



Internet

**SurfControl Web Filter for
Juniper Networks Security Devices**
Administrators Guide

NOTICES

Updates to the SurfControl documentation and software, as well as Support information are available at www.surfcontrol.com

Copyright ©1998-2005 SurfControl plc. All rights reserved.

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

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

Version 5 printed April 2005.

Notices

TABLE OF CONTENTS

| | |
|-------------------------|-----|
| Notices | i |
| Table of Contents | iii |

WEB FILTER SERVICE

| | |
|--|----|
| Introduction | 2 |
| How to configure the Web Filter Service..... | 2 |
| Service settings | 3 |
| Start/Stop Service tab..... | 4 |
| Advanced tab | 5 |
| E-mail Notification tab | 7 |
| Database tab..... | 8 |
| Real-Time Monitor tab..... | 10 |
| SCFP tab..... | 11 |

REMOTE ADMINISTRATOR

| | |
|--|----|
| Introduction | 14 |
| What The Remote Administrator Does | 14 |
| Prerequisites | 14 |
| Remote Service in a multi-collector environment..... | 15 |
| Remote Service Control Options | 15 |

LICENSING

| | |
|----------------------------|----|
| Licensing Web Filter | 18 |
|----------------------------|----|

DATABASES

| | |
|---------------------------------------|----|
| Database management | 20 |
| Purge | 21 |
| Archive..... | 22 |
| Compact | 23 |
| Delete | 24 |
| Restore | 25 |
| Create a new SQL Server Database..... | 26 |
| Updating your database manually..... | 28 |

PRIVACY EDITION

| | |
|---|----|
| What it does | 32 |
| Comparing the Standard and Privacy Editions | 32 |
| Privacy Edition features | 33 |
| Viewing User Details | 34 |

MONITOR

| | |
|-----------------------------|----|
| Introduction | 36 |
| Opening the Monitor..... | 36 |
| How the Monitor works | 37 |

Table of Contents

| | |
|--|----|
| Privacy Edition Features | 37 |
| Users Panel..... | 37 |
| Sites Panel..... | 39 |
| Right-Click Menus | 40 |
| Submit a site to SurfControl..... | 43 |
| Searching for Users and Sites | 44 |
| Using Groups..... | 45 |
| Monitored Data | 47 |
| Printing the User and Site Panel Information | 54 |
| Changing the Monitor Database | 55 |

REAL TIME MONITOR

| | |
|------------------------|----|
| Introduction | 58 |
| Display Columns | 59 |
| Category Color..... | 60 |
| Collector Details..... | 61 |

RULES ADMINISTRATOR

| | |
|---|----|
| Introduction | 64 |
| Guidelines for rule creation..... | 65 |
| Rule Objects | 66 |
| Who Objects | 67 |
| Creating User Defined Who Objects..... | 69 |
| Where Objects | 72 |
| Creating User Defined Where Objects..... | 73 |
| Category Object..... | 77 |
| Where Lists | 80 |
| When Objects | 81 |
| Allowance Objects | 85 |
| 30 Minute Time Object..... | 85 |
| Notify Objects | 87 |
| HTTP Deny Page Objects | 89 |
| Default | 89 |
| Other HTTP Deny Page objects | 91 |
| Constructing HTTP Deny Pages..... | 91 |
| Changing the Rules Administrator Database | 92 |

SCHEDULER

| | |
|----------------------------|-----|
| Introduction | 94 |
| Available Events | 95 |
| URL Category List..... | 95 |
| Command Line..... | 95 |
| Database Management | 96 |
| Database Update | 99 |
| Network Group Updates..... | 100 |
| Scheduler Options..... | 101 |

VIRTUAL CONTROL AGENT

| | |
|---|-----|
| Introduction | 104 |
| How it Works | 104 |
| Using the VCA | 105 |
| VCA List of Sites tab | 105 |
| VCA Settings tab..... | 107 |
| VCA Results tab..... | 109 |
| The VCA Control Panel application | 111 |

HELP DESK

| | |
|----------------------------------|-----|
| Introduction | 114 |
| How it works | 114 |
| Setting up the Help Desk | 115 |
| Configuring IIS..... | 116 |
| Other Configuration changes..... | 119 |
| Creating a DSN (IIS 5 & 6)..... | 119 |
| Using the Help Desk | 127 |

