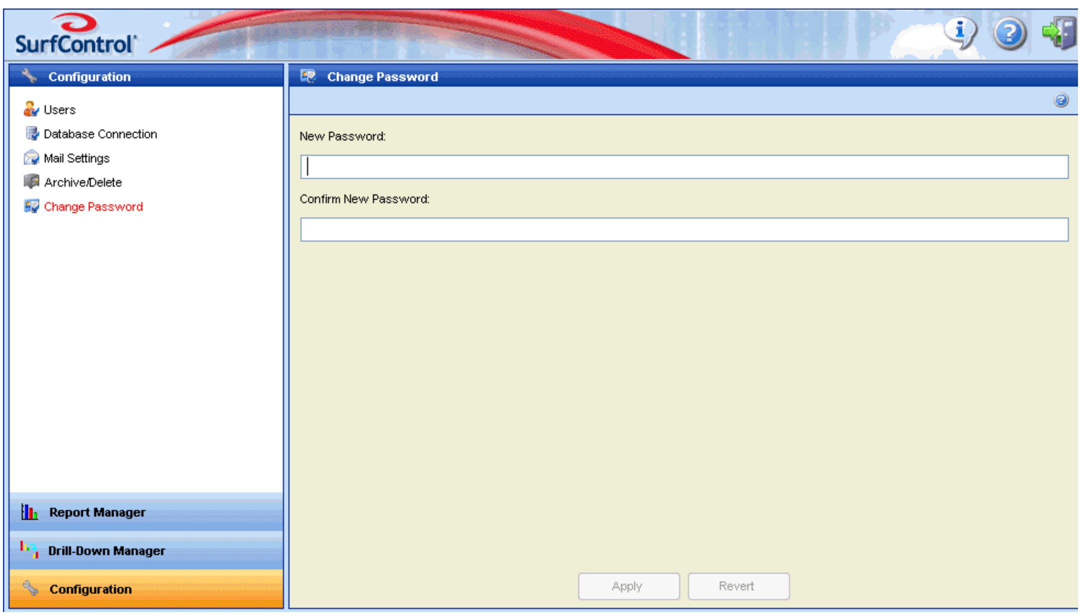
This chapter explains how to:

- Configure user accounts.
- Configure connections to databases from which to run your reports.
- Configure connections to a mail server to enable you to send reports by e-mail.
- Perform housekeeping tasks, such as deleting and archiving old reports.

CONFIGURATION OPTIONS

To configure Report Central, select **Configuration**. See Figure 2-1.

Figure 2-1 Configuration menu



The options available depend on the user permissions and the type of user. The possible options are:

- **Users** – To add, edit and delete users. See Configuring User Accounts on page 15.
- **Database Connection** – To create, edit and delete connections to databases. See Databases - Web Filter on page 19 or Databases - E-mail Filter on page 23.
- **Mail Settings** – To set up a connection to your mail server so that you can send reports by e-mail. See Mail Settings on page 30.
- **Archive/Delete** – To archive or delete your saved reports. See Archiving or Deleting Reports on page 30.
- **Change Password** – To change your own password. See Changing Passwords on page 32.

CONFIGURING USER ACCOUNTS

Your first task is to configure user accounts, you need to:

1 Set log on details.
2 Set user permissions.
3 Set report permissions.

To access the user configuration options, select

Users > New

The **User Configuration** dialog box is displayed.

SETTING LOG ON DETAILS

To configure log on details, see Procedure 2-1.

Procedure 2-1 Setting log on details

Step	Action
1	In the **User Configuration** dialog box, select the **General** tab.
2	Enter the following information: • User Name • Password • Confirm Password

SETTING USER PERMISSIONS

There are three levels of access, which have specific permitted actions, see Table 2-1.

Table 2-1 User permissions

Permission Setting	Permitted Actions
Reports Administrator	Can create and edit users. This user also has all Reports Manager privileges.
Reports Manager	Has one or more of the following privileges: • Able to create/modify databases. • Able to save reports in the Shared folders. • Able to save reports in a Personal folder.
Restricted User	Can run reports that have been set up by a Reports Administrator or Reports Manager, but cannot change the content of any report.

To set user permissions, follow the steps in Procedure 2-2.

Procedure 2-2 Setting user permissions

Step	Action
1	In the **User Configuration** dialog box, select the **General** tab.
2	Select the check box for the level of permission.

SPECIFYING REPORT PERMISSIONS

There are three types of report permission:

- Drill-Down
- Report Template
- Saved/Scheduled.

Drill-Down Reports

Drill-down reports enable you to investigate the data that a report is based upon. See Chapter 3 for more details.

Report Templates

There are pre-configured, standard templates for reporting on SurfControl products that enable you to generate reports immediately:

The pre-configured types of report supplied with Report Central are:

- Web Filter report templates:
  - Quick Reports
  - Summary Reports
  - Comparison Reports
  - Detail Reports
- E-mail Filter report templates:
  - Trend Reports
  - Management Reports – Connection Based
  - Management Reports – Traffic Based
  - Summary Reports – Inbound Traffic
  - Summary Reports – Outbound Traffic
  - Comparison Reports
  - Forensic Reports.

For security, you can restrict a user's access to one or more report categories, or specific reports within categories. This ensures that only authorized users have access to specific reports.

For a detailed description of each category and report, see:

- Web Filter reports, see Chapter 4.
- E-mail Filter reports, see Chapter 5.

Saved and Scheduled Reports

Authorized users can save reports and schedule reports to run. Reports can be saved in two types of folder:

- Shared – These reports can be run by any user that has the relevant permissions.
- Personal – These reports can only be run and viewed by the user who saved them.

For more details, see:

- Web Filter reports, see Saving Reports on page 71.
- E-mail Filter reports, see Saving Reports on page 107.

Restrict User to Selected Saved or Scheduled Reports Only

To restrict a user to be able to run a specific saved report only, select the check box for the report in the Saved/Scheduled folder.

Note: To enable a user to run a new Saved/Scheduled report, you have to edit the user's details. See Changing User Details on page 18.

To specify report permissions for a user, follow Procedure 2-3.

Procedure 2-3 Specifying report permissions

Step	Action
1	In the **User Configuration** dialog box, select the **Reports** tab.
2	Select the reports that the user has access to by selecting the check boxes: • Drill-Down Reports • All Reports • Report Template – Select either: - one or more categories - one or more reports within a category. • Saved/Scheduled Reports – Enables the user to select and view reports in the Shared and Personal folders. • Restrict User to Selected Saved/Scheduled Reports – Restricts the user access to only the selected saved reports.
3	Click **Create**.

CHANGING USER DETAILS

Users with Reports Administrator status can edit user details or delete user accounts. Procedure 2-4 describes how to edit user details.

Procedure 2-4 Editing user details

Step	Action
1	From the **Configuration** options, select **Users**.
2	Select the user in the **Existing Users** pane.
3	Click **Edit**. The **User Configuration** dialog box shows the user's existing details.
4	You can change all existing **General** and **Report** settings except for the **User Name**.
5	Click **OK** to confirm your changes**.**

Procedure 2-5 describes how to delete a user.

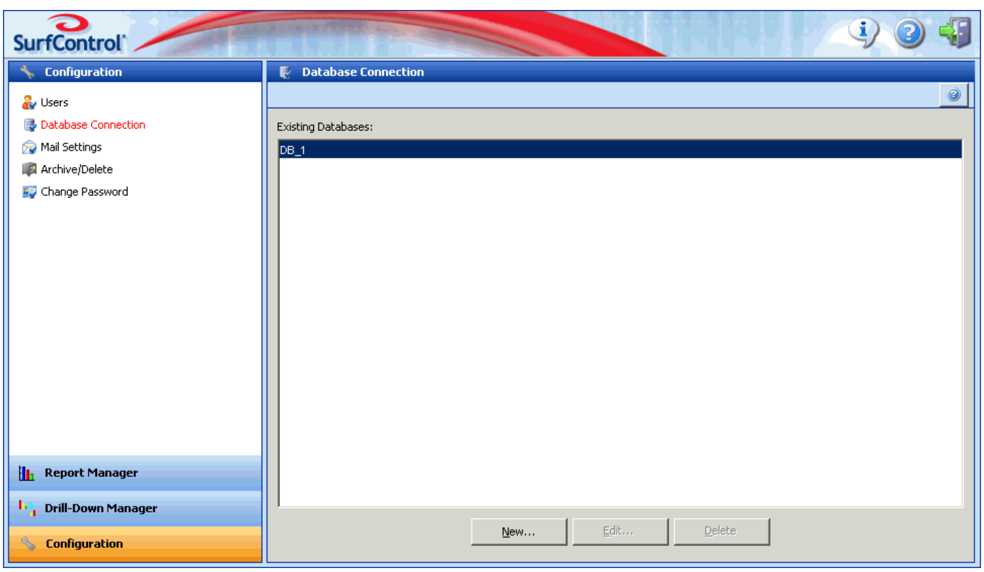
Procedure 2-5 Deleting a user

Step	Action
1	From the **Configuration** option, select **Users**.
2	Select the user in the **Existing Users** pane.
3	Click **Delete**. A Confirm Delete warning is displayed.
4	Click **Yes** to confirm the deletion of the user or **No** to cancel.

DATABASES - WEB FILTER

The first screen shows existing database connections.

Figure 2-2 Database Connection screen - E-mail Filter reports



From this screen, you can:

- Add a new connection
- Edit the settings for an existing connection
- Delete a connection
- Set up database summarization tasks
- Set up performance improvement task.

ADDING A NEW DATABASE CONNECTION

To report on a new database, you must first add the database connection details to the list. You can only add a database connection if you are either:

- A Reports Administrator
- A Reports Manager with the 'Able to change/modify databases' privilege.

Adding a new database connection is a two part procedure (Procedure 2-8). You must:

1. Add a connection to the database.
2. Schedule update tasks (see Table 2-2 on page 21).

Procedure 2-6 Adding a new database connection

Step	Action
1	Select **Database Connection.**
2	Click **New...**
3	On the **Connectivity** tab enter the following information: • A **Display Name** for the database. This will be added to the connections list in the configuration screen. • The name or IP address of the **Server**.
4	Select the **Authentication** method. **Note:** SurfControl recommends that you use Windows authentication. If you choose SQL authentication, enter the user name and password of an account with administrator access to the database. **Note:** A local or remote account must be part of the Local Administrator group on the local computer.
5	From the drop-down list box, select the database to connect to.
6	If you need to create drill-down reports or run the cached reports task, click the **Update Tasks** tab, select **Enable Scheduling**, and then configure the update and cache settings. It is important that this update is run for the drill-down reports to show accurate information.
7	Click **Create**.

Update Tasks

You can use the Update Tasks tab to set the scheduling, update and cache settings for the database connection.

Table 2-2 Update Task options

Option	Description
Enable Scheduling	To schedule the updates that are needed for drill-down reporting. If you select this check box, all other options become available.
Scheduler Time Settings	Default start time = 01:01 (24 hr clock) At this time, the Scheduler starts the database update and the pre-processing of reports for caching. SurfControl recommend that the database update is run when network traffic is quiet. It is important that this update is run for the drill-down reports to show accurate information.
Update Information for Drill-Down reports	Selecting this option updates the drill-down reporting information between the Scheduled Time updates. If you clear this option, the other Update Summary Settings options become unavailable.
Time between updates in minutes	Default = 15 minutes This option determines how often the data for drill-down reports is updated between Scheduled Time updates.
Use this database for threat dashboard reports	Default = cleared Selecting this option uses the information from this database for the reports viewed from the logon screen.
Update Information for Drill-Down Reports now	Select this option to perform a complete update for the drill-down reports when you click **Create**. The update will be run according to the Scheduler Time Settings.
Cache data for quick and summary reports	Default = All options selected. For details of the options, see Caching Options.

Database Update Log Files. Database update log files are stored in the WebFilter50/scheduler.log file. Logs include details of:

- The start and end of each scheduled update task.
- Any failures of the task.
- Retry attempts – If the task fails, it has up to three more attempts before it fails completely.

Caching Options

Report Central pre-processes Quick and Summary Reports and caches the results in the database. Caching enables standard reports to be generated faster, and is available for various time periods:

- Yesterday
- Last 7 Days
- Last Full Month

The cached reports are run using the default criteria for each report. For more details of criteria, see Specifying Report Criteria on page 46.

The following options for the cached version of the reports are configurable:

- Cost criteria
- Top N values.

If a cached report is run after any other option or criteria (Users, Sites etc.) has been changed, the report is generated without using the cached data. For more details of criteria, see Specifying Report Criteria on page 46.

Changing the Account for the SRC Service

If you have changed the user name or password, you need to ensure that the user's access rights for either the SRC server or the SQL server are correct. See the SurfControl Report Central Installation Guide for details of SRC service account/SQL database combinations.

To change the account for the SRC service, follow Procedure 2-10.

Procedure 2-7 Changing the account for the SRC service

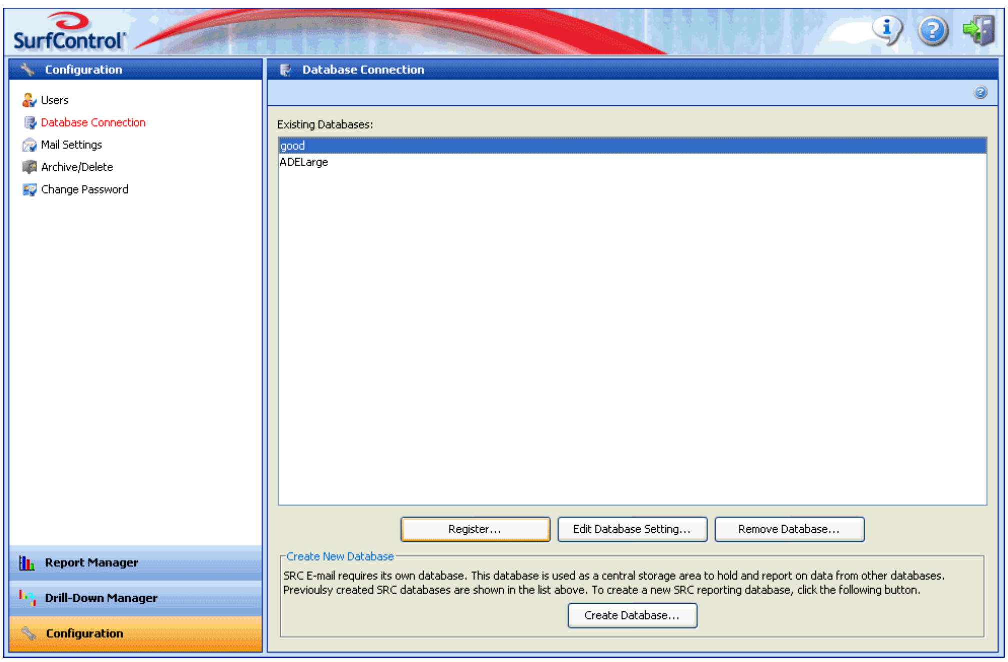
Step	Action
1	Select **Start > All Programs > Administrative Tools > Services** The Services window is displayed.
2	From the list in the right-hand panel, right-click **SurfControl Reports Central Service**, and then select **Properties**. The Properties dialog box is displayed.
3	Select the **Log On** tab, and then enter or browse to a user name, and enter a password.
4	Restart **SurfControl Reports Central Service**. You can now enter database connection details from Reports Central.

DATABASES - E-MAIL FILTER

Note: When you log in to SRC for E-mail Filter for the first time, the Post Install Configuration screens are displayed for you to create a new database connection or register an existing database connection to create a link between your current E-mail Filter database server and your SRC database server. For details, see the *SurfControl Report Central Starter Guide, chapter 2, section 'Post-Installation Procedures', subsection 'SRC for E-mail Filter Reports – Linked Servers'*.

The first screen shows existing database connections.

Figure 2-3 Database Connection screen - E-mail Filter reports



From this screen, you can:

- Create a database
- Register an existing database connection
- Edit the settings for an existing connection
- Remove a connection
- Schedule database update tasks
- Schedule database maintenance tasks.

ADDING DATABASE CONNECTIONS

To report on a new database, you must first add the database connection details to the list. You can only add a database connection if you are either:

- A Reports Administrator
- A Reports Manager with the 'Able to change/modify databases' privilege.

Adding a new database connection is a two part procedure. You must:

1. Add a connection to the database.

   You can use one of the following methods to add a new database:

   – Create a new database – SRC for E-mail Filter needs its own needs its own database, which is used as a central storage area to hold and report on data from other databases. See Procedure 2-8.

   – Register an existing database – To register a connection an existing database for SRC. See Procedure 2-9.

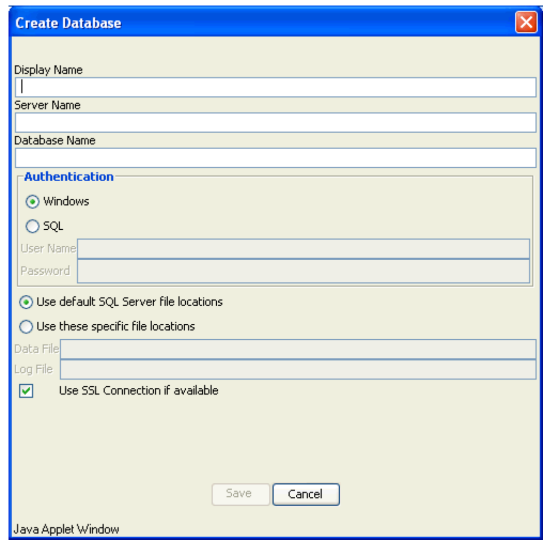
2. Schedule update tasks. See Update Tasks tab on page 27.

If needed, you can also schedule a database archive and/or purge. Regular archiving/purging of a database is useful for reducing the amount of information stored in the database. See Maintenance tab on page 28.

Creating a Database Connection for E-mail Filter Reports

To create a database connection for E-mail Filter reports, follow Procedure 2-8.