TROUBLESHOOTING

| | |
|---|-----|
| The Monitor | 130 |
| All Editions | 130 |
| The Monitor does not display traffic | 130 |
| ("\\") Appears in the Users Pane of the Monitor | 132 |
| Databases | 133 |
| Create SQL Database Utility Error Message | 133 |
| Database Tools Fail with MSDE Database | 133 |
| Report Central | 136 |
| Uninstalling the JRE v1.4.2 | 136 |
| VCA | 136 |
| VCA results not shown in the Monitor | 136 |

APPENDIX A

| | |
|--------------------------------|-----|
| Custom Reports | 140 |
| Table details | 141 |
| Categories | 142 |
| Connections | 142 |
| Pages..... | 142 |
| Protocols..... | 144 |
| Protocol_Number..... | 144 |
| Sites | 145 |
| Workstations | 145 |
| Workstation_Groups..... | 147 |
| Workstation_Group_Members..... | 147 |
| WS_Info | 147 |

INDEX

Table of Contents



Chapter 1

Web Filter Service


| | |
|-------------------------|---------|
| Introduction | page 2 |
| Service settings | page 3 |
| Start/Stop Service tab | page 4 |
| Advanced tab | page 5 |
| E-mail Notification tab | page 7 |
| Database tab | page 8 |
| Real-Time Monitor tab | page 10 |
| SCFP tab | page 11 |

INTRODUCTION

You can use the Web Filter Service settings to configure how SurfControl Web Filter monitors Internet traffic and actions that it performs when blocking access to sites.

HOW TO CONFIGURE THE WEB FILTER SERVICE

There are two ways of opening the Web Filter Service:

- Right Click on the SurfControl icon in the status area of the task bar .
- Select SurfControl Web Filter from the Control Panel.

SERVICE SETTINGS

To configure the Web Filter Service, open the Web Filter Service Settings dialog box as in Figure 1-1:

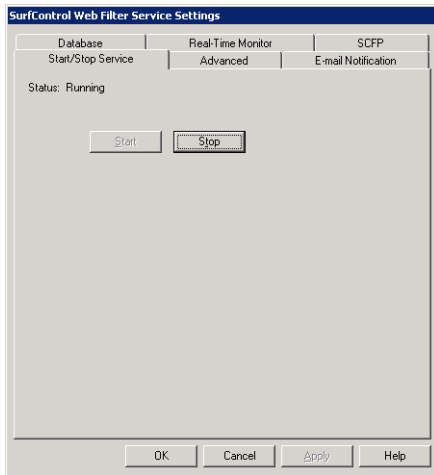


Figure 1-1 Web Filter Service Settings

You can use this dialog box to:

- Start and stop the Web Filter Service.
- Define how users and sites can be viewed in the monitor.
- Define how monitored traffic is transferred to your database.
- Edit the e-mail notifications set up during installation.
- Configure the Real-Time Monitor connection settings.
- Control the connection between Web Filter and the Juniper Networks security device.

START/STOP SERVICE TAB

Applying changes to the Service Settings and the Monitored Data Settings (see “Monitored Data” on page 47 for more details), require that the service be stopped before you can proceed. Figure 1-2 shows the Start/Stop Service tab:

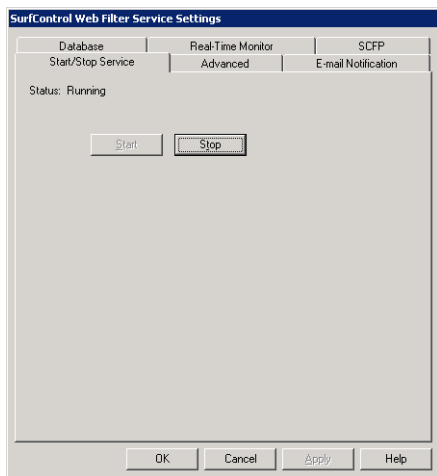


Figure 1-2 Start/Stop Service tab

When you stop the Web Filter Service, the SurfControl icon in the status area of the task bar will be grayed out. When you start the service, the icon will revert back to color.



Note: You can quickly start and stop the service from the SurfControl icon in the status area on the task bar.

ADVANCED TAB

From the Advanced tab you can define the following:

- Monitor to Database Settings
- Categorization Settings
- TCP/IP Name Resolution (DNS)
- Network Settings

Figure 1-3 shows the Advanced tab:

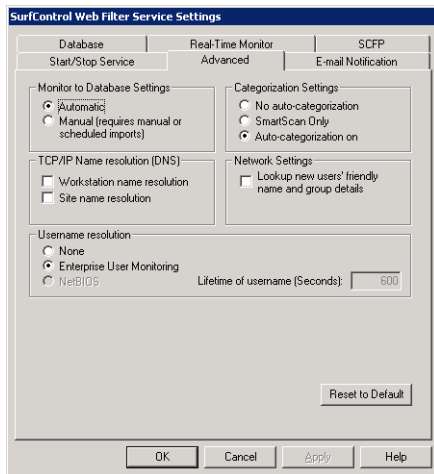


Figure 1-3 Advanced tab

Monitor to Database Settings

By default the Web Filter Service writes data to flat files, which are then updated to the database automatically. The Monitor to Database settings control how the flat files are imported into your database. The options are:

- **Automatic** – (default setting). Flat files are continuously imported into your database as they are created.
- **Manual** – select this option to update the flat files to your database manually. This can be done in the following ways:
 - Use the **Database Updater** tool. See “Updating your database manually” on page 28 for more details.
 - Schedule a database update event in the **Scheduler**. See “Database Update” on page 99 for more details.

SurfControl recommends using a scheduled event for manually updating your database. This avoids you having to remember to perform a manual update and therefore your database is kept up to date.

Categorization Settings

Web sites seen by the Web Filter Monitor are assigned to one of forty five categories in the SurfControl Web Filter URL Category List. You can configure how Web Filter manages categorization on this tab. The options are:

- **No auto-categorization** - this disables all categorization.
- **SmartScan Only** - URLs are categorized against a list of keywords entered in the SmartScan dialog box. See “Category Object” on page 77 for more details.
- **Auto-categorization on** (Default setting) - enables all categorization.

TCP/IP Name Resolution (DNS)

These settings affect how SurfControl Web Filter resolves Domain names:

- **Enable Workstation name resolution** - determines a workstation name based on IP address.
- **Enable Site name resolution** - gives DNS resolution for site names.

SurfControl recommends you leave these settings cleared to increase performance. If you need workstation and site name resolution enabled, you must define the DNS settings on all SurfControl servers. It is critical that DNS requests from those servers do not time out nor take excessive time to respond.

Network Settings

These settings affect how Web Filter reacts to new users and sites not yet categorized.

- **Lookup new users’ friendly name and group details** - if selected, when new users are detected by the Web Filter Monitor, their friendly name and group details are retrieved from the domain controller.

E-MAIL NOTIFICATION TAB

During installation you were asked to give the following information about the Systems Administrator:

- E-mail Server
- Recipient Address
- From Address

You were also asked to select from the following message types that the System Administrator should receive alerts about:

- **Service status changes** - if the Web Filter service is stopped or started.
- **Catch up mode notifications** - if the service becomes overloaded, monitoring will be restricted to HTTP traffic. If the overload becomes critical, monitoring will be temporarily suspended.
- **Scheduled task failures** - if any scheduled task does not complete.
- **URL Category List License reminders** - a reminder will be sent when a subscription to the URL Category List updates is due for renewal within 28 days. Once a list licence has expired a reminder will be sent every 24 hours.

You can edit these settings via the E-mail Notification tab as shown in Figure 1-4:

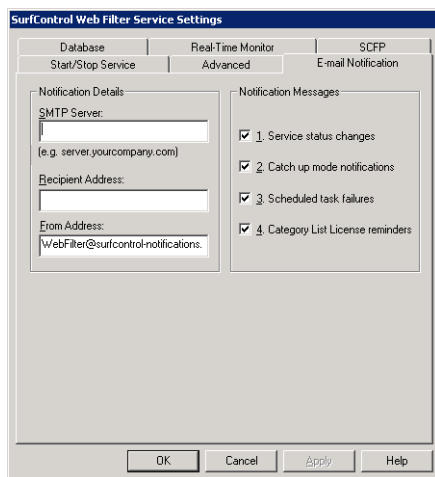


Figure 1-4 E-mail Notification tab

There are three other e-mail alerts that the recipient address will receive:

- Unregistered product reminders. If you are still using an unregistered product past its thirty day trial period, you will be sent daily reminders.
- URL Category List changes by the SurfControl Content team. The Content team may dynamically add new categories to the URL Category List. This e-mail will inform you of any additions that have been made.
- If it is more than a week (seven days) since a URL Category List update.