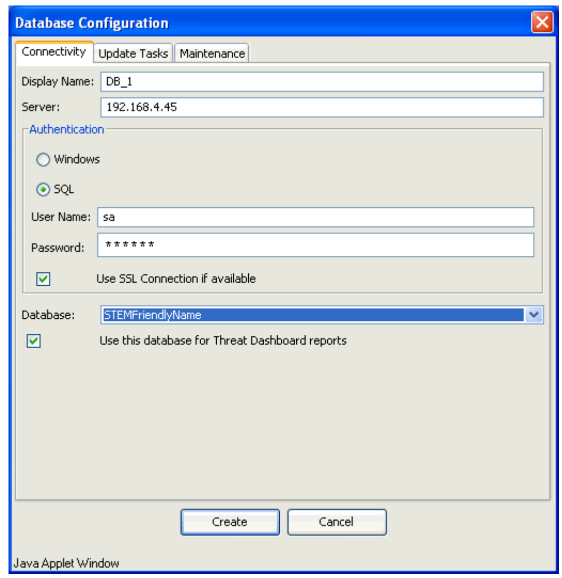
Procedure 2-8 Creating a new database connection for E-mail Filter reports

Step	Action	Action
1	Click **Create Database...**	
2	In the Create Database dialog box, enter the following information: • A **Display Name** for the database – This is shown in the main Database Connection screen. • The **Server Name** – The name or IP address of the server. • **Database Name** – The name of the database that you are connecting to.	
3	Select the **Authentication** method. **Note:** SurfControl recommends that you use Windows authentication. If you choose SQL authentication, enter the user name and password of an account with administrator access to the database. **Note:** A local or remote account must be part of the Local Administrator group on the local computer.	
4	Select to use default SQL Server file locations, or enter your preferred file locations for the Data file and Log file.	
5	If you want your database to use a secure connection, select **Use SSL Connection if available**.	
6	Click **Save**.	
7	If you need to schedule database updates or archiving and/or purging: 1 On the Database Connection main screen, click **Edit Database Setting...** 2 Use the settings in the: - **Update Tasks** tab, and/or - **Maintenance** tab. See Update Tasks tab on page 27, and Maintenance tab on page 28.	

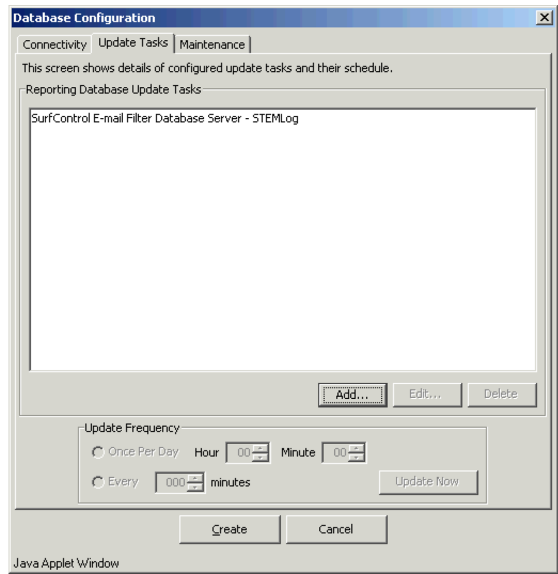
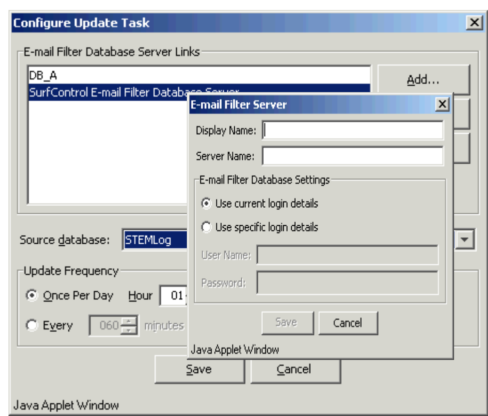
Registering a Database

To register a database connection, follow Procedure 2-9.

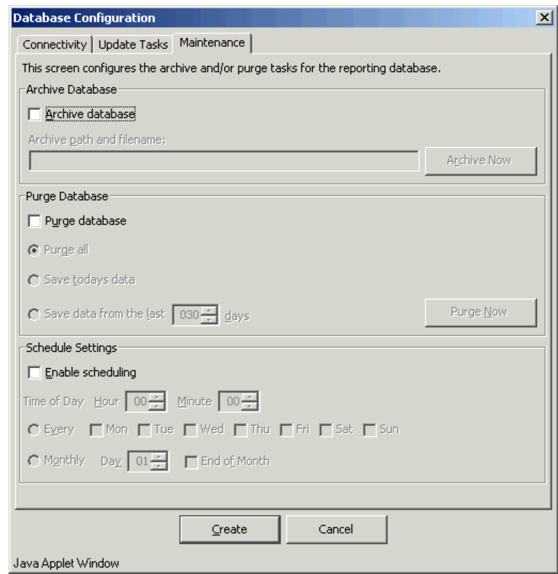
Procedure 2-9 Registering a database connection

Step	Action	Action
1	Click **Register...**	
Connectivity tab		
2	Enter the following information: • A **Display Name** for the database. This will be added to the connections list in the configuration screen. • The name or IP address of the **Server**.	
3	Select the **Authentication** method. **Note:** SurfControl recommends that you use Windows authentication. If you select SQL authentication, enter the user name and password of an account with administrator access to the database. **Note:** A local or remote account must be part of the Local Administrator group on the local computer.	
4	If you want your database to use a secure connection, select **Use SSL Connection if available**.	
5	From the drop-down list box, select the database to connect to.	
6	To use the information from this database for the reports viewed from the login screen, select **Use this database for Threat Dashboard reports**. Default = cleared **Note:** Only one database can be used at any one time for the Threat Dashboard display.	
7	If you need to schedule database updates or archiving and/or purging, see Update Tasks tab on page 27, and Maintenance tab on page 28. Otherwise, click **Create**.	
(Sheet 1 of 3)		

Procedure 2-9 Registering a database connection (Continued)

Step	Action	Action
Update Tasks tab		
8	Use this tab to set the scheduling of database updates for a database connection. Click **Add...** to configure an update task for your database. **Note:** SRC for E-mail Filter uses SQL linked servers to copy data from the source E-mail Filter database to the SRC database. This requires that a linked server definition be created. The following screen will be used to select an existing linked server or to add a new linked server definition.	
9	In the Configure Update Task dialog box, click **Add...** to set: • A display name. • The server's name or IP address. • Login details. • The source database on the server. • The frequency of the update. Default start time = 01:01 (24 hr clock) At this time, the Scheduler starts the database update. **Note:** SurfControl recommend that the database update is run when network traffic is light. However, for E-mail Filter reports it can be run regularly during the day. It is important that this update is run for the drill-down reports to show accurate information.	
10	Click **Save**. The database and server name are displayed in the **Reporting Database Update Tasks** list in the Update Tasks page.	
(Sheet 2 of 3)		

Procedure 2-9 Registering a database connection (Continued)

Step	Action	Action
Maintenance tab		
11	Use this tab to schedule regular archiving and/or purging of the database. **Archive Database** – Enter the path to the archive folder. **Purge Database** – Select the data to purge or save. **Schedule Settings** – To schedule the updates that are needed for drill-down reporting. **Enable Scheduling** – If you select this check box, all other options become available. **Scheduler Time Settings** Default start time = 01:01 (24 hr clock) At this time, the Scheduler starts the database maintenance tasks. **Note:** SurfControl recommend that the database maintenance is run when network traffic is light.	
(Sheet 3 of 3)		

Database Update Log Files. Database update log files are stored in the EmailFilter50/scheduler.log file. Logs include details of:

- The start and end of each scheduled update task.
- Any failures of the task.
- Retry attempts – If the task fails, it has up to three more attempts before it fails completely.

Changing the Account for the SRC Service

If you have changed the user name or password, you need to ensure that the user's access rights for either the SRC server or the SQL server are correct. See the SurfControl Report Central Installation Guide for details of SRC service account/SQL database combinations.

To change the account for the SRC service, follow Procedure 2-10.

Procedure 2-10 Changing the account for the SRC service

Step	Action
1	Select **Start > All Programs > Administrative Tools > Services** The Services window is displayed.
2	From the list in the right-hand panel, right-click **SurfControl Reports Central Service**, and then select **Properties**. The Properties dialog box is displayed.
3	Select the **Log On** tab, and then enter or browse to a user name, and enter a password.
4	Restart **SurfControl Reports Central Service**. You can now enter database connection details from Reports Central.

RECOMMENDATIONS FOR DATABASES AND TASKS

The following recommendations are for:

- The amount of free space needed on the SRC database to copy data from an E-mail Filter database during a database update task.

  Recommendation: There should be 1.5 times as much free space as the size of the E-mail Filter database.

  Example: E-mail Filter database = 60 GB, SRC database free space = 90 GB

- The time to allow between automated database update tasks for the SRC database.

  Recommendation: Small databases (approx. 50000 e-mails) = 5 minutes, Large databases = 10 minutes.

  If the time between tasks is set too low, the next task will attempt to start, but fail. An error " Failed scheduled database update..." is logged in the scheduler.log file and shows the linked server, source catalog and the database display name.

  This error will not affect the performance of your system, but it indicates that you should increase the interval between the database update tasks. Therefore, it is also recommended that you check the log file regularly for this error.

MAIL SETTINGS

For a user with the necessary permissions to be able to send reports by e-mail, a mail server must be specified. See Procedure 2-11.

Procedure 2-11 Specifying a mail server

Step	Action
1	Select **Mail Settings**.
2	In the Hostname field, enter the server name of the mail server to be used to distribute reports, for example myserver.mycompany.com
3	In the Port field, enter the number of the port to be used to send outbound e-mail. This is usually port 25.
4	In the Senders E-mail Address field, enter the e-mail address from which to send reports, for example, reporting@reportcentral.com.
5	Click **Apply**.

ARCHIVING OR DELETING REPORTS

You can specify how Report Central deals with reports that are no longer current. When you have enabled archiving or deletion (Procedure 2-12), use the Archive/Delete options to specify:

- which reports are deleted or archived
- when deletion or archiving takes place.

ENABLING REPORT ARCHIVING AND DELETION

To delete or archive reports you must first enable the archive and delete facility.

Procedure 2-12 Enabling report archiving and deletion

Step	Action
1	Select **Archive/Delete**.
2	Select **Enable Deletion and Archiving**. By default, the **Delete Reports** option is selected and the deletion settings are available. To enable the archive settings, select the **Archive Reports** option.

You can now set the archive/delete options by following Procedure 2-13 or Procedure 2-14.

DELETING REPORTS

The **Delete Reports** options enable you to select the age of the reports to delete and when they should be deleted. See Procedure 2-13.

Procedure 2-13 Deleting reports

Step	Action
Specifying which reports are to be deleted	
1	From the **Configuration** options, select **Archive/Delete**.
2	Select the **Enable Deletion and Archiving** check box. By default, the **Delete Reports** option is selected.
3	Select the **Delete Options** tab.
4	Select one of the options: • All (the default setting) • Before today • Older than last 7 days • Older than last full month
Specifying the date and time to delete the reports	
5	Select the **Date /Time** tab.
6	In the **Time of Day** area, specify a time of day (24hr clock) to delete your reports.
7	Select the day(s) on which to delete the reports: • To delete the selected reports on a certain day, days or every day, select **Every**, and then select the relevant check box(es). • To delete the selected reports on a specific day in the month, select **Monthly** and change the **Day** field. • To delete the reports on the last day of each month, select **End of Month**.
8	Click **Apply**.

ARCHIVING REPORTS

The **Archive Reports** options enable you to select the age of the reports to archive and when they should be archived. See Procedure 2-14.

Note: Reports are archived individually in their original format.

Procedure 2-14 Selecting reports to archive

Step	Action
Specifying which reports are to be archived	
1	Select **Archive/Delete**.
2	Select the **Enable Deletion and Archiving** check box, and then select the **Archive Reports** option.
3	Select the **Archive Options** tab.
4	Select one of the options: • All (the default setting) • Before today • Older than last 7 days • Older than last full month
Specifying the date and time to archive the reports	
5	Select the **Date /Time** tab.
6	In the **Time of Day** area, specify a time of day (24hr clock) to archive your reports.
7	In the **Archive Location** field, specify a folder in which to store the archived reports.
8	Click **Apply**.

CHANGING PASSWORDS

Any user can change their own password.

A Reports Administrator can also change the password of other users from the **Users > Edit** option. See Changing User Details on page 18.

PORT NUMBER

To change the port number that Report Central listens on (default of 8888 for HTTP, 8443 for HTTPS) following installation, follow Procedure 2-15.

Procedure 2-15 Changing the Default SRC Port Number

Step	Action
1	Stop the Report Central and Scheduler services.
2	Change the permissions of the 'server.xml' file to enable you to write to it. In a default installation, this file is in: C:\Program Files\SurfControl\Report Central\Tomcat\Conf\
3	Open the file in a text editor.
4	If you are connecting using HTTP, change the port setting (8888) in the line Connector port="8888". If you are connecting using HTTPS, change the port setting (8443) in the line Connector port="8443".
5	Save the server.xml file.
6	In the Registry, change the value of the following key to the same as in server.xml: HKEY_LOCAL_MACHINE\SOFTWARE\SurfControl\Report Central\WebFilter<nn>\Default\Web Server Port
7	Start the Report Central and Scheduler services.
8	From the **Start** menu, select and right-click **Program Files > SurfControl Report Central**, and then select **Properties**.
9	Edit the URL to reflect the new port number, that is, change the 8888 or 8443 part of the URL: http://<SRC.server.name>:8888/WebFilter<nn>/Html/startup.html (for HTTP) https://<SRC.server.name>:8443/WebFilter<nn>/Html/startup.html (for HTTPS)
10	Repeat Steps 8 to 9 for the Web Filter Reports - Secure Connection.

Note: You need to re-distribute a copy of each shortcut to your remote users after changing the port number:
1. From the Start menu, right-click **Web Filter Reports**.
2. From the right-click menu, select **Send To > Mail Recipient**.
3. Repeat for Web Filter Reports - Secure Connection.

SCHEDULER LOG

A log file (`Scheduler.log)` is created for all scheduled events, with the exception of refreshes to the summary data in between scheduled updates. The default installation folder for the log file is:

```
C:\Program Files\SurfControl\Report Central\Tomcat\webapps\WebFilter<nn>
```

Drill-Down Manager

INTRODUCTION

Drill-down reports enable you to investigate the data that a report is based upon. Drill-down report data is updated on a daily basis. The timing of these updates can be scheduled in the **Update Tasks** tab from the **Configuration > Database** settings. See Databases - Web Filter on page 19 or Databases - E-mail Filter on page 23 for more details.

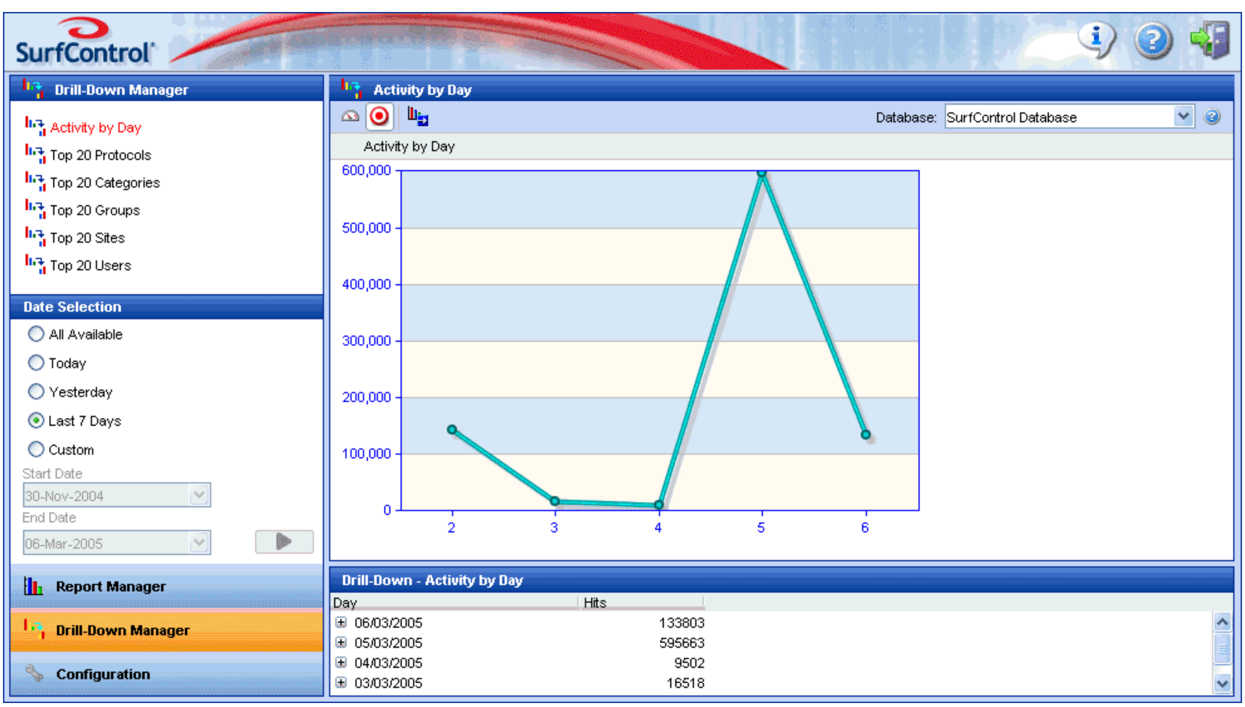
Note: Only permitted users have access to Drill-Down Reporting. See Setting User Permissions on page 16 for more details.

THE DRILL-DOWN REPORTS SCREEN

Figure 3-1 shows the initial drill down screen. The screen is split into the following parts:

- Drill-Down Manager
- Date Selection
- Report View
- Drill Down Data.

Figure 3-1 Drill-Down Reports initial view (example for Web Filter)



DRILL-DOWN MANAGER PANEL - WEB FILTER REPORTS

The available reports are:

- Activity by Day (the default report view)
- Top 20 Protocols
- Top 20 Categories
- Top 20 Groups – Also has a filter for more specific drill-down reporting. The filter supports the use of wildcards.
- Top 20 Sites
- Top 20 Users – Also has a filter for more specific drill-down reporting. The filter supports the use of wildcards.