DATABASE TAB

The Database tab shows the current database being used for Monitoring and Rules in Web Filter. The default database name is SurfControl_WebFilter.

SurfControl recommends you do not have separate databases for Monitoring and Rules.

Figure 1-5 shows the Database tab:

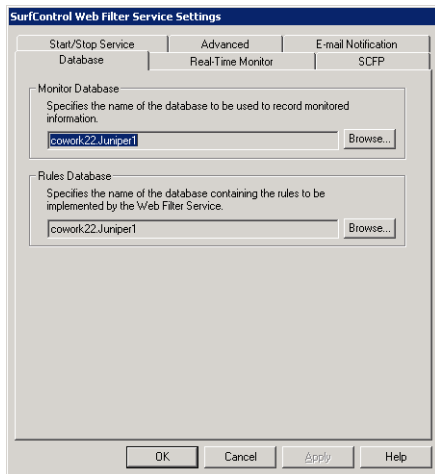


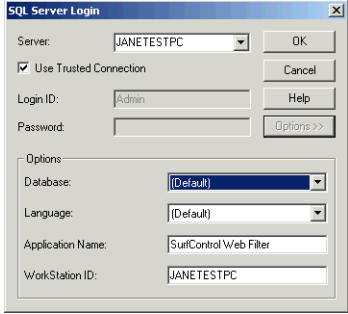


Figure 1-5 Database tab

| Procedure 1-1: Changing the Web Filter Database | | |
|---|--|---|
| Step | Action | |
| 1 | Stop the Web Filter service. Right Click the Web Filter icon  in the status area on the task bar and select Stop Web Filter Service from the SurfControl Web Filter Service Settings dialog box. | |
| 2 | <p>From the Database tab on the Web Filter Service Settings dialog box, click Browse on either the Monitor Database or the Rules Database. A SQL Server Login dialog box appears.</p> <p>The Use Trusted Connection option is selected by default. If you want to use a SQL Server Login ID and Password, clear this option and enter the details in the relevant fields.</p> |  |
| 3 | From the drop-down list box, select the server you want to connect to. The Options button will then be enabled. Click Options to expand the login dialog box. |  |
| 4 | Select the database you want to connect to. | |
| 5 | Add an Application Name to identify the database. Click OK . | |
| 6 | Start the Web Filter Service. | |

REAL-TIME MONITOR TAB

The Real-Time Monitor tab displays the connection details for the Real-Time Monitor. Figure 1-6 shows the Real-Time Monitor tab:

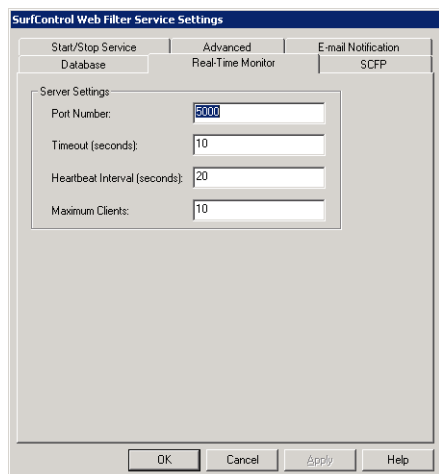


Figure 1-6 Real-Time Monitor Settings

The settings are:

- **Port Number** – this is the port number that the Real-Time Monitor connects to the Web Filter Service on. The default number is 5000. This port number must be the same as in the Collector Details dialog box in the Real-Time Monitor. See page 61 for more details.
- **Timeout (seconds):** – if the connection to the server is lost, this is the time that the Real-Time Monitor will try re-connecting to the server before timing out and reporting an error.
- **Heartbeat Interval (seconds):** – the Web Filter Service will send an ‘I’m here’ message to the Real-Time Monitor. The Real-Time Monitor will then send one back. This setting is the interval between receiving a message and returning it. If no message is received by the Real-Time Monitor it assumes that the connection to the Web Filter Service has stopped.
- **Maximum Clients** – the maximum allowed number of Real-Time Monitor connections to the server at any one time.

SCFP TAB



Warning: Do not change any of these settings unless advised by SurfControl Technical Support.