The report currently displayed is highlighted in red.

DRILL-DOWN MANAGER PANEL - E-MAIL FILTER REPORTS

The available reports are:

- Gateway/Connection Reports:
  - Connections by Day (the default report view)
  - Connections by Type
  - Top 20 IP Addresses
- Message Reports:
  - Total Messages by Day
  - Inbound/Outbound
  - Top 20 Policy Types
  - Top 20 Internal Addresses
  - Top 20 Rules
  - Protected Domains.

The report currently displayed is highlighted in red.

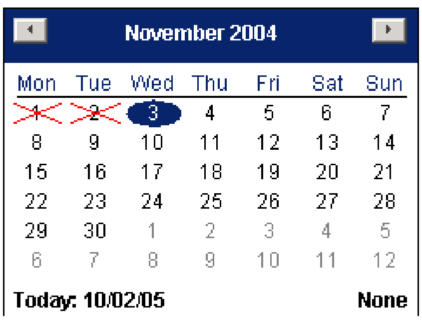
DATE SELECTION

The Date Selection panel enables you to select specific dates for the report view. The options are:

- All Available
- Today
- Yesterday
- Last 7 Days (the default view)
- Custom.

When you select Custom, the Start and End Date drop-down lists become active, which enables you to specify a range of dates from a calendar (Figure 3-2).

Figure 3-2 Date selection calendar



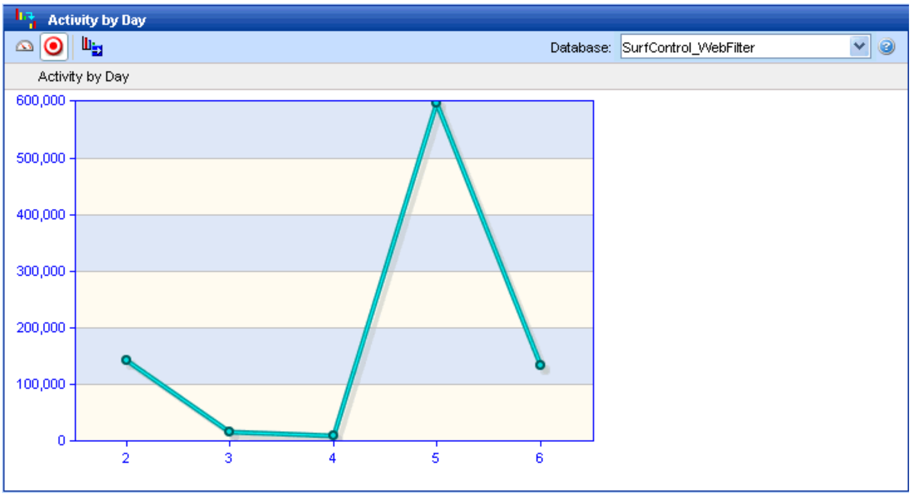
Note: Dates marked with a red cross are not available for selection.

When you have specified a start and end date, click **Go** .

DRILL-DOWN REPORT VIEW

Figure 3-3 shows the Drill-Down Report view panel.

Figure 3-3 Report view panel (example for Web Filter)



Viewing the Drill-Down Report

For Web Filter reports, you can display the reports by:

- Hits (default)
- Bandwidth .

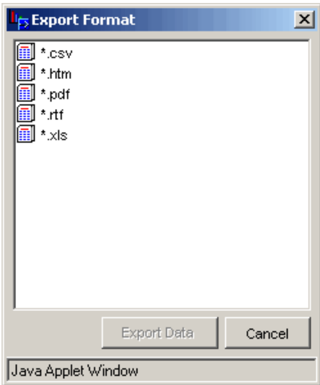
For E-mail Filter reports, you can display the reports by:

- Message size (including attachments)
- Number of messages (volume)

Exporting Report Data

To export the report data, click , and then select a format from the **Export Format** dialog box (Figure 3-4).

Figure 3-4 Export Format dialog box



The available formats are:

- ***.csv** – for use in spreadsheet or database programs, such as Microsoft Excel or Microsoft Access.
- ***.htm** – for viewing in a Web browser.
- ***.pdf** – for viewing in a portable document format viewer, such as Adobe Acrobat.
- ***.rtf** – for use in a word processor, such as Microsoft Word.
- ***.xls** – for use in Microsoft Excel (version 8 or later).

You can select other configured database connections from the **Database** drop-down list box. For more information on database connections, see Databases - E-mail Filter on page 23.

THE DRILL-DOWN DATA PANEL

Figure 3-5 shows the Drill-Down Data panel. The initial view shows a collapsed view of the report data.

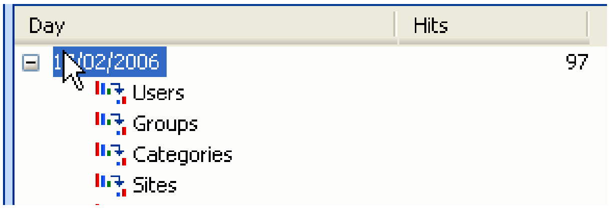
Note: The data displayed varies according to the report selected, and whether you are viewing by Size or Volume.

Figure 3-5 Drill-Down data panel

Navigating the Drill-Down Data

Expanding a category enables you to view the drill-down data in sub-categories. These sub-categories are hyperlinks to the data (Figure 3-6).

Figure 3-6 Expanded data

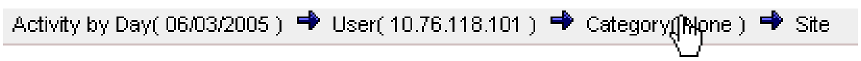


The graph shows the selected data, which depends on the data available in the report.

To help you to navigate through the data, there is a breadcrumb navigation system above the graph. Each step is a hyperlink that enables you to go back to a previous step in the drill-down process.

Figure 3-7 shows an example of the breadcrumb navigation.

Figure 3-7 Breadcrumb navigation



Report Manager – Web Filter

INTRODUCTION

This chapter explains how to generate reports from the Report Manager.

There are two types of report:

- Report Templates– reports generated using supplied settings (criteria).
- Saved/Scheduled – reports generated using your own saved settings.

PRECONFIGURED TYPES OF REPORT

The preconfigured types of report supplied with Report Central are:

- Quick Reports
- Summary Reports
- Comparison Reports
- Detail Reports.

All reports use the **Date/Time** and **Options** criteria. By default, reports are based on all available criteria and data for the last 7 days. For details of available criteria that you can change to create reports, see Specifying Report Criteria on page 56.

All reports contain the Date Range and the date on which the report was run, but the data shown depends on the type of report.

The contents of the reports are detailed in the following sections.

QUICK REPORTS

The following table describes Quick reports.

Table 4-1 Quick reports

Report name	Type	Data shown in report	Ordered by
Blocked Category Summary	Table	• Category • No. of Blocked Connections	Connections
Top 10 Categories	Bar Chart & Table	• Category • No. of Connections	Connections
Top 10 Groups	Bar Chart & Table	• Group • No. of Connections	Connections
(Sheet 1 of 2)			

Table 4-1 Quick reports (Continued)

Report name	Type	Data shown in report	Ordered by
Top 10 Groups by Cost	Bar Chart & Table	• Browse Sensitivity • Cost per hour • Group • Cost	Cost
Top 10 pages	Table	• No. of Connections • Page	Connections
Top 10 Protocols (only for Windows and ISA Server)	Bar Chart & Table	• Protocol • No. of Connections	Connections
Top 10 Sites (only for Windows and ISA Server)	Bar Chart & Table	• Site • Connections	Connections
Top 10 SMTP E-mail Receivers by Size (only for Windows and ISA Server)	Bar Chart	• Receiver • Bytes Received	Bytes Received
Top 10 SMTP E-mail Senders by Size (only for Windows and ISA Server)	Bar Chart	• Sender • Bytes Sent	Bytes Sent
Top 10 Users by Browse Times	Bar Chart & Table	• Browse Sensitivity • User • Hours	Browse Time
Top 10 Users by Connections	Bar Chart	• User • No. of Connections	Connections
Top 10 Users by Connections showing Categories	Bar Chart & Table	• User • No. of Connections • Category	Connections
Top 10 Users by Cost	Bar Chart & Table	• Browse Sensitivity • Cost per hour • User • Cost	Cost
Top 10 Workstations by Connections (not available in the Privacy Edition of Web Filter)	Bar Chart & Table	• Workstation • No. of Connections	Connections
(Sheet 2 of 2)			

SUMMARY REPORTS

The following table describes Summary reports.

Table 4-2 Summary reports

Report name	Type	Data shown in report	Ordered by
Top N Categories by Connections	Table	• Category • No. of Connections • Bytes Sent • Bytes Received	Connections
Top N Groups by Connections	Table	• Groups • No. of Connections • Bytes Sent • Bytes Received	Connections
Top N Groups by Cost	Table	• Browse Sensitivity • Cost per hour • Groups • Total Cost • Total Browse Time	Total Cost
Top N Groups showing Category by User	Table	• Group • User • No. of Connections • Category	Category within group
Top N Protocols (only for Windows and ISA Server)	Table	• No. of Connections • Protocol • Data Sent/Received	Connections
Top N sites by Bandwidth (only for Windows and ISA Server)	Table	• No. of Connections • Site • Total Data Sent/Received	Total Data
Top N sites by Connections	Table	• Site • No. of Connections • Data Sent • Data Received	Connections
Top N SMTP E-mail Receivers by Quantity (only for Windows and ISA Server)	Table	• Recipient • E-mail Receiver	E-mails received
(Sheet 1 of 2)			

Table 4-2 Summary reports (Continued)

Report name	Type	Data shown in report	Ordered by
Top N SMTP E-mail Receivers by Size (only for Windows and ISA Server)	Table	• Recipient • Total Size • Receiver	Bytes Received
Top N SMTP E-mail Senders by Quantity (only for Windows and ISA Server)	Table	• Sender • E-mails Sent	E-mails Sent
Top N SMTP E-mail Senders by Size (only for Windows and ISA Server)	Table	• Total Size • Sender **Note:** This report is not available in the Privacy Edition of Web Filter	Total Size
Top N Users by Browse Times	Table	• Browse Sensitivity • User • Total Browse Time	Total Browse Time
Top N Users by Connections	Table	• User • No. of Connections • Data Sent • Data Received	Connections
Top N Users by Connections showing Categories	Table	• User • No. of Connections • Category	Connections
Top N Users by Connections showing Protocols (only for Windows and ISA Server)	Table	• User • No. of Connections • Protocol	Connections
Top N Users by Cost	Table	• Browse Sensitivity • Cost per hour • User • Total Cost • Total Browse Time	Cost
Top N Workstations by Connections (not available in the Privacy Edition of Web Filter)	Table	• Workstation • No. of Connections • Data Sent • Data Received	Connections
(Sheet 2 of 2)			

COMPARISON REPORTS

The following table describes Comparison reports.

Table 4-3 Comparison reports

Report name	Type	Data shown in report	Ordered by
Bandwidth by Category (only for Windows and ISA Server)	Bar Chart	• Category • Data Sent • Data Received	Data Sent and Data Received
Bandwidth by Date (only for Windows and ISA Server)	Bar Chart	• Date • Bytes Sent • Bytes Received	Date
Bandwidth by Group (only for Windows and ISA Server)	Bar Chart	• Group • Data Sent • Data Received	Data
Bandwidth by Hour (only for Windows and ISA Server)	Bar Chart	• Date • Bytes Sent • Bytes Received	Hour
Category by Connections and Group	Table	• Category • Group • No. of Connections	Connections
Category Time Analysis	Line Graph	• Category • No. of Connections • Time	N/A
Connections by Date	Bar Chart & Table	• Date • No. of Connections	Date
Connections by Day of Week	Bar Chart & Table	• Day • No. of Connections	Day
Connection by Hour of Day	Bar Chart & Table	• Hour • No. of Connections	Hour
Group Time Analysis	Line Graph	• Group • No. of Connections • Time	N/A
Groups by Category and Connections	Table	• Group • Category • No. of Connections • Time	Connections
(Sheet 1 of 2)			

Table 4-3 Comparison reports (Continued)

Report name	Type	Data shown in report	Ordered by
Protocol Data Analysis (only for Windows and ISA Server)	Table	• Protocol • User • Bytes Sent • Bytes Received • First Access • Last Access	Protocol
Protocol Time Analysis	Line Graph	• Protocol • Time • No. of Connections	N/A
(Sheet 2 of 2)			

DETAIL REPORTS

The following table describes Detail reports.

Table 4-4 Detail reports

Report name	Type	Data shown in report	Ordered by
Blocked AVA Detail (only for ISA server with AVA)	Table	• Date/Time • User • Page • Category: – Malware – Denial of Service • Subcategory: – Treat DoS Criteria As Infected – Treat Encrypted Files As Infected – Treat Errors As Infected – Treat Macros As Infected – Heuristic Analysis – Macro Analysis – Scan All Macros – Delete All Macros – Malicious Apps – Jokes Hoax	Date/Time
Blocked Category Detail	Table	• Category • Site • Page • User • No. of Connections	Category
Blocked Page Detail	Table	• Site • Page • User • No. of Connections	Category
Blocked User Activity	Table	• User • Site • Category • Access Time	User
(Sheet 1 of 3)			

Table 4-4 Detail reports (Continued)

Report name	Type	Data shown in report	Ordered by
Browse Time Activity Detail	Table	• Browse Sensitivity • Browse Allowance • User • Date • From • To • Duration	User
Browse Time by User and Category	Table	• Browse Sensitivity • User • Category • Duration	User
Category Bandwidth Detail (only for Windows and ISA Server)	Table	• Category • Bytes Sent • Bytes Received	Category
Newsgroup Analysis (only for Windows and ISA Server)	Table	• User • Date • Time • Page • Size	User
Site Access by Connections	Table	• Site • IP Address • No. of Connections	Connections
Site Activity (only for Windows and ISA Server)	Table	• Site • Activity • User • Protocol • Bytes Sent • Bytes Received • Date/Time of Connection	Site
Site Categorization Details	Table	• Category • Site • Page • No. of Connections	Category
User Access	Table	• User • No. of Connections • First Access • Last Access	Connections
(Sheet 2 of 3)			

Table 4-4 Detail reports (Continued)

Report name	Type	Data shown in report	Ordered by
User Activity	Table	• User • Category • Site • Last Access	User
User Activity Detail	Table	• User • Site • Activity • Category • Date/Time • Duration	User
User Bandwidth Detail (only for Windows and ISA Server)	Table	• User • Bytes Sent • Bytes Received	User
User Cost Analysis	Table	• Browse Sensitivity • Cost per hour • User • Duration • Cost • First Access • Last Access	User
(Sheet 3 of 3)			

HOW BROWSE TIME IS CALCULATED FOR REPORTS

Report Central splits a day into segments, which have a default length of three minutes. The length of a segment is known as the browse time sensitivity (BTS), and is the maximum notional period of time that a user will spend browsing each page. The number of segments in which there are connections is then calculated to give a browse time. You can change the BTS using the **Options** tab. See Options on page 65 for more details.

HOW BROWSE TIME SENSITIVITY IS USED

Browse time sensitivity is used differently for the following:

- Single connection
- Multiple connections
- Browse Time by User and Category reports
- User Activity Detail reports.

Single Connection

A single connection to a Web site—using the default browse time sensitivity setting—is calculated as having a browse time of three minutes. This is even if you connect to the site for more or less than three minutes.

Note: Some reports that use browse time sensitivity also show when the duration of a connection reaches a limit. The default for this threshold limit is five minutes. See Options on page 65 for more details.

Multiple Connections

Table 4-5 shows how browse time sensitivity is used for multiple connections.

Table 4-5 Multiple connections and browse time sensitivity

Site	From	To	Calculated Browse Time
site1.com	09:57	10:00	3 minutes
site2.com	09:57	10:00	
site3.com	10:00	10:03	3 minutes
Total Calculated Browse Time			**6 minutes**

In the three minute segment of 09:57 to 10:00, you make two connections to different sites. This gives a browse time sensitivity of three minutes because the number of sites are not important in the calculation, only the amount of time a user spends on the Internet within any one segment.

When you make another connection in the next three minute period (10:00 to 10:03), this counts as another connection. Therefore, this is calculated as having a browse time of three minutes, which gives a total of six minutes.

Browse Time by User and Category Report

Table 4-6 shows how browse time sensitivity is used in this report.

Table 4-6 Browse time by user and category

Site	Category	From	To	Calculated Browse Time
site1.com	1	09:57	10:00	3 minutes
site2.com	2	09:57	10:00	3 minutes
site3.com	1	10:00	10:03	3 minutes
Total Calculated Browse Time				**9 minutes**

You browse to two sites within a single three minute segment. Site1.com is in one category, site2.com is in another. To report by category these are counted as two separate connections and are given a separate browse time. If these two sites were in the same category, the browse time sensitivity would be the same as in Table 4-6.

When you connect to site3.com in the next time segment, this is counted as another connection and given a browse time of three minutes. This can give different totals than other reports using browse time sensitivity for the same time period.

User Activity Detail Report

For this report, the browse time for each user is calculated as the sum of the differences between each Web page connection by that user. However, each connection is limited to a maximum of the browse time sensitivity (BTS). For details of BTS, see How Browse Time is Calculated For Reports on page 53.

Table 4-7 shows how a browse time sensitivity of three minutes is used in these reports.

Table 4-7 Browse time for User Activity Detail report

Site	From	To	Potential Browse Time	Calculated Browse Time
site1.com (first page)	16:51:00	17:05:00	14 minutes	3 minutes (BTS)
site2.com	17:05:00	17:05:10	10 seconds	10 seconds
site2.com\page 1	17:05:10	17:05:30	20 seconds	20 seconds
site2.com\page 2	17:05:30	17:10:00	4 mins 30 secs	3 minutes (BTS)
site3.com	17:10:00	17:12:00	2 minutes	2 minutes
Total Calculated Browse Time				**12 mins 30 secs**

Table 4-7 Browse time for User Activity Detail report

Site	From	To	Potential Browse Time	Calculated Browse Time
site4.com	17:12:00	17:13:00	1 minute	1 minutes
site5.com (last page)	17:13:00	-	Unknown	3 minutes (BTS)
Total Calculated Browse Time				**12 mins 30 secs**

SETTING UP REPORTS

There are a maximum of four stages to setting up a report:

1 Selecting the report to run
2 Specifying report criteria
3 Specifying running options
4 Specifying scheduling options.

SELECTING A REPORT

From the Report Manager options, select a report from one of the categories. The criteria for that report is displayed in the right-hand pane.