The SurfControl Content Filtering Protocol (SCFP) tab allows you to configure how Web Filter communicates with your Juniper Networks Security Device.

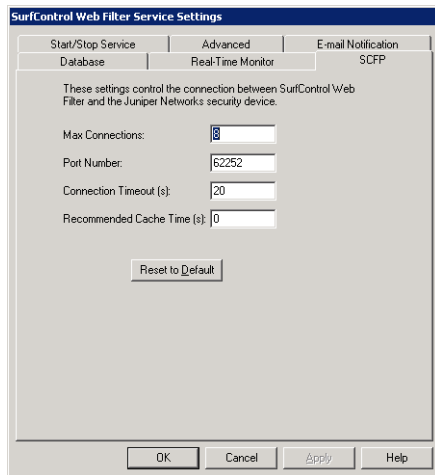


Figure 1-7 SCFP settings

The settings are:



Note: If a Juniper device is reset, you will need to stop and restart the Web Filter service to re-establish all valid connections.

- **Max Connections** - the maximum number of connections to the Web Filter service at any one time. Juniper Networks Security Devices must have eight concurrent connections to operate at maximum efficiency. The default is set at 32, which allows four Juniper Networks Security Devices to be connected. If you wish to connect more than four, this value must be incremented in multiples of eight.
- **Port Number** - the listening SCFP client port number. Default is 62252.
- **Connection Timeout (s)** - the connection timeout between the SCFP service and the Web Filter service in seconds. Default is 20, range is 1 - 60.
- **Recommended Cache Time (s)** - the maximum time the Juniper Networks Security Device caches responses from Web Filter in seconds. Default is 0 (caching is disabled). Maximum is 65535 seconds.

To restore the default settings at anytime, click **Restore to Default**.



WEB FILTER SERVICE *Service settings*



Chapter 2 Remote Administrator

| | |
|---|---------|
| Introduction | page 14 |
| What The Remote Administrator Does | page 14 |
| Prerequisites | page 14 |
| Remote Service in a multi-collector environment | page 15 |
| Remote Service Control Options | page 15 |

INTRODUCTION

The Remote Administrator installation allows you to remotely create reports, design or edit rules, and view the database, without being sat at the SurfControl Web Filter server.

You can install the Web Filter Remote Administrator on any Windows 2000 or 2003 computer in your network. For details on installing the Remote Administrator, see Procedure 8 in the Installation chapter of the *Installation Guide*.

WHAT THE REMOTE ADMINISTRATOR DOES

You can use the Remote Administrator to access the following Web Filter server functions from a different computer:

- **The Monitor** - to view Internet traffic.
- **The Rules Administrator** - to create and edit rules.
- **The Web Filter database** - connect to your database without being at the actual machine.
- **The Real-Time Monitor** - to see your Internet traffic in real time rather than after it has been stored in the Monitor database.

You cannot use the Remote Service to:

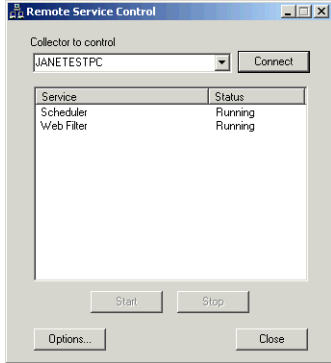
- Configure the Web Filter Service.

PREREQUISITES

For each Computer:

- Install the Remote Administration version of Web Filter. See the Installation chapter of the *Installation Guide* for more details.

Procedure 2-1: Remotely accessing another server

| Step | Action |
|------|--|
| 1 | <p>From any Web Filter computer (remote or server), select Remote Service Control from the Start > Programs > SurfControl Web Filter menu. The Remote Service Control dialog box will appear.</p>  |
| 2 | <p>Add a collector name in the Collector to control drop down list box. This makes it easier for subsequent connections. Up to ten names will be stored in the drop down list box.</p> |
| 3 | <p>Click Connect on a collector name. The available Web Filter Services will appear, showing their current status.</p> |

REMOTE SERVICE IN A MULTI-COLLECTOR ENVIRONMENT

The Remote Service is also useful in a multi collector environment. It allows you to remotely view and manage the service status for the other Web Filter collectors on your network.

REMOTE SERVICE CONTROL OPTIONS

The Remote Service Control constantly checks the status of the available services. You can change the time period (in seconds) between these checks by clicking **Options** from the Remote Service Control dialog box.