Note: The time and date on the computer where Report Central is installed must be the same as the SQL Server. If these do not match, the time and date may not be reported accurately.

When you select a report, SurfControl Report Central retrieves the time and date information from the database. If there is a problem connecting to your database you will receive an error message detailing the problem.

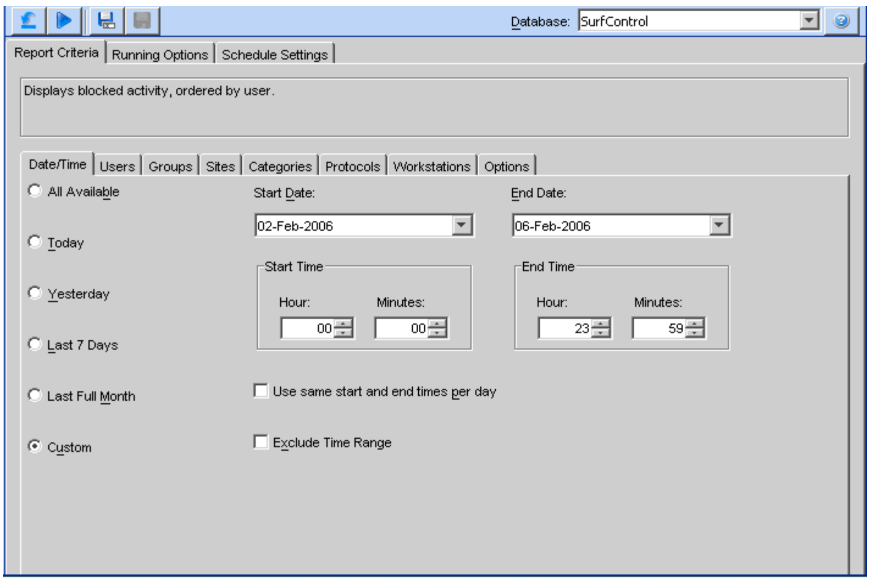
You should check that:

- Report Central is connecting to a valid database (**Configuration > Database Connections**).
- The database that Report Central is connecting to contains valid data.
- the SQL Server is running correctly (**SQL Service Manager**).

SPECIFYING REPORT CRITERIA

The options in the Report Criteria page enable you to select the criteria for your reports. The tabs available in this page depend on the type of report and your user permissions. Figure 4-1 shows a typical Report Criteria page.

Figure 4-1 Report Criteria



The tabs are:

- Date/Time – page 57
- Users – page 59
- Groups – page 60
- Sites – page 61
- Categories – page 62
- Protocols – page 63
- Workstations – page 64
- Options – page 65.
- Database – page 66. This tab is only available for saved reports.

You also have the following options from this screen:

- Revert to Saved/Default Report Settings – 
- Run Report – 

- Save As – 
- Save (only available for saved reports) – 

Use the **Database:** drop-down list box to select the database from which to run your reports.

Date/Time

Table 4-8 shows the Date/Time criteria.

Table 4-8 Time/Date criteria

Time/Date	Description
All Available	All available data stored on the database.
Today	All data logged to the database today.
Yesterday	All data logged to the database yesterday (between 00hrs and 24hrs).
Last 7 Days	all data logged to the database in the last seven days, (the default setting).
Last full month	All data logged to the database in the last full month.
Custom	All data logged to the database in the time period you specify. See Procedure 4-1.

Specifying a Custom Time Period for Reports. Use this option to report on data from a time period that you specify (Procedure 4-1).

Procedure 4-1 Specifying a custom time period for reports

Step	Action
1	Select a **Start Date** by clicking the drop-down list box and selecting a day from the calendar. **Note:** Dates marked with a red cross are not available for selection.
2	Select an **End Date** by clicking the drop-down list box and selecting a day from the calendar. **Note:** Dates marked with a red cross are not available for selection.
3	Specify a **Start Time** (in 24 hr clock).
4	Specify an **End Time** (in 24 hr clock).
5	To report on data from the same time period each day, select **Use same start and end times each day.** See Table 4-9 for an explanation of this feature.
6	To report on data from outside the time period you specify, select **Exclude Time Range.** See Table 4-10 for an explanation of this feature.

Use Same Start and End Times Each Day

Use this option to report on data from the same time frame each day.

Table 4-9 Use same start and end times each day check box

Checkbox	What happens	Example
Cleared	The report uses data from the entire date range you specify, beginning at the start time on the start date and ending at the end time on the end date.	Between 9am on day 1 and 5pm on day 3.
Selected	SurfControl Report Central uses report data from the time period you specify, for each day between the start and end date.	Between 9am and 5pm on day 1, 9am and 5pm on day 2, etc.

Exclude Time Range

You can use the **Exclude Time Range** check box independently of the **Use same start and end times per day** check box.

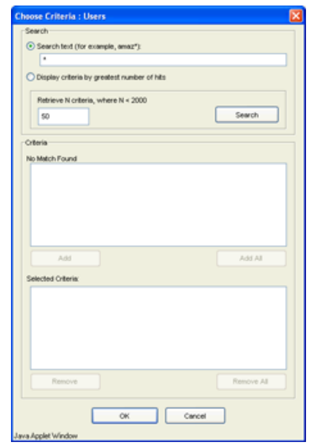
Table 4-10 Exclude Time Range check box

Checkbox	What happens	Example
Cleared	The report uses data from the time period you specify.	Between 9am and 5pm on day 1.
Selected	The report uses any data excluded by the Use same start and end times per day options.	Midnight until 9am and 5pm until 11:59pm on day 1.

Users

The **Users** tab is used to specify selected users, or to exclude users from reports. By default, all monitored users are included in reports. Any new users are added automatically.

Procedure 4-2 Specifying users in a report

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td>1</td><td colspan="2">Select the Users tab.</td></tr>
<tr><td>2</td><td>
To include all users in the report, click Include all.
To include or exclude specific users, select Include selected items or Exclude selected items. A Choose Criteria: Users dialog box is displayed.
Note: If there are already users in the Selected Criteria: list on the Users tab, you need to click Add to display the Choose Criteria: dialog box.
</td><td>


</td></tr>
<tr><td>3</td><td colspan="2">
You have three methods for selecting users:

Search for a user by entering search text. You can use wildcards. Click Search. The search results are displayed in the Available Criteria: list.
To filter users based on the number of times a user has accessed an Internet site (hits), select Display criteria by greatest number of hits. Enter the number of search requests to display (between 1 to 2000). Click Search. The users will be displayed in descending order of hits in the Available Criteria: list.

Note: To increase the maximum number of records returned to greater than 2000, consult Knowledge Base article 1596 from http://kb.surfcontrol.com

Select users by scrolling through the Available Criteria: list. To select multiple users, use Ctrl or Shift. Click Add. To select all users, click Add All. The selected users are displayed in the Selected Criteria: list.
To remove one or more users from the Selected Criteria: list, either select the users, and then click Remove. To remove all users from the list, click Remove All.

Note: Restricted users cannot change User criteria.
</td></tr>
<tr><td>4</td><td colspan="2">Click OK to confirm the selection.</td></tr>
</table>

Groups

You can use the **Groups** tab to include only selected groups or to exclude selected groups for your reports. By default, all groups defined in SurfControl Web Filter are included in reports Any new groups are added automatically.

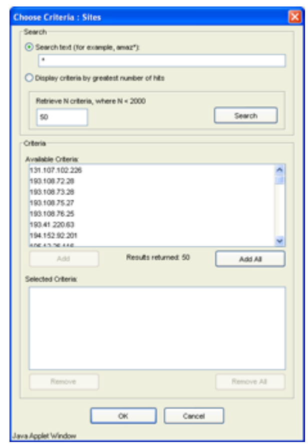
Procedure 4-3 Specifying groups in a report

Step	Action	
1	Select the **Groups** tab.	
2	To include all groups in the report, click **Include all**. To include or exclude specific groups, select **Include selected items** or **Exclude selected items**. A **Choose Criteria: Groups** dialog box is displayed. **Note:** If there are already groups in the Selected Criteria: list on the Groups tab, you need to click Add to display the Choose Criteria: dialog box.	
3	You have three methods for selecting groups: • Search for a group by entering search text. You can use wildcards. Click **Search**. The search results are displayed in the **Available Criteria:** list. • To filter groups based on the number of times a group has accessed an Internet site (hits), select **Display criteria by greatest number of hits**. Enter the number of search requests to display (between 1 to 2000). Click **Search**. The groups will be displayed in descending order of hits in the **Available Criteria:** list. **Note:** To increase the maximum number of records returned to greater than 2000, consult Knowledge Base article 1596 from http://kb.surfcontrol.com • Select groups by scrolling through the **Available Criteria:** list. To select multiple groups, use Ctrl or Shift. Click **Add**. To select all groups, click **Add All**. The selected groups are displayed in the **Selected Criteria:** list. To remove one or more groups from the **Selected Criteria:** list, either select the groups, and then click **Remove**. To remove all groups from the list, click **Remove All**. **Note:** Restricted users cannot change the criteria for Groups.	
4	Click **OK** to confirm the selection.	

Sites

You can use the **Sites** tab to include only selected sites or to exclude selected sites for your reports. By default, all Web sites logged by the SurfControl Web Filter database are included in reports Any new sites are added automatically.

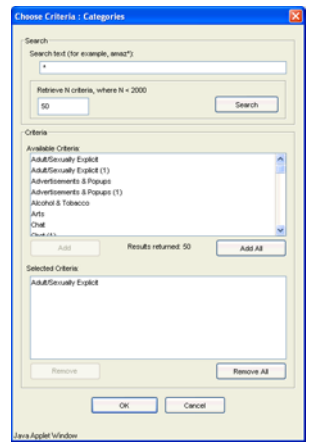
Procedure 4-4 Specifying sites in a report

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td>1</td><td colspan="2">Select the Sites tab.</td></tr>
<tr><td>2</td><td>To include all sites in the report, click Include all.
To include or exclude specific sites, select Include selected items or Exclude selected items. A Choose Criteria: Sites dialog box is displayed.
Note: If there are already sites in the Selected Criteria: list on the Sites tab, you need to click Add to display the Choose Criteria: dialog box.</td><td>
</td></tr>
<tr><td>3</td><td colspan="2">You have three methods for selecting sites:
• Search for a sites by entering search text. You can use wildcards. Click Search. The search results are displayed in the Available Criteria: list.
• To filter sites based on the number of times a site has accessed an Internet site (hits), select Display criteria by greatest number of hits. Enter the number of search requests to display (between 1 to 2000). Click Search. The sites will be displayed in descending order of hits in the Available Criteria: list.
Note: To increase the maximum number of records returned to greater than 2000, consult Knowledge Base article 1596 from http://kb.surfcontrol.com
• Select sites by scrolling through the Available Criteria: list. To select multiple sites, use Ctrl or Shift. Click Add. To select all sites, click Add All. The selected sites are displayed in the Selected Criteria: list.
To remove one or more sites from the Selected Criteria: list, either select the sites, and then click Remove. To remove all sites from the list, click Remove All.
Note: Restricted users cannot change the criteria for Sites.</td></tr>
<tr><td>4</td><td colspan="2">Click OK to confirm the selection.</td></tr>
</table>

Categories

You can use the **Categories** tab to only include selected categories or to exclude selected categories for your reports. By default, sites classed by Web Filter as ‘Uncategorized’ are excluded from the report.

Procedure 4-5 Specifying categories in a report

Step	Action
1	Select the **Categories** tab.
2	To include all categories in the report, click **Include all**. To include or exclude specific categories, select **Include selected items** or **Exclude selected items**. A **Choose Criteria: Categories** dialog box is displayed. **Note:** If there are already categories in the Selected Criteria: list on the Categories tab, you need to click Add to display the Choose Criteria: dialog box. 
3	You have three methods for selecting categories: • Search for a category by entering search text. You can use wildcards. Click **Search**. The search results will be displayed in the **Available Criteria:** list. • To filter categories based on the number of times a category has accessed an Internet site (hits), select **Display criteria by greatest number of hits**. Enter the number of search requests to display (between 1 to 2000). Click **Search**. The categories will be displayed in descending order of hits in the **Available Criteria:** list. **Note:** To increase the maximum number of records returned to greater than 2000, consult Knowledge Base article 1596 from http://kb.surfcontrol.com • Select categories by scrolling through the **Available Criteria:** list. To select multiple categories, use Ctrl or Shift. Click **Add**. To select all categories, click **Add All**. The selected categories are displayed in the **Selected Criteria:** list. To remove one or more categories from the **Selected Criteria:** list, either select the categories, and then click **Remove**. To remove all categories from the list, click **Remove All**. **Note:** Restricted users cannot change the criteria for Categories.
4	Click **OK** to confirm the selection.

Protocols

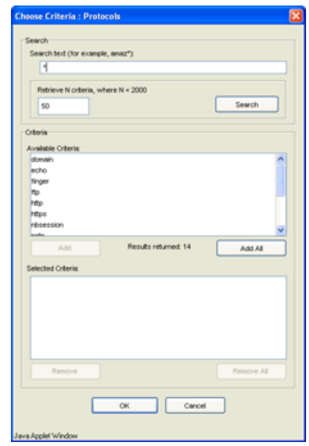
By default, all protocols are included in a report. Use the **Protocols** tab to exclude protocols you do not want to report on.

Procedure 4-6 Specifying protocols in a report

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td>1</td><td colspan="2">Select the Protocols tab.</td></tr>
<tr><td>2</td><td>To include all protocols in the report, click Include all.

To include or exclude specific protocols, select Include selected items or Exclude selected items. A Choose Criteria: Protocols dialog box is displayed.

Note: If there are already protocols in the Selected Criteria: list on the Protocols tab, you need to click Add to display the Choose Criteria: dialog box.</td><td>



</td></tr>
<tr><td>3</td><td colspan="2">You have three methods for selecting protocols:

• Search for a protocols by entering search text. You can use wildcards. Click Search. The search results are displayed in the Available Criteria: list.

• To filter protocols based on the number of times a protocol has accessed an Internet site (hits), select Display criteria by greatest number of hits. Enter the number of search requests to display (between 1 to 2000). Click Search. The protocols will be displayed in descending order of hits in the Available Criteria: list.

Note: To increase the maximum number of records returned to greater than 2000, consult Knowledge Base article 1596 from http://kb.surfcontrol.com

• Select protocols by scrolling through the Available Criteria: list. To select multiple protocols, use Ctrl or Shift. Click Add. To select all protocols, click Add All. The selected protocols are displayed in the Selected Criteria: list.

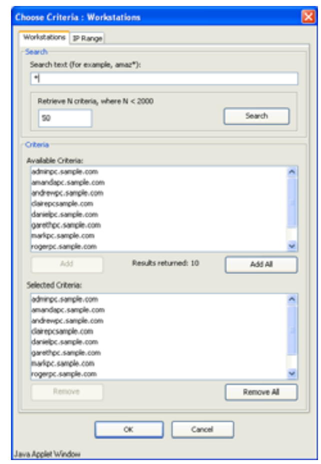
To remove one or more protocols from the Selected Criteria: list, either select the protocols, and then click Remove. To remove all protocols from the list, click Remove All.

Note: Restricted users cannot change the criteria for Protocols.</td></tr>
<tr><td>4</td><td colspan="2">Click OK to confirm the selection.</td></tr>
</table>

Workstations

Use this tab to include or exclude workstation names and/or IP address ranges in your report.

Procedure 4-7 Specifying workstations and/or IP address ranges in a report

Step	Action
1	Select the **Workstations** tab.
2	To include all workstations and/or IP addresses in the report, click **Include all**. To include or exclude specific workstations and /or IP addresses, select **Include selected items** or **Exclude selected items**. A **Choose Criteria: IP Addresses** dialog box is displayed. **Note:** If there are already workstations or IP addresses in the Selected Criteria: list on the Workstations tab, you need to click Add to display the Choose Criteria: dialog box. 
3	You have four methods for selecting workstation names and/or IP addresses: • Search for a workstation name by entering search text. You can use wildcards. Click **Search**. The search results are displayed in the **Available Criteria:** list. Click **Add**. The selected workstation names are displayed in the **Selected Criteria:** list. • To filter workstations based on the number of times a workstation has accessed an Internet site (hits), select **Display criteria by greatest number of hits**. Enter the number of search requests to display (between 1 to 2000). Click **Search**. The workstations will be displayed in descending order of hits in the **Available Criteria:** list. **Note:** To increase the maximum number of records returned to greater than 2000, consult Knowledge Base article 1596 from http://kb.surfcontrol.com • Select workstations by scrolling through the **Available Criteria:** list. To select multiple workstations, use Ctrl or Shift. Click **Add**. To select all workstations, click **Add All**. The selected workstations are displayed in the **Selected Criteria:** list. To remove one or more workstations from the **Selected Criteria:** list, either select the workstations, and then click **Remove**. To remove all workstations from the list, click **Remove All**. • Click the **IP Range** tab, and then enter a range of IP addresses in the **From:** and **To:** text fields. The **From:** address must be lower than the **To:** address, and both must be in a valid format between 0.0.0.0 and 255.255.255.255. Click **Add** to add the range to the **Selected Criteria:** list in the tab. When you have made your selection, click **OK**. The range is added to the **Selected Criteria:** list in the **Workstations** tab. **Note:** Restricted users cannot change the criteria for workstation names or IP addresses.
4	Click **OK** to confirm the selection.

Options

The **Options** tab is available for all Summary Reports and the following:

- Quick Reports:
  - Top 10 Groups by Cost
  - Top 10 Users by Cost
  - Top 10 Users by Browse Time.
- Detail Reports:
  - Blocked AVA Detail (only for ISA server with AVA)
  - Blocked Category Detail
  - Blocked Page Detail
  - Blocked Protocol Detail
  - Blocked User Activity
  - Browse Time Activity Detail
  - Browse Time by User and Category
  - Browse Time by User and Site showing Category
  - Site Activity
  - User Activity Detail
  - User Cost Analysis.

For all Summary Reports you can set the value of ‘N’ to display the specific number of results. The default is 10.

Additionally for some Summary Reports, Quick Reports and Detail Reports, depending on the type of report, you can specify:

Workstation cost per hour - You can set a cost of Internet activity for each workstation. The default is 30.00. Report Central uses the Regional Settings currency for the server, where installed.

Browse time sensitivity – The number of minutes that are used to calculate browse sensitivity data. See How Browse Time is Calculated For Reports on page 53 for more details. The default is three minutes.

File extension filter - Depending on the report, you can specify file extensions to include in or exclude from the report. The format is *.[file extension]. To specify multiple file extensions, separate each extension with a comma.

Browse duration alert – Any browsing that exceeds this limit will be highlighted in red in the report. The default setting is five minutes.

Database

The **Database** tab is displayed for Saved/Scheduled reports only and shows you the database connection settings used when the report was originally saved. SurfControl recommends that you do not attempt to change databases if reports are potentially being generated from the current one.

Procedure 4-8 Changing the database used for reports

Step	Action
1	Select the **Database** tab.
2	Select a database connection from the drop-down list box.

You can now do one of the following:

- Revert to the last saved settings –
- Run Report –
- Save As –
- Save to replace the default settings –

If you do not use any of the save options, the new settings are discarded when you log out of Report Central.

SPECIFYING RUNNING OPTIONS

Use the **Running Options** tab to control how your report is produced and where it is saved.

Display Selected Criteria

You can choose to display the report criteria on the last page. If you choose to do this, the criteria that you have selected will be printed. For example, if you choose to generate a report on Users, the criteria displayed on the report will be of the form:

Selected Users: April, Brian, Mary

Note: If you use the default setting of including all criteria, the selected criteria is not shown, even if you select Display Selected Criteria.

Format

You can generate reports in the following formats in Table 4-11.

Table 4-11 Report formats

Format	Details
.csv	Comma Separated Value – a text format that can be used by spreadsheet and database programs such as Microsoft Excel and Access.
.htm	You can view the report in HTML format using a Web browser.
.pdf	Portable Document Format is the default format. You require a reader such as Adobe Acrobat Reader to view. Adobe Acrobat Reader is available as a free download from www.adobe.com). **Note:** You need version 6 or later of Adobe Acrobat Reader to read reports in this format. **Note:** SurfControl recommends that you use PDF files as attachments to e-mails.
.rtf	Rich Text Format files can be viewed in word processors, such as Microsoft Word.
.xls	Microsoft Excel Format (version 8 or later).

Caution: Pop-up blockers, such as those used by Google, Yahoo! or Microsoft Windows XP SP2, can prevent reports displaying in your browser. You need to alter your settings to allow pop-ups from the Report Central address.

Caution: If using a secure (HTTPS) connection to Report Central, you need to make changes in Internet Explorer to be able to view reports in pdf and rtf format.
In the Tools > Internet Options...> Advanced tab, clear the "Do not save encrypted pages to disk" check box.

Destination Type

You can specify how you want a report to be displayed. If you choose to e-mail a report, note that reports are e-mailed in their native format and will not be compressed. If you are unsure about the size of a report to e-mail, save the report to your machine using the Schedule options. You can then check the size of the report before you send it. Table 4-12 shows the destination type options.

Note: If you create a report and e-mail it in HTML format, some e-mail programs may not preview the report correctly. However, if you open the e-mail, the report will display successfully.

Table 4-12 Destination type options

Option	Details
Show in Browser (default)	Reports in HTML and PDF format will open automatically in a browser window.
Send by e-mail	The report will be sent as an attachment to the e-mail address you specify. You can add multiple recipients by separating the addresses with a semicolon. **Note:** SurfControl recommends that you use PDF files as attachments to e-mails.

Procedure 4-9 describes how to specify running options:

Procedure 4-9 Specifying running options

Step	Action
1	Select the **Running Options** tab.
2	To display the report criteria, select **Display Selected Criteria**.
3	Select a report format from the list.
4	From the **Destination Type** menu, select how you want the report to be displayed.
5	If you have selected to send the report as an e-mail, enter one or more e-mail addresses in the **Receiver's E-mail Address** field. **Note:** SurfControl recommends that you use PDF files as attachments to e-mails.
6	Click **Run** to run the report.

SCHEDULE SETTINGS

You can use the **Schedule Settings** tab to set up reports to run automatically at specific times or dates.

Enabling Report Scheduling

To enable report scheduling, select the **Schedule Report** check box. When you enable report scheduling, two tabs become available:

- Date/Time
- Save Options.

Date/Time

On this tab you can specify the following:

- **Time of Day** - Specify the hour and minute to run a report (using the 24 hr clock).
- **Every** - Specify which days of the week to run a report. You can run reports every day, once a week or on selected days.
- **Monthly** - Specify a day of the month to run a report, or run a report on the last day of the month. If you select the monthly check box, the Daily/Weekly options are unavailable.

Save Options

When the report you have scheduled is generated, you can automatically save it to your hard drive by specifying save options.

Table 4-13 Save Options

Option	Details
Format	You can save the report in the following formats: .csv .htm .pdf - Recommended format for an attachment to an e-mail. .rtf .xls See Format on page 67 for information about each format.
Destination type	Save on Hard drive – The report will be saved to your computer's hard drive. This is useful if you want to check the size of the file before sending it by e-mail.
	Send by e-mail – The report will be sent as an attachment to the e-mail address you specify. **Note:** SurfControl recommends that attachments should be PDF files.

GENERATING REPORTS

When you have set up your criteria, you are ready to generate the report.

Managing Large Reports

Some reports can generate extremely large volumes of data, especially in large organizations with heavy network traffic. SurfControl Report Central limits the amount of information to 20,000 lines (approximately 1000 pages) for each report. If you run reports that exceed this limit, a note is added to the first page of the report.

There are two ways to manage large reports:

- Print the report to file, see Save Options on page 69. You can then view the report without having to print it, or print only selected pages.
- Constrain a scheduled report by limiting the range of data you are reporting on.

Table 4-14 shows the reports that can generate large volumes of data.

Table 4-14 High-volume reports

Report type	Report name	How to Constrain it
Detail reports	Browse Time Activity Detail	Specify a user.
	Browse Time by User and Category	
	Newsgroup Analysis	Limit the number of sites to 1000 or fewer.
	Site Access by Connections	
	Site Activity	Specify a site or a user.
	Site Categorization Details	Limit the number of sites to 1000 or fewer.
	User Access	Limit the number of users to 10 or fewer.
	User Activity	
	User Activity Detail	
	User Bandwidth Detail	Specify a user.
	User Cost Analysis	

When you have set up your report, click **Run**. Alternatively, to return all the report options to their default settings, click **Revert to Default**.

SAVING REPORTS

When you have set up your report, you can save a copy to your hard drive. There are two ways to save a report:

- Save the report to a Shared folder.
- Save the report to a Personal folder.

See Configuring User Accounts on page 15 for more information about folders and permissions. Procedure 4-10 details how to save a report.

SHARED FOLDER

Any user can view report criteria saved in the Shared folder. Users with the necessary permissions can also change the report criteria.

Note: If you change a report from the Shared folder, use Save As to make sure that you do not overwrite another user's report.

PERSONAL FOLDER

A report saved to the Personal folder can be viewed only by the user who created it.

To save a report:

Procedure 4-10 Saving a report

Step	Action
1	Set up the report using your required criteria and options.
2	Click **Save As**. The **Save Report** dialog box opens.
3	Select the folder in which to save the report.
4	In the **Report Name** field, enter a name for your report.
5	Click **Save**. The **Saved Reports** tab is displayed in the dialog box.

SAVED REPORTS

When you have saved a report to the Shared or Personal folders, a new tab, **Saved Reports,** will be added to the dialog box. This tab shows which reports have been generated.

Note: Only reports that have been saved using the 'Save on Hard Drive' option are displayed in the Saved Reports tab (see Save Options on page 69). Reports sent by e-mail are not displayed.

CREATING FOLDERS WITHIN SHARED AND PERSONAL FOLDERS

To create folders within the Shared and Personal folders:

1 Select the Shared or Personal folder.

2 Click .

DELETING REPORTS OR FOLDERS FROM SHARED AND PERSONAL FOLDERS

To delete reports or folders from Shared and Personal folders:

1 Select the folder or report within the Shared or Personal folder.

2 Click .

Report Manager – E-mail Filter

INTRODUCTION

This chapter explains how to generate reports from the Report Manager.

There are two types of report:

- Report Templates– reports generated using supplied settings (criteria).
- Saved/Scheduled – reports generated using your own saved settings.

PRECONFIGURED TYPES OF REPORT

The preconfigured types of report supplied with Report Central are:

- Trend Reports (Trend Reports on page 79)
- Management Reports:
  - Connection Based (Management Reports – Connection Based on page 79)
  - Traffic Based (Management Reports – Traffic Based on page 80)
- Summary Reports:
  - Inbound Traffic (Summary Reports – Inbound Traffic on page 81)
  - Outbound Traffic (Summary Reports – Outbound Traffic on page 83)
- Comparison Reports (Comparison Reports on page 85)
- Forensic Reports (Forensic Reports on page 86)
- Legacy Reports (Legacy Reports on page 87).

All reports use the **Date/Time** and **Options** criteria. By default, reports are based on all available criteria and data for the last 7 days. For details of available criteria that you can change to create reports, see Specifying Report Criteria on page 90.

All reports contain the Date Range and the date on which the report was run, but the data shown depends on the type of report.

The contents of the reports are detailed in the following sections.

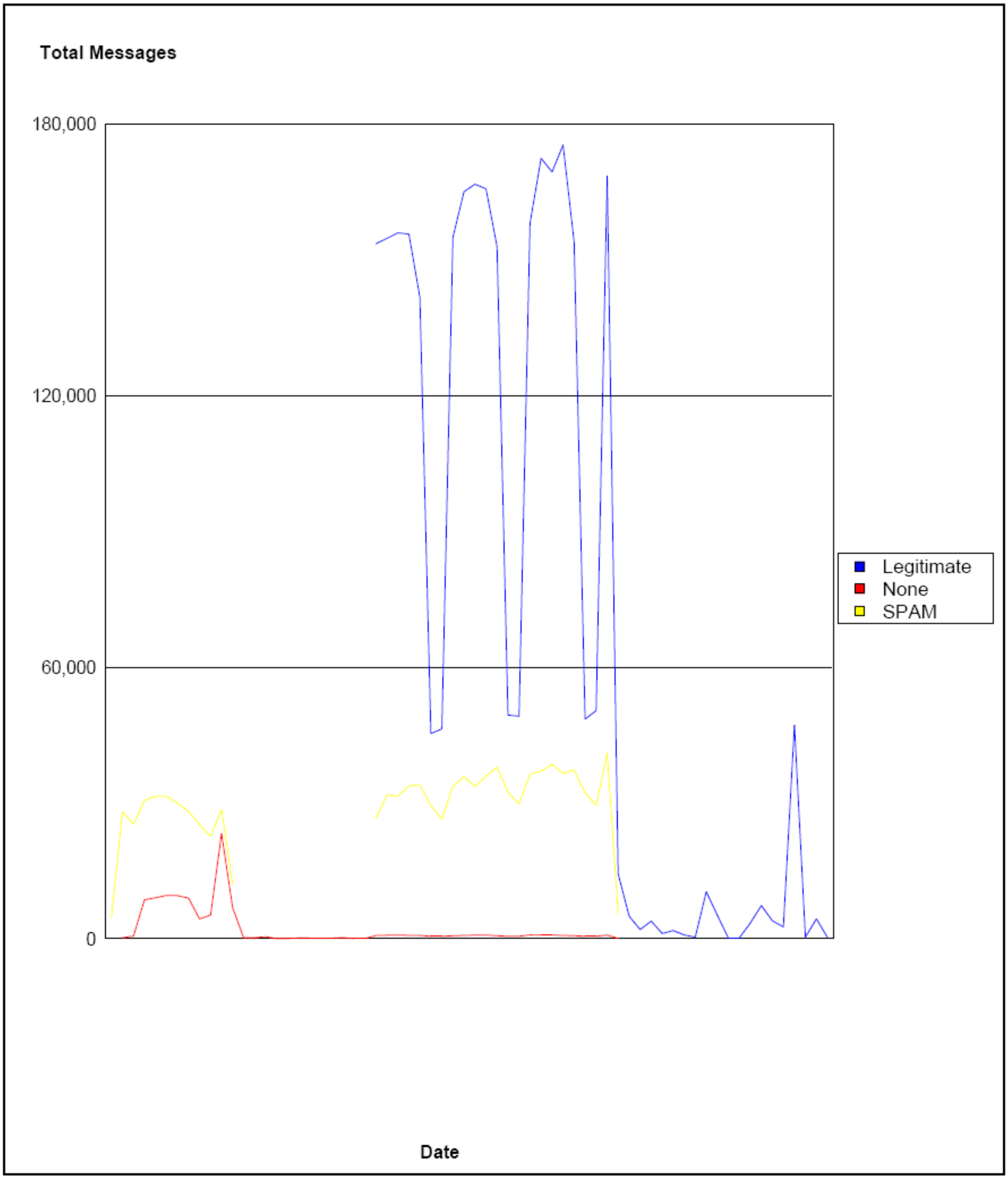
REPORT DISPLAY AND CHART TYPES

Some reports are displayed as a table, but some reports are also displayed as charts. The types of chart available are:

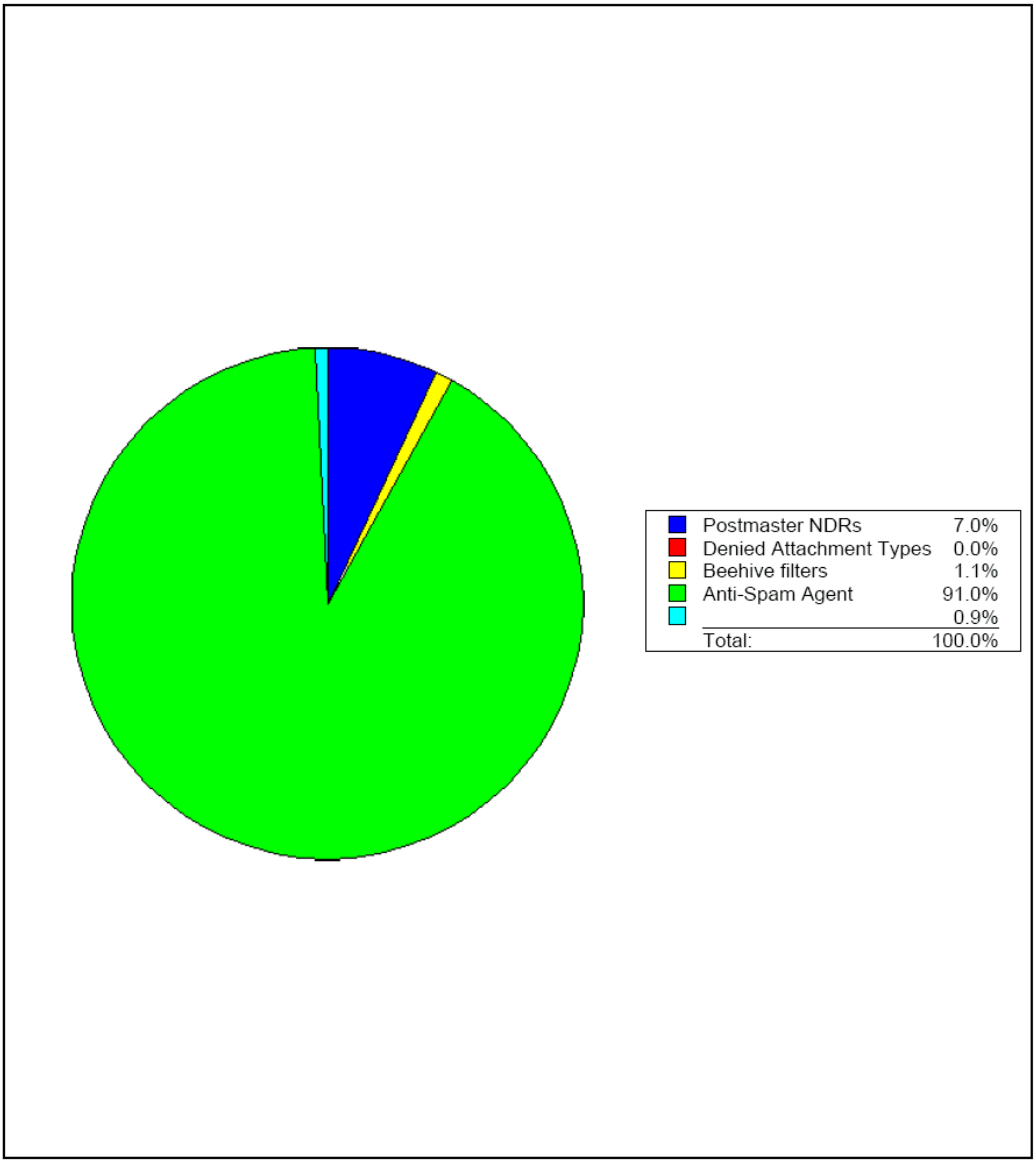
- Line plot
- Pie chart
- Bar chart - horizontal
- Bar chart - horizontal (split)

The following sections detail the types of chart available.