The Remote Service Control Options dialog box appears as in Figure 2-1.

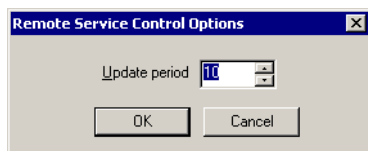


Figure 2-1 Remote Service Control Options

The default setting is 10 seconds.



Chapter 3 Licensing


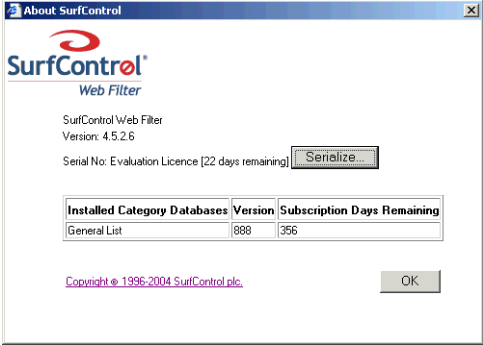
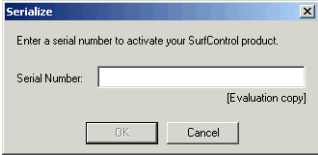
Licensing Web Filter

page 18

LICENSING WEB FILTER

If you have installed SurfControl Web Filter without obtaining a license, you can use the software on a trial basis for 30 days. To continue to use the full functionality of the product past the trial period, including updating the URL Category List you must contact SurfControl to obtain a license appropriate to your business needs. For more details on obtaining a license, visit www.surfcontrol.com

Procedure 3-1: Entering License information

| Step | Action | |
|------|---|--|
| 1 | Obtain a license serial number from SurfControl | |
| 2 | Right-click the SurfControl icon in the status area of the taskbar  . From the menu, select About . The About SurfControl dialog box will appear. |  |
| 3 | Click Serialize . The Serialize dialog box will appear. enter the Serial Number obtained from SurfControl in the field. Click OK . |  |

The next time you view the about dialog box, you will see your serial number and user license details. This dialog box also holds information on the latest URL Category List installed as well as the number of days your subscription has left. When you purchase a license for Web Filter, a one year subscription to URL Category List updates is included. A reminder e-mail will be sent to the Systems Administrator when this subscription is due for renewal. See “E-mail Notification tab” on page 7 for more details.



Chapter 4 Databases

| | |
|----------------------------------|---------|
| Database management | page 20 |
| Purge | page 21 |
| Archive | page 22 |
| Compact | page 23 |
| Delete | page 24 |
| Restore | page 25 |
| Create a new SQL Server Database | page 26 |
| Updating your database manually | page 28 |

DATABASE MANAGEMENT

As SurfControl Web Filter builds up its database of Internet traffic, you need to consider how to manage the volume of data it contains. Web Filter has the following database tools that allow you to manage your data efficiently.

- Purge
- Archive
- Compact
- Delete
- Restore

These tools are all available from the **Start > Programs > SurfControl Web Filter > Database Tools > Database Management** menu.

The following options can also be set up as events in the **Scheduler**:

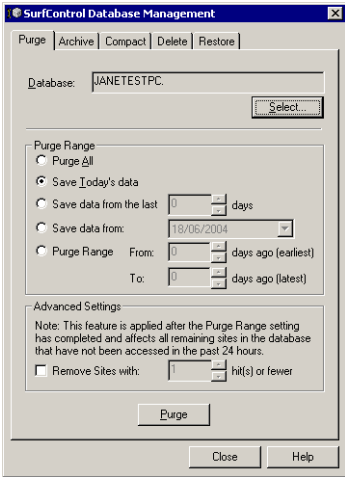
- Purge
- Archive
- Compact

See “Database Management” on page 96 for more details on setting up these tasks in the Scheduler.

PURGE

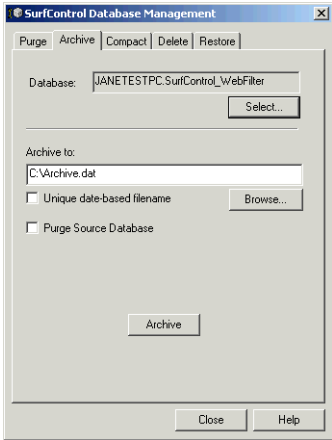
Purging your database reduces its size by removing connection details for users, sites and groups. You can purge your database in various ways from the Purge tab.