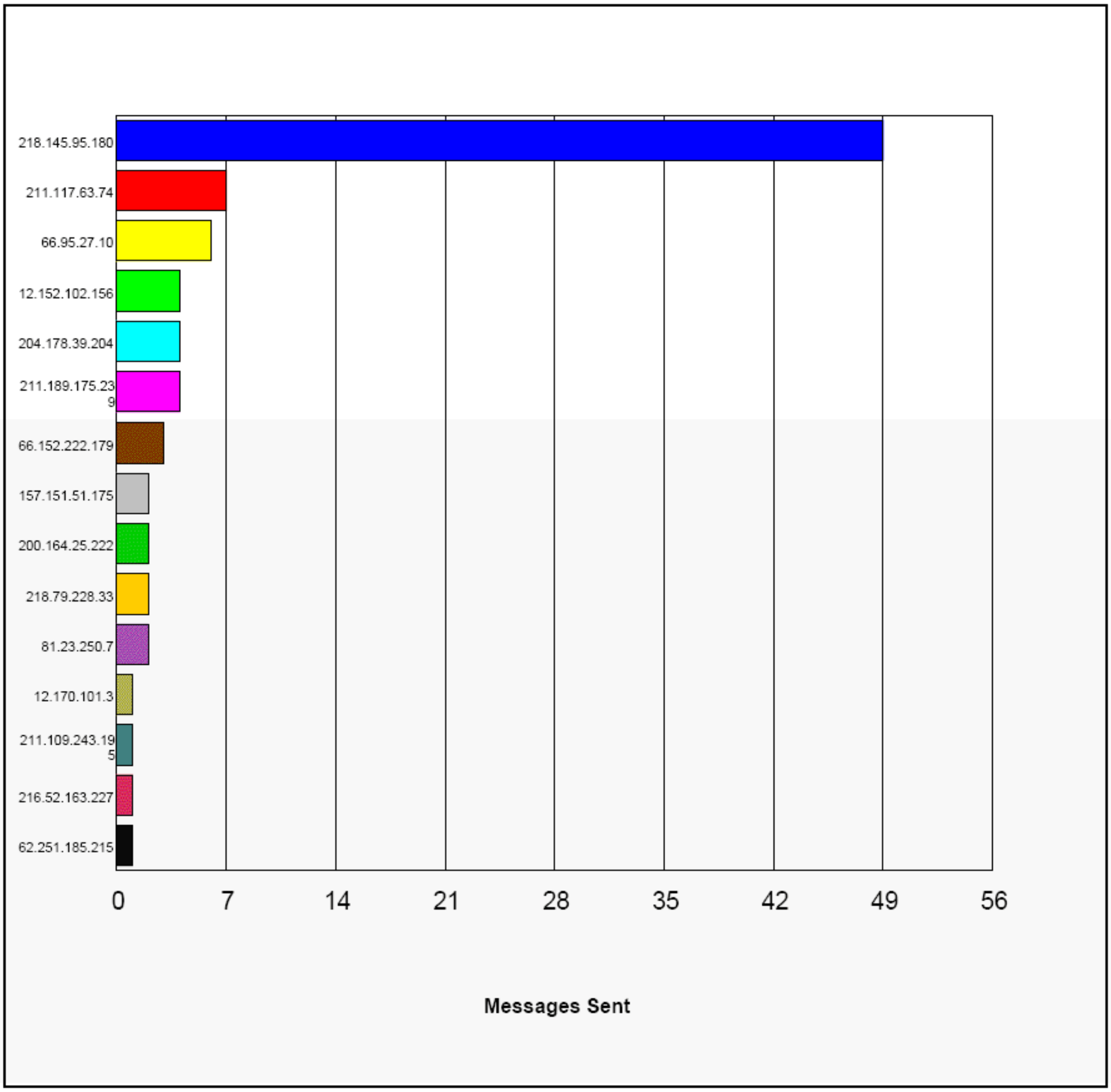
Line Plot



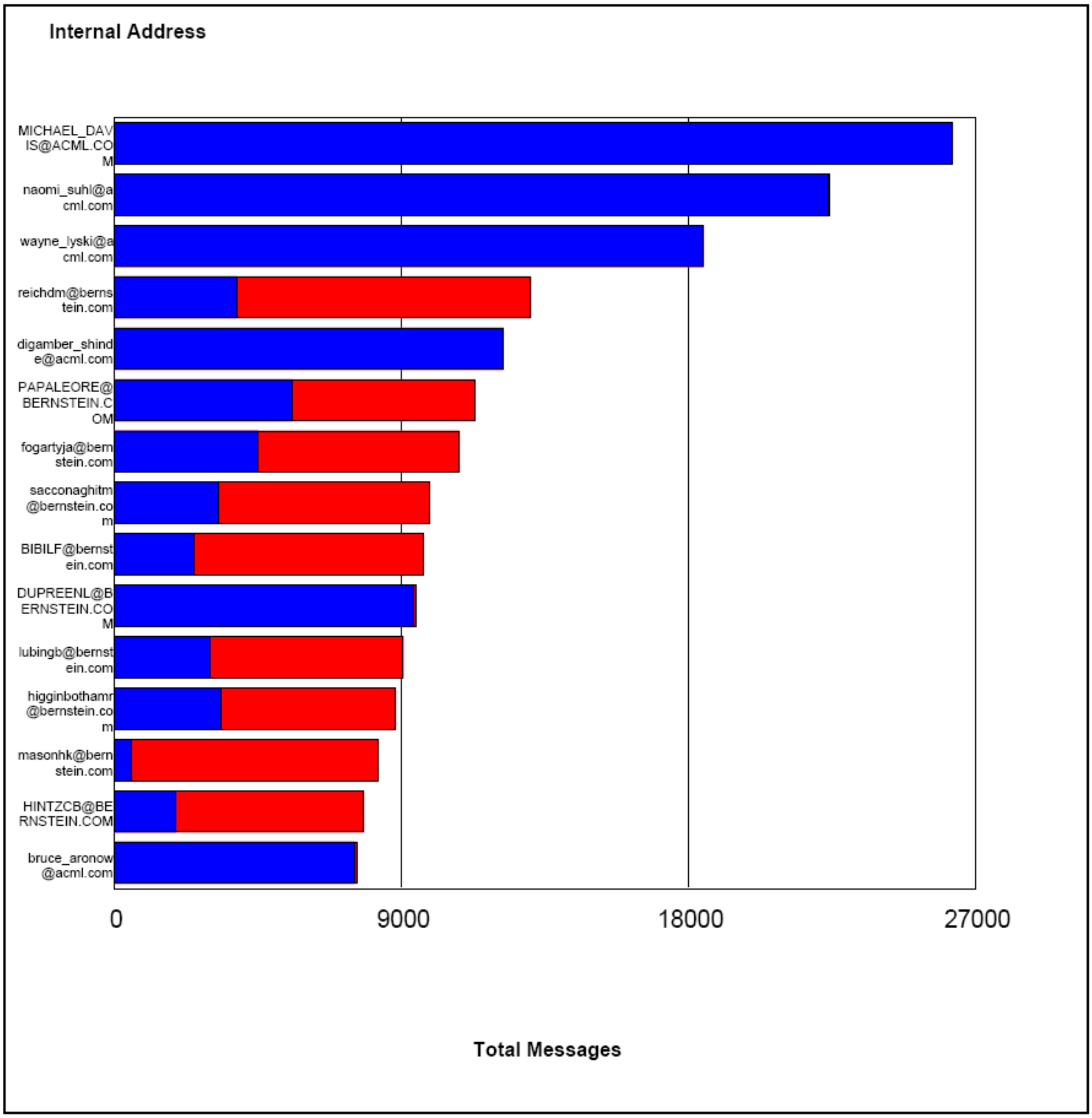
Pie Chart


Postmaster NDRs 7.0%
Denied Attachment Types 0.0%
Beehive filters 1.1%
Anti-Spam Agent 91.0%
0.9%
Total: 100.0%

Bar chart – horizontal



Bar chart – horizontal (split)



TREND REPORTS

The following table describes the content of Trend reports. All reports use Date/Time and Options criteria.

Table 5-1 Trend reports

Report name	Type	Data shown in report	Report criteria used
Connections by Type – Trend	Line plot & Pie chart	• Date/Time • Connection Type • Total Connections	
Messages by Type – Trend	Line plot & Pie chart	• Date/Time • Total Messages • No. of Connections	• Protected Domain

MANAGEMENT REPORTS – CONNECTION BASED

The following table describes the content of connection-based Management reports. All reports use Date/Time and Options criteria..

Table 5-2 Management reports – connection based

Report name	Type	Data shown in report	Report criteria used
Connections by Type – Summary	Pie chart	• Connection Type • Total Connections	• Connection Type • IP Address
Top 15 Connections	Bar chart - horizontal	• IP Address • Accepted Connections	• Connection Type • IP Address
Top N Connections by Type	Table	• Connection Type • IP Address • Total Connections	• Connection Type • IP Address

MANAGEMENT REPORTS – TRAFFIC BASED

The following table describes the content of traffic-based Management reports. All reports use Date/Time and Options criteria.

* An entry of Manual in this column indicates that a manual action on the e-mail, such as Release, has been carried out in E-mail Filter Message Administrator or Personal E-mail Manager. For more information, please see the Administrator's Guide for each of these products.

Table 5-3 Management reports – traffic based

Report name	Type	Data shown in report	Report criteria used
Message Traffic by Action	Pie chart	• Date • Message Action* • Total Messages	• Protected Domain • Policy Type
Message Traffic by Type	Pie chart	• Date • Policy Type • Total Messages	• Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type
Top 10 Rules by Percent	Pie chart	• Rule • Total Triggered • Percentage	• Protected Domain
Top N Incoming IPs	Bar chart – horizontal	• Incoming Host IP • Host Name • Number of Messages Sent • Volume	• Protected Domain
Top N Internal Addresses	Bar chart – horizontal (split)	• Address • Inbound • Total Messages	• Protected Domain • Policy Type
Top N Rules Triggered	Bar chart – horizontal	• Rule • Times Triggered	

Summary Reports – Inbound Traffic

The following table describes the content of Summary reports for inbound traffic. All reports use Date/Time and Options criteria.

Table 5-4 Summary reports – inbound traffic

Report name	Type	Data shown in report	Report criteria used
Inbound Message Traffic by Type	Pie chart	• Policy Type • Total Messages	• Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type
Top 10 Rules by Percent Triggered by Received Messages	Bar chart – horizontal	• Rule • Times Triggered • Percentage	• Internal Address • Protected Domain • External Domain • External Address • Day of Week • Rule Name • Policy Type
Top 15 External Senders by Rules Triggered	Bar chart – horizontal (split)	• Rule • Sender • Times Triggered	• Internal Address • IP Address • Protected Domain • External Domain • External Address • Day of Week • Rule Name • Policy Type
Top N External Senders by Total Size	Bar chart – horizontal	• Sender • Total Size (KB)	• Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type
Top N External Senders by Total Volume	Bar chart – horizontal	• Sender • Total Messages	• Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type
(Sheet 1 of 2)			

Table 5-4 Summary reports – inbound traffic (Continued)

Report name	Type	Data shown in report	Report criteria used
Top N Internal Recipients by Total Size	Bar chart – horizontal	• Recipient • Total Size (kb)	• Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type
Top N Internal Recipients by Total Volume	Bar chart – horizontal	• Recipient • Total Messages	• Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type
Top N IPs by Rule	Table	• Incoming Host IP • Host Name • Rule • Times Triggered	• Internal Address • Protected Domain • IP Address • External Domain • External Address • Day of Week • Rule Name • Policy Type
Top N Rules by IPs	Table	• Rule • Incoming Host IP • Host Name • Times Triggered	• Internal Address • Protected Domain • IP Address • External Domain • External Address • Day of Week • Rule Name • Policy Type
Top N Rules Triggered by Received Messages	Bar chart – horizontal	• Rule • Times Triggered	• Internal Address • IP Address • Protected Domain • External Domain • External Address • Day of Week • Rule Name • Policy Type
(Sheet 2 of 2)			

SUMMARY REPORTS – OUTBOUND TRAFFIC

The following table describes the content of Summary reports for outbound traffic. All reports use Date/ Time and Options criteria.

Table 5-5 Summary reports – outbound traffic

Report name	Type	Data shown in report	Report criteria used
Outbound Message Traffic by Type	Pie chart	• Policy Type • Total Messages	• Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type
Top 10 Rules by Percent Triggered by Sent Messages	Bar chart – horizontal	• Rule • Times Triggered • Percent	• Internal Address • IP Address • Protected Domain • External Domain • External Address • Day of Week • Rule Name • Policy Type
Top 15 Internal Senders by Rules Triggered	Bar chart – horizontal (split)	• Internal Sender • Rule • Times Triggered	• Internal Address • IP Address • Protected Domain • External Domain • External Address • Day of Week • Rule Name • Policy Type
Top N External Recipients by Total Size	Bar chart – horizontal	• Recipient • Total Size (KB)	• Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type
(Sheet 1 of 2)			

Table 5-5 Summary reports – outbound traffic (Continued)

Report name	Type	Data shown in report	Report criteria used
Top N External Recipients by Total Volume	Bar chart – horizontal	• Recipient • Total Messages	• Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type
Top N Internal Senders by Total Size	Bar chart – horizontal	• Sender • Total Size (KB)	• Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type
Top N Internal Senders by Total Volume	Bar chart – horizontal	• Sender • Total Messages	• Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type
Top N Rules Triggered by Sent Messages	Bar chart – horizontal	• Rule • Times Triggered	• Internal Address • IP Address • Protected Domain • External Domain • External Address • Day of Week • Rule Name • Policy Type
(Sheet 2 of 2)			

COMPARISON REPORTS

The following table describes the content of Comparison reports. All reports use Date/Time and Options criteria.

Table 5-6 Comparison reports

Report name	Type	Data shown in report	Report criteria used
Message Traffic by Date	Bar chart – horizontal (split)	• Date • Inbound • Total Messages	• Internal Address • Protected Domain • External Domain • External Address • Policy Type
Message Traffic by Hour	Bar chart – horizontal (split)	• Hour • Inbound • Total Messages	• Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type
Message Traffic by Weekday	Bar chart – horizontal (split)	• Day of Week • Inbound • Total Messages	• Internal Address • IP Address • Protected Domain • External Domain • External Address

FORENSIC REPORTS

The following table describes the content of Forensic reports. All reports use Date/Time and Options criteria.

* A blank entry in the Attachments column indicates that SRC could not determine if the e-mail caontained attachements.

Table 5-7 Forensic reports

Report name	Type	Data shown in report	Report criteria used
Message History	Table	• Internal Address • Date/Time • Direction • External Address • Subject • No. of Attachments * • Rule Triggered	• Internal Address • Protected Domain • External Domain • External Address • Rule Name • Direction • Policy Type
Messages by Size	Table	• Message Size • Sender • Date/Time	• Internal Address • Protected Domain • External Domain • External Address • Rule Name • Direction • Policy Type
Rules by Date	Table	• Rule • Date • Sender • Recipient • Subject	• Internal Address • Protected Domain • External Domain • External Address • Rule Name • Direction • Policy Type
Rules by Sender – Details	Table	• Sender • Rule • Date/Time • Action • Recipient	• Internal Address • Protected Domain • External Domain • External Address • Rule Name • Direction • Policy Type
(Sheet 1 of 2)			

Table 5-7 Forensic reports (Continued)

Report name	Type	Data shown in report	Report criteria used
Rules by Sender – Summary	Table	• Sender • Rule • Total Messages • Total Size (kb)	• Internal Address • Protected Domain • External Domain • External Address • Rule Name • Direction • Policy Type
Rules by Sender Showing Recipient	Table	• Sender • Rule • Date • Recipient • Subject	• Internal Address • Protected Domain • External Domain • External Address • Rule Name • Direction • Policy Type
(Sheet 2 of 2)			

LEGACY REPORTS

The following table describes the content of Legacy reports. All reports use Date/Time and Options criteria.

Table 5-8 Legacy reports

Report name	Type	Data shown in report	Report criteria used
Top 10 Rules by Percent	Bar chart - horizontal	• Rule • Total Triggered • Percentage	• Internal Address • Protected Domain • External Domain • External Address • Day of Week
Top 15 Recipients by Total Messages	Bar chart - horizontal	• Recipient • Total Messages	• Internal Address • Protected Domain • External Domain • External Address • Day of Week
(Sheet 1 of 2)			

Table 5-8 Legacy reports (Continued)

Report name	Type	Data shown in report	Report criteria used
Top 15 Recipients by Total Size	Bar chart - horizontal	• Recipient • Total Size	• Internal Address • Protected Domain • External Domain • External Address • Day of Week
Top 15 Rules	Bar chart - horizontal	• Rule • Total Messages	• Internal Address • Protected Domain • External Domain • External Address • Day of Week
Top 15 Senders by Percent	Bar chart - horizontal	• Sender • Total Messages • Percent	• Internal Address • Protected Domain • External Domain • External Address • Day of Week
Top 15 Senders by Rules Triggered	Bar chart - horizontal	• Sender • Rule • No. of Times Triggered	• Internal Address • Protected Domain • External Domain • External Address • Day of Week
Top 15 Senders by Total Messages	Bar chart - horizontal	• Sender • Total Messages	• Internal Address • Protected Domain • External Domain • External Address • Day of Week
Top 15 Senders by Total Size	Bar chart - horizontal	• Sender • Total Size	• Internal Address • Protected Domain • External Domain • External Address • Day of Week
Top N Incoming IPs	Bar chart - horizontal	• IP Address • Total Messages	• Internal Address • Protected Domain • External Domain • External Address • Day of Week
(Sheet 2 of 2)			

SETTING UP REPORTS

There are a maximum of four stages to setting up a report:

1 Selecting the report to run.
2 Specifying report criteria.
3 Specifying running options.
4 Specifying scheduling options.

SELECTING A REPORT

From the Report Manager options, select a report from one of the categories. The criteria for that report is displayed in the right-hand pane.

Note: The time and date on the computer where Report Central is installed must be the same as the SQL Server. If these do not match, the time and date may not be reported accurately.

When you select a report, SurfControl Report Central retrieves the time and date information from the database. If there is a problem connecting to your database you will receive an error message detailing the problem.

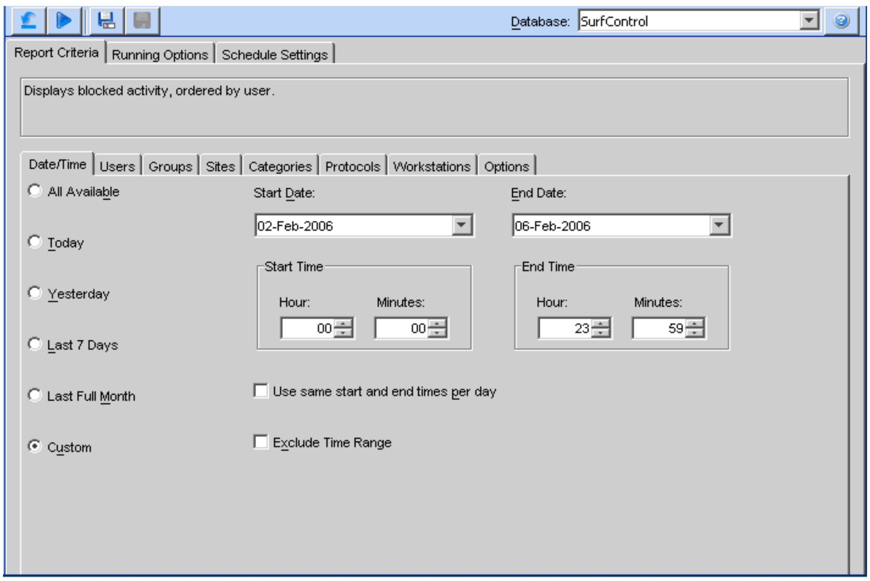
You should check that:

- Report Central is connecting to a valid database (**Configuration > Database Connections**).
- The database that Report Central is connecting to contains valid data.
- the SQL Server is running correctly (**SQL Service Manager**).

SPECIFYING REPORT CRITERIA

The options in the Report Criteria page enable you to select the date and time period for your report, and various other details. For example, you can inlcude or exclude specific IP addresses or domains. The tabs available in this page depend on the type of report and your user permissions. Figure 5-1 shows a typical Report Criteria page.

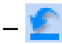
Figure 5-1 Report Criteria



The tabs are:

- Date/Time – Available for all reports. See page 91.
- Options – Available for all reports. See page 92.
- Connection Type – Available only for connection-based Management reports. See page 93.
- IP Address – See page 94.
- Protected Domain – See page 95.
- External Domain – See page 96.
- Policy Type – See page 97.
- Internal Address – See page 98.
- External Address – See page 99.
- Day of Week – See page 100.
- Rule Name – Available only for Forensic and some Summary reports. See page 101.
- Direction – Available only for Forensic reports. See page 102.

You can also use the following options from this screen before you generate a report:

- Revert to the last saved, or the default, report settings – 
- Save the settings to a different report name – 
- Save to replace the default settings (only available for saved reports) – 

For details of the save options, see Saving Reports on page 107. If you do not use any of the save options, the new settings are discarded when you log out of Report Central.

Date/Time

Table 5-9 shows the Date/Time criteria.

Table 5-9 Time/Date criteria

Time/Date	Description
All Available	All available data stored on the database.
Today	All data logged to the database today.
Yesterday	All data logged to the database yesterday (between 00hrs and 24hrs).
Last 7 Days	all data logged to the database in the last seven days, (the default setting).
Last full month	All data logged to the database in the last full month.
Custom	All data logged to the database in the time period you specify. See Procedure 5-1.

Specifying a Custom Time Period for Reports. Use this option to report on data from a time period that you specify (Procedure 5-1).

Procedure 5-1 Specifying a custom time period for reports

Step	Action
1	Select a **Start Date** by clicking the drop-down list box and selecting a day from the calendar. **Note:** Dates marked with a red cross are not available for selection.
2	Select an **End Date** by clicking the drop-down list box and selecting a day from the calendar. **Note:** Dates marked with a red cross are not available for selection.
3	Specify a **Start Time** (in 24 hr clock).
4	Specify an **End Time** (in 24 hr clock).

(Sheet 1 of 2)

Procedure 5-1 Specifying a custom time period for reports (Continued)

Step	Action
5	To report on data from the same time period each day, select **Use same start and end times each day.** See Table 5-10 for an explanation of this feature.
6	To report on data from outside the time period you specify, select **Exclude Time Range.** See Table 5-11 for an explanation of this feature.
(Sheet 2 of 2)	

Use Same Start and End Times Each Day. Use this option to report on data from the same time frame each day.

Table 5-10 Use same start and end times each day check box

Checkbox	What happens	Example
Cleared	The report uses data from the entire date range you specify, beginning at the start time on the start date and ending at the end time on the end date.	Between 9am on day 1 and 5pm on day 3.
Selected	SurfControl Report Central uses report data from the time period you specify, for each day between the start and end date.	Between 9am and 5pm on day 1, 9am and 5pm on day 2, etc.

Exclude Time Range. You can use the **Exclude Time Range** check box independently of the **Use same start and end times per day** check box.

Table 5-11 Exclude Time Range check box

Checkbox	What happens	Example
Cleared	The report uses data from the time period you specify.	Between 9am and 5pm on day 1.
Selected	The report uses any data excluded by the Use same start and end times per day options.	Midnight until 9am and 5pm until 11:59pm on day 1.

Options

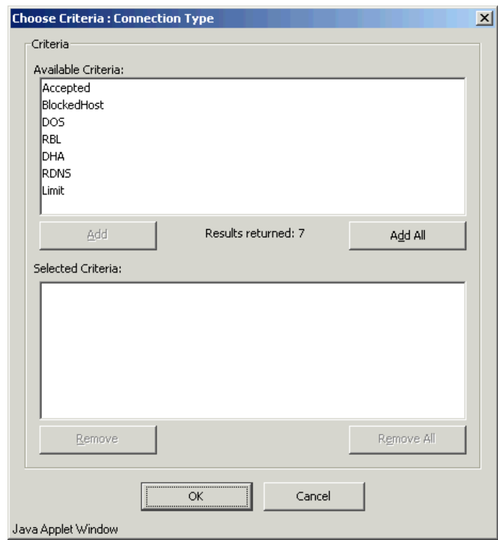
The **Options** tab is only available for certain reports. There are two possible settings:

- **Exclude Postmaster:** – Not available for Trend or Management reports. Use this to specify internal e-mail addresses that are to be excluded from the report. For multiple e-mail addresses, you can only use a comma (,) to separate the addresses.
- **Display Top N Results:** – This is used for reports where you want to specify a number of results, such as, Top N IPs by Rule, Top N Rules Triggered, and so on. Default N = 15.

Connection Type

Use this tab to include or exclude types of connection, such as Accepted, Blocked Host, RBL, RDNS, and so on.

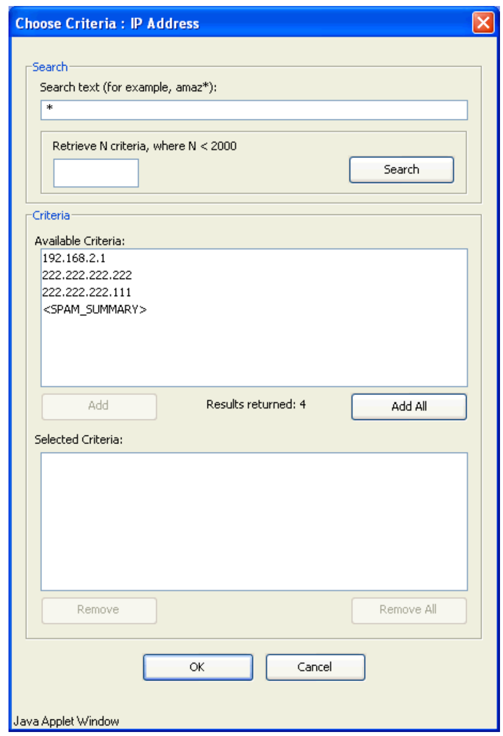
Procedure 5-2 Specifying types of connection in a report

Step	Action
1	Select the **Connection Type** tab.
2	To include all types of connection in the report, select **Include all**. To include or exclude specific types of connection, select either: • **Include selected items**, or • **Exclude selected items**. A Choose Criteria: Connection Type dialog box is displayed. **Note:** If there are already connection types in the **Selected Criteria:** list on the **Connection Type** tab, you need to click **Add** to display the **Choose Criteria:** dialog box. 
3	Select connection types from the **Available Criteria:** list. To select multiple connection types, use Ctrl or Shift. Click **Add**. To select all connection types, click **Add All**. The selected connection types are displayed in the **Selected Criteria:** list. To remove one or more connection types from the **Selected Criteria:** list, select the connection types, and then click **Remove**. To remove all connection types from the list, click **Remove All**. **Note:** Restricted users cannot change the criteria for connection types.
4	Click **OK**. The connection types are added to the **Selected Criteria:** list in the **Connection Type** tab.

IP Address

Use this tab to include or exclude IP addresses.

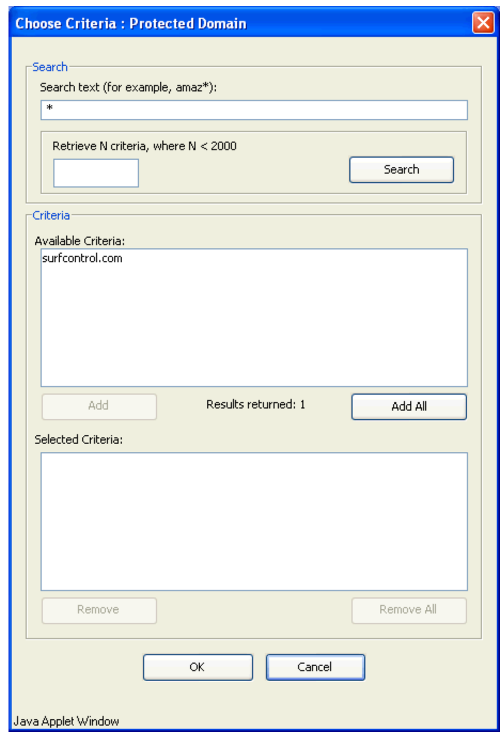
Procedure 5-3 Specifying IP addresses in a report

Step	Action
1	Select the **IP Address** tab.
2	To include all IP addresses in the report, select **Include all**. To include or exclude specific IP addresses, select either: • **Include selected items**, or • **Exclude selected items**. A Choose Criteria: IP Addresses dialog box is displayed. **Note:** If there are already IP addresses in the **Selected Criteria:** list on the **IP Address** tab, you need to click **Add** to display the **Choose Criteria:** dialog box. 
3	You have two methods for selecting IP addresses: • Search for IP addresses by entering search text. You can use wildcards. Enter the number of search requests to display (1 to 2000), and then click **Search**. The search results are displayed in the **Available Criteria:** list. Click **Add**. The selected IP addresses are displayed in the **Selected Criteria:** list. **Note:** To increase the maximum number of records returned to greater than 2000, consult Knowledge Base article 1596 from http://kb.surfcontrol.com • Select IP addresses by scrolling through the **Available Criteria:** list. To select multiple IP addresses, use Ctrl or Shift. Click **Add**. To select all IP addresses, click **Add All**. The selected IP addresses are displayed in the **Selected Criteria:** list. To remove one or more IP addresses from the **Selected Criteria:** list, select the IP addresses, and then click **Remove**. To remove all IP addresses from the list, click **Remove All**. **Note:** Restricted users cannot change the criteria for IP addresses.
4	Click **OK**. The IP addresses are added to the **Selected Criteria:** list in the **IP Address** tab.

Protected Domain

Use this tab to include or exclude protected domains.

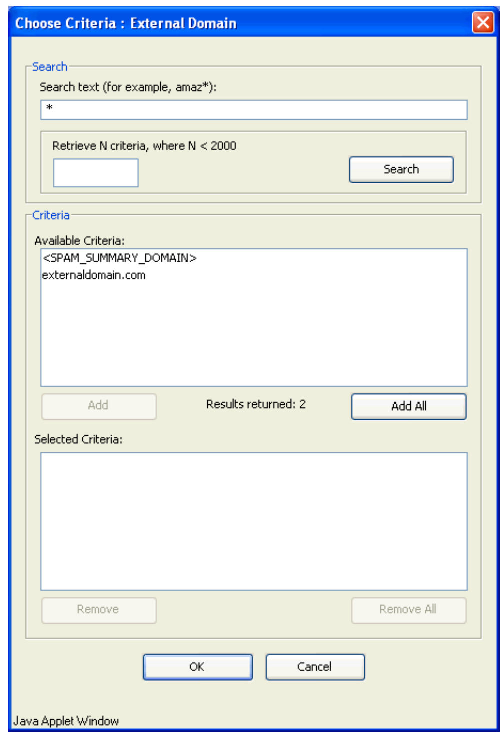
Procedure 5-4 Specifying protected domains in a report

Step	Action
1	Select the **Protected Domain** tab.
2	To include all protected domains in the report, select **Include all**. To include or exclude specific protected domains, select either: • **Include selected items**, or • **Exclude selected items**. A Choose Criteria: Protected Domain dialog box is displayed. **Note:** If there are already protected domains in the **Selected Criteria:** list on the **Protected Domain** tab, you need to click **Add** to display the **Choose Criteria:** dialog box. 
3	You have two methods for selecting protected domains: • Search for protected domains by entering search text. You can use wildcards. Enter the number of search requests to display (1 to 2000), and then click **Search**. The search results are displayed in the **Available Criteria:** list. Click **Add**. The selected protected domains are displayed in the **Selected Criteria:** list. **Note:** To increase the maximum number of records returned to greater than 2000, consult Knowledge Base article 1596 from http://kb.surfcontrol.com • Select protected domains by scrolling through the **Available Criteria:** list. To select multiple protected domains, use Ctrl or Shift. Click **Add**. To select all protected domains, click **Add All**. The selected protected domains are displayed in the **Selected Criteria:** list. To remove one or more protected domains from the **Selected Criteria:** list, select the protected domains, and then click **Remove**. To remove all protected domains from the list, click **Remove All**. **Note:** Restricted users cannot change the criteria for protected domains.
4	Click **OK**. The protected domains are added to the **Selected Criteria:** list in the **Protected Domain** tab.

External Domain

Use this tab to include or exclude external domains.

Procedure 5-5 Specifying external domains in a report

Step	Action
1	Select the **External Domain** tab.
2	To include all external domains in the report, select **Include all**. To include or exclude specific external domains, select either: • **Include selected items**, or • **Exclude selected items**. A Choose Criteria: External Domain dialog box is displayed. **Note:** If there are already external domains in the **Selected Criteria:** list on the **External Domain** tab, you need to click **Add** to display the **Choose Criteria:** dialog box. 
3	You have two methods for selecting external domains: • Search for external domains by entering search text. You can use wildcards. Enter the number of search requests to display (1 to 2000), and then click **Search**. The search results are displayed in the **Available Criteria:** list. Click **Add**. The selected external domains are displayed in the **Selected Criteria:** list. **Note:** To increase the maximum number of records returned to greater than 2000, consult Knowledge Base article 1596 from http://kb.surfcontrol.com • Select external domains by scrolling through the **Available Criteria:** list. To select multiple external domains, use Ctrl or Shift. Click **Add**. To select all external domains, click **Add All**. The selected external domains are displayed in the **Selected Criteria:** list. To remove one or more external domains from the **Selected Criteria:** list, select the external domains, and then click **Remove**. To remove all external domains from the list, click **Remove All**. **Note:** Restricted users cannot change the criteria for external domains.
4	Click **OK**. The external domains are added to the **Selected Criteria:** list in the **External Domain** tab.

Policy Type

Use this tab to include or exclude policy types.

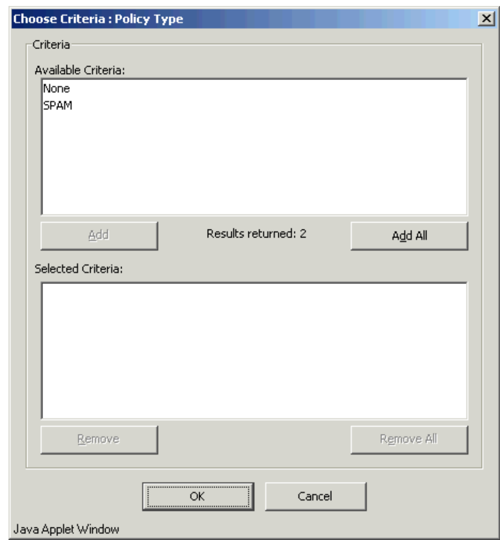
Procedure 5-6 Specifying policy types in a report

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td>1</td><td colspan="2">Select the Policy Type tab.</td></tr>
<tr><td>2</td><td>
To include all policy types in the report, select Include all.

To include or exclude specific types, select either:

- Include selected items, or
- Exclude selected items.

A Choose Criteria: Policy Type dialog box is displayed.

Note: If there are already policy types in the Selected Criteria: list on the Policy Type tab, you need to click Add to display the Choose Criteria: dialog box.
</td><td>


</td></tr>
<tr><td>3</td><td colspan="2">
Select policy types from the Available Criteria: list. To select multiple policy types, use Ctrl or Shift. Click Add. To select all policy types, click Add All. The selected policy types are displayed in the Selected Criteria: list.

To remove one or more policy types from the Selected Criteria: list, select the policy types, and then click Remove. To remove all policy types from the list, click Remove All.

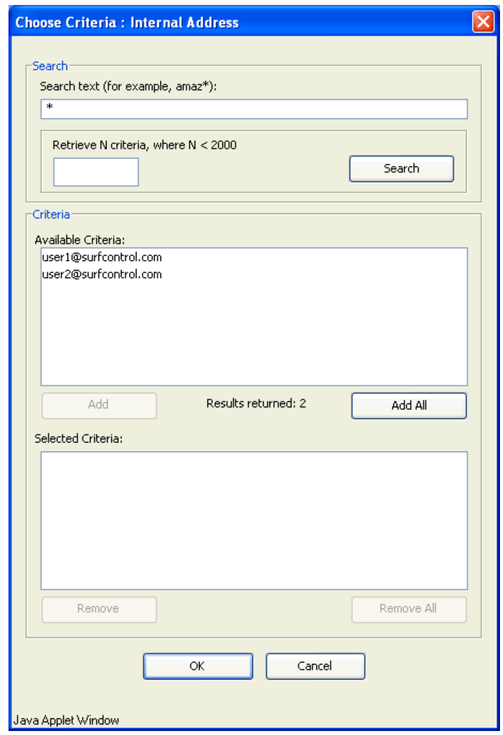
Note: Restricted users cannot change the criteria for policy types.
</td></tr>
<tr><td>4</td><td colspan="2">
Click OK.

The policy types are added to the Selected Criteria: list in the Policy Type tab.
</td></tr>
</table>

Internal Address

Use this tab to include or exclude internal e-mail addresses.

Procedure 5-7 Specifying internal e-mail addresses in a report

Step	Action
1	Select the **Internal Address** tab.
2	To include all internal e-mail addresses in the report, select **Include all**. To include or exclude specific internal e-mail addresses, select either: • **Include selected items**, or • **Exclude selected items**. A Choose Criteria: Internal Address dialog box is displayed. **Note:** If there are already e-mail addresses in the **Selected Criteria:** list on the **Internal Address** tab, you need to click **Add** to display the **Choose Criteria:** dialog box. 
3	You have two methods for selecting internal e-mail addresses: • Search for e-mail addresses by entering search text. You can use wildcards. Enter the number of search requests to display (1 to 2000), and then click **Search**. The search results are displayed in the **Available Criteria:** list. Click **Add**. The selected e-mail addresses are displayed in the **Selected Criteria:** list. **Note:** To increase the maximum number of records returned to greater than 2000, consult Knowledge Base article 1596 from http://kb.surfcontrol.com • Select e-mail addresses by scrolling through the **Available Criteria:** list. To select multiple e-mail addresses, use Ctrl or Shift. Click **Add**. To select all e-mail addresses, click **Add All**. The selected e-mail addresses are displayed in the **Selected Criteria:** list. To remove one or more e-mail addresses from the **Selected Criteria:** list, select the e-mail addresses, and then click **Remove**. To remove all e-mail addresses from the list, click **Remove All**. **Note:** Restricted users cannot change the criteria for internal addresses.
4	Click **OK**. The internal e-mail addresses are added to the **Selected Criteria:** list in the **Internal Address** tab.

External Address

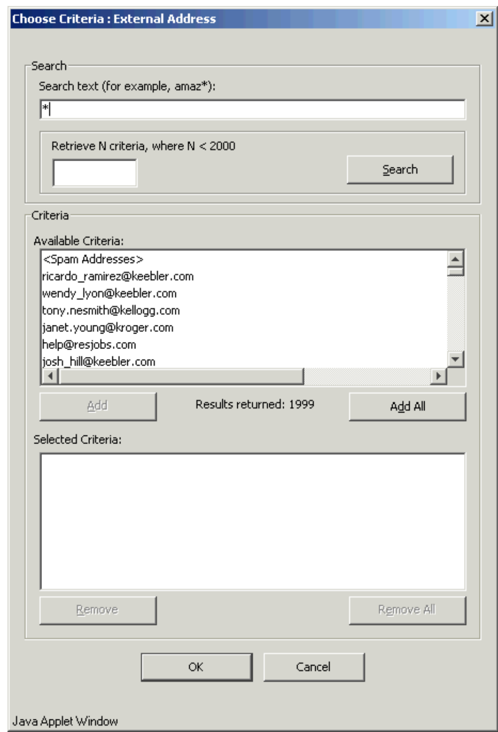
Use this tab to include or exclude external e-mail addresses.

Procedure 5-8 Specifying external e-mail addresses in a report

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td>1</td><td colspan="2">Select the External Address tab.</td></tr>
<tr><td>2</td><td>To include all external e-mail addresses in the report, select Include all.

To include or exclude specific external e-mail addresses, select either:
• Include selected items, or
• Exclude selected items.

A Choose Criteria: External Address dialog box is displayed.

Note: If there are already e-mail addresses in the Selected Criteria: list on the External Address tab, you need to click Add to display the Choose Criteria: dialog box.</td><td>
</td></tr>
<tr><td>3</td><td colspan="2">You have two methods for selecting external e-mail addresses:
• Search for e-mail addresses by entering search text. You can use wildcards. Enter the number of search requests to display (1 to 2000), and then click Search.
The search results are displayed in the Available Criteria: list. Click Add. The selected e-mail addresses are displayed in the Selected Criteria: list.

Note: To increase the maximum number of records returned to greater than 2000, consult Knowledge Base article 1596 from http://kb.surfcontrol.com

• Select e-mail addresses by scrolling through the Available Criteria: list. To select multiple e-mail addresses, use Ctrl or Shift. Click Add. To select all e-mail addresses, click Add All. The selected e-mail addresses are displayed in the Selected Criteria: list.

To remove one or more e-mail addresses from the Selected Criteria: list, select the e-mail addresses, and then click Remove. To remove all e-mail addresses from the list, click Remove All.

Note: Restricted users cannot change the criteria for external addresses.</td></tr>
<tr><td>4</td><td colspan="2">Click OK.

The external e-mail addresses are added to the Selected Criteria: list in the External Address tab.</td></tr>
</table>

Day of Week

Use this tab to include or exclude the day that e-mails have been sent or received.

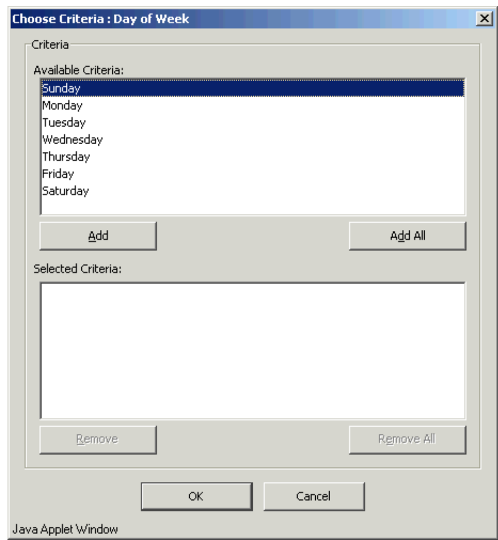
Procedure 5-9 Specifying the day of the week in a report

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td>1</td><td colspan="2">Select the Day of Week tab.</td></tr>
<tr><td>2</td><td>To include all days of the week in the report, select Include all.

To include or exclude days of the week, select either:

• Include selected items, or
• Exclude selected items.

A Choose Criteria: Day of Week dialog box is displayed.

Note: If there are already days of the week in the Selected Criteria: list on the Day of Week tab, you need to click Add to display the Choose Criteria: dialog box.</td><td>
</td></tr>
<tr><td>3</td><td colspan="2">Select the days from the Available Criteria: list. To select multiple days, use Ctrl or Shift. Click Add. To select all days, click Add All. The selected days are displayed in the Selected Criteria: list.

To remove one or more days from the Selected Criteria: list, select the days, and then click Remove. To remove all days from the list, click Remove All.

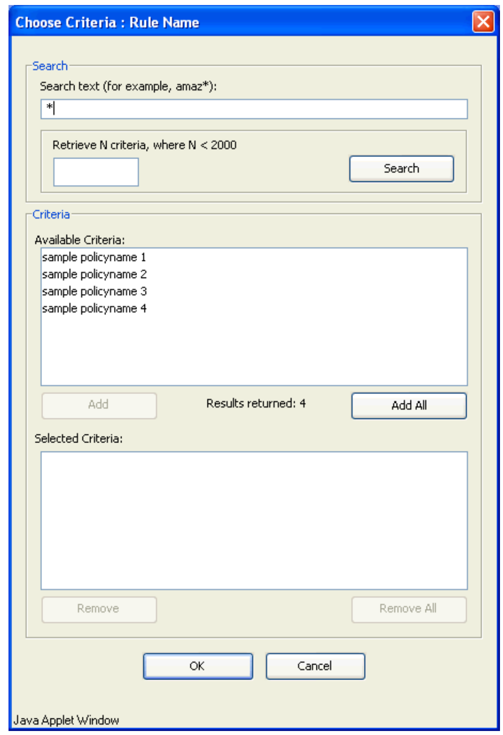
Note: Restricted users cannot change the criteria for days of the week.</td></tr>
<tr><td>4</td><td colspan="2">Click OK.

The days are added to the Selected Criteria: list in the Day of Week tab.</td></tr>
</table>

Rule Name

Use this tab to include or exclude rule names.

Procedure 5-10 Specifying rule names in a report

Step	Action
1	Select the **Rule Name** tab.
2	To include all rule names in the report, select **Include all**. To include or exclude specific rule names, select either: • **Include selected items**, or • **Exclude selected items**. A Choose Criteria: Rule Name dialog box is displayed. **Note:** If there are already rule names in the **Selected Criteria:** list on the **Rule Name** tab, you need to click **Add** to display the **Choose Criteria:** dialog box. 
3	You have two methods for selecting rule names: • Search for rule names by entering search text. You can use wildcards. Enter the number of search requests to display (1 to 2000), and then click **Search**. The search results are displayed in the **Available Criteria:** list. Click **Add**. The selected rule names are displayed in the **Selected Criteria:** list. **Note:** To increase the maximum number of records returned to greater than 2000, consult Knowledge Base article 1596 from http://kb.surfcontrol.com • Select rule names by scrolling through the **Available Criteria:** list. To select multiple rule names, use Ctrl or Shift. Click **Add**. To select all rule names, click **Add All**. The selected rule names are displayed in the **Selected Criteria:** list. To remove one or more rule names from the **Selected Criteria:** list, select the rule names, and then click **Remove**. To remove all rule names from the list, click **Remove All**. **Note:** Restricted users cannot change the criteria for rule names.
4	Click **OK**. The rule names are added to the **Selected Criteria:** list in the **Rule Names** tab.

Direction

This tab is displayed for Forensic reports only. Use this tab to include or exclude the direction of e-mails.

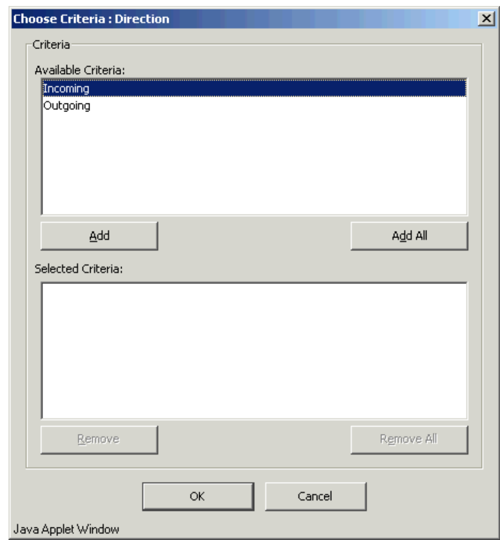
Procedure 5-11 Specifying the direction of e-mails in a report

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td>1</td><td colspan="2">Select the Direction tab.</td></tr>
<tr><td>2</td><td>To include all inbound and outbound e-mails in the report, select Include all.

To include or exclude either inbound, outbound or both directions, select either:
• Include selected items, or
• Exclude selected items.

A Choose Criteria: Direction dialog box is displayed.

Note: If there are already directions in the Selected Criteria: list on the Direction tab, you need to click Add to display the Choose Criteria: dialog box.</td><td>



</td></tr>
<tr><td>3</td><td colspan="2">Select directions from the Available Criteria: list. To select multiple directions, use Ctrl or Shift. Click Add. To select all directions, click Add All. The selected directions are displayed in the Selected Criteria: list.

To remove one or more directions from the Selected Criteria: list, select the directions, and then click Remove. To remove all directions from the list, click Remove All.

Note: Restricted users cannot change the criteria for directions.</td></tr>
<tr><td>4</td><td colspan="2">Click OK.

The directions are added to the Selected Criteria: list in the Direction tab.</td></tr>
</table>

SPECIFYING RUNNING OPTIONS

Use the **Running Options** tab to control how your report is produced and where it is saved.

Display Selected Criteria

You can choose to display the report criteria on the last page. If you choose to do this, the criteria that you have selected will be printed. For example, if you choose to generate a report on Users, the criteria displayed on the report will be of the form:

Selected Users: April, Brian, Mary

Note: If you use the default setting of including all criteria, the selected criteria is not shown, even if you select Display Selected Criteria.

Format

You can generate reports in the following formats in Table 5-12.

Table 5-12 Report formats

Format	Details
.csv	Comma Separated Value – a text format that can be used by spreadsheet and database programs such as Microsoft Excel and Access.
.htm	You can view the report in HTML format using a Web browser.
.pdf	Portable Document Format is the default format. You require a reader such as Adobe Acrobat Reader to view. Adobe Acrobat Reader is available as a free download from www.adobe.com). **Note:** You need version 6 or later of Adobe Acrobat Reader to read reports in this format. **Note:** SurfControl recommends that you use PDF files as attachments to e-mails.
.rtf	Rich Text Format files can be viewed in word processors, such as Microsoft Word.
.xls	Microsoft Excel Format (version 8 or later).

Caution: Pop-up blockers, such as those used by Google, Yahoo! or Microsoft Windows XP SP2, can prevent reports displaying in your browser. You need to alter your settings to allow pop-ups from the Report Central address.

Caution: If using a secure (HTTPS) connection to Report Central, you need to make changes in Internet Explorer to be able to view reports in pdf and rtf format.
In the Tools > Internet Options...> Advanced tab, clear the "Do not save encrypted pages to disk" check box.

Destination Type

You can specify how you want a report to be displayed. If you choose to e-mail a report, note that reports are e-mailed in their native format and will not be compressed. If you are unsure about the size of a report to e-mail, save the report to your machine using the Schedule options. You can then check the size of the report before you send it. Table 5-13 shows the destination type options.

Note: If you create a report and e-mail it in HTML format, some e-mail programs may not preview the report correctly. However, if you open the e-mail, the report will display successfully.

Table 5-13 Destination type options

Option	Details
Show in Browser (default)	Reports in HTML and PDF format will open automatically in a browser window.
Send by e-mail	The report will be sent as an attachment to the e-mail address you specify. You can add multiple recipients by separating the addresses with a semicolon. **Note:** SurfControl recommends that you use PDF files as attachments to e-mails.

Procedure 5-12 describes how to specify running options:

Procedure 5-12 Specifying running options

Step	Action
1	Select the **Running Options** tab.
2	To display the report criteria, select **Display Selected Criteria**.
3	Select a report format from the list.
4	From the **Destination Type** menu, select how you want the report to be displayed.
5	If you have selected to send the report as an e-mail, enter one or more e-mail addresses in the **Receiver's E-mail Address** field. **Note:** SurfControl recommends that you use PDF files as attachments to e-mails.
6	Click **Run** to run the report.

SCHEDULE SETTINGS

You can use the **Schedule Settings** tab to set up reports to run automatically at specific times or dates.

Enabling Report Scheduling

To enable report scheduling, select the **Schedule Report** check box. When you enable report scheduling, two tabs become available:

- Date/Time
- Save Options.

Date/Time

On this tab you can specify the following:

- **Time of Day** - Specify the hour and minute to run a report (using the 24 hr clock).
- **Every** - Specify which days of the week to run a report. You can run reports every day, once a week or on selected days.
- **Monthly** - Specify a day of the month to run a report, or run a report on the last day of the month. If you select the monthly check box, the Daily/Weekly options are unavailable.

Save Options

When the report you have scheduled is generated, you can automatically save it to your hard drive by specifying save options.

Table 5-14 Save Options

Option	Details
Format	You can save the report in the following formats: .csv .htm .pdf - Recommended format for an attachment to an e-mail. .rtf .xls See Format on page 103 for information about each format.
Destination type	Save on Hard drive – The report will be saved to your computer's hard drive. This is useful if you want to check the size of the file before sending it by e-mail.
	Send by e-mail – The report will be sent as an attachment to the e-mail address you specify. **Note:** SurfControl recommends that attachments should be PDF files.

Report History Tab

When a scheduled report has been run, it is displayed in the **Report History** tab in the Report Manager.

If this tab is open when the report is run, the report is not shown in the list. You must click **Update** to see the report in the list.

Generating Reports

When you have set up your criteria, you are ready to save and generate the report, or just generate the report. You can:

- Save the settings to a different report name – 
- Save to replace the default settings (only available for saved reports) – 
- Generate the report – 

Use the **Database:** drop-down list box to select the database from which to run your reports.

For details of the save options, see Saving Reports on page 107. If you do not use any of the save options, the new settings are discarded when you log out of Report Central.

Managing Large Reports

Forensic reports can generate extremely large volumes of data, especially in large organizations with heavy network traffic. SurfControl Report Central limits the amount of information to 20,000 lines (approximately 1000 pages) for each report. If you run reports that exceed this limit, a note is added to the first page of the report.

There are two ways to manage large reports:

- Print the report to file, see Save Options on page 105. You can then view the report without having to print it, or print only selected pages.
- Constrain a scheduled report by limiting the range of data to specific criteria, such as Users or Rules.

SAVING REPORTS

When you have set up your report, you can save a copy to your hard drive. There are two ways to save a report:

- Save the report to a Shared folder.
- Save the report to a Personal folder.

See Configuring User Accounts on page 15 for more information about folders and permissions. Procedure 5-13 on page 107 details how to save a report.

SHARED FOLDER

Any user can view report criteria saved in the Shared folder. Users with the necessary permissions can also change the report criteria.

Note: If you change a report from the Shared folder, use Save As to make sure that you do not overwrite another user's report.

PERSONAL FOLDER

A report saved to the Personal folder can be viewed only by the user who created it.

To save a report:

Procedure 5-13 Saving a report

Step	Action
1	Set up the report using your required criteria and options.
2	Click **Save As**. The **Save Report** dialog box opens.
3	Select the folder in which to save the report.
4	In the **Report Name** field, enter a name for your report.
5	Click **Save**. The **Report History** tab is displayed in the dialog box. This tab displays a list of the reports that have been run according to your schedule. For details of scheduling reports, see Schedule Settings on page 105.

SAVED REPORTS

When you have saved a report to the Shared or Personal folders, a new tab **Report History** is displayed in Report Manager. This tab shows the scheduled reports that have been generated.

Note: Only reports that have been saved using the 'Save on Hard Drive' option are displayed in the Report History tab (see Save Options on page 105). Reports sent by e-mail are not displayed.

CREATING FOLDERS WITHIN SHARED AND PERSONAL FOLDERS

To create folders within the Shared and Personal folders:

1 Select the Shared or Personal folder.

2 Click .

DELETING REPORTS OR FOLDERS FROM SHARED AND PERSONAL FOLDERS

To delete reports or folders from Shared and Personal folders:

1 Select the folder or report within the Shared or Personal folder.

2 Click .

Index

O

P

Q

R