Procedure 4-1: Purging a database

| Step | Action |
|------|--|
| 1 | Select Database Management from the Start > Programs > SurfControl Web Filter > Database Tools menu. |
| 2 | <p>Select the Purge tab:</p>  |
| 3 | Click Select to browse to the SQL Server, then click Options to choose the database. |
| 4 | <p>Choose from the following purge options:</p> <ul style="list-style-type: none"> • Purge All, which removes all connection details. • Save Today's data, which removes all but that day's connection details. • Save data from the last "N" days. "N" is the number of days to retain connection details. • Save data from DD/MM/YY, which removes all connections details before the specified date. • Purge Range, which removes all connections for the specified range. • Advanced Settings - you can choose to remove sites not accessed in the last 24hrs, but were outside of the purge range. Select the Remove Sites with: check box and set the number of hits. Sites will be removed that have less than, or equal to, the number of hits specified. The Advanced Settings are not available if you have selected Purge All or Save Today's data. <p>Note: <i>Manually categorized sites that meet the Advanced Settings criteria will not be deleted.</i></p> |
| 5 | Click Purge . |

ARCHIVE

Procedure 4-2: Archiving a database

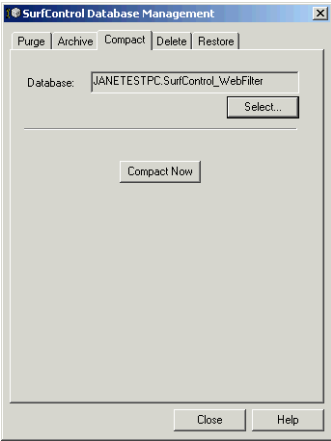
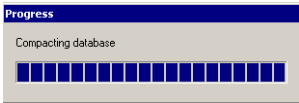
| Step | Action |
|------|--|
| 1 | Stop the Web Filter Service. |
| 2 | Select Database Management from the Start > Programs > SurfControl Web Filter > Database Tools menu. |
| 3 | Select the Archive tab:  |
| 4 | Click Select to browse to the SQL Server and database. |
| 5 | Under Archive To , click Browse and specify a location for the archived database. The default location is C:\ but you may want to specify a different location to prevent the archive file being over-written the next time you archive your database. |
| 6 | Choose from the following archive options: <ul style="list-style-type: none"> • Unique date-based filename - this will also save you over-writing an existing archive file. • Purge Source Database - this will purge all connection details apart from that day's data. |
| 7 | Click Archive . |
| 8 | When the Archive process has finished, start the Web Filter Service. |

If you have left all the options at their default settings, with all check boxes clear, you will archive your whole database to C:\Archive.dat.

COMPACT

Compacting your database eliminates the redundant space contained within it, thus reducing its size.

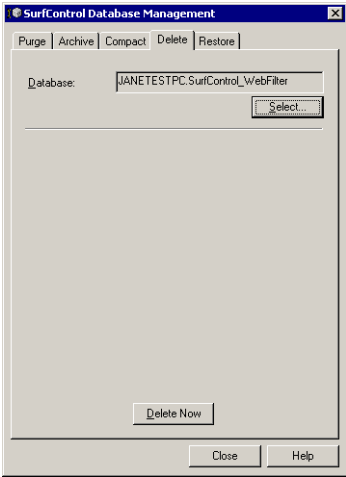
Procedure 4-3: Compacting a database

| Step | Action |
|------|---|
| 1 | Stop the Web Filter Service. |
| 2 | Select Database Management from the Start > Programs > SurfControl Web Filter > Database Tools menu. |
| 3 | Select the Compact tab:  |
| 4 | The current database will be shown in the Database field. If you want to compact another database, click Select to choose another via the SQL Server Login dialog box. |
| 5 | Click Compact Now . A progress dialog box will appear:  |
| 6 | Click Close once the Progress dialog box closes. |
| 7 | Start the Web Filter Service. |

DELETE

Use the delete tab to permanently delete a database from your system.

Procedure 4-4: Deleting a database

| Step | Action |
|------|--|
| 1 | Select Database Management from the Start > Programs > SurfControl Web Filter > Database Tools menu. |
| 2 | Select the Delete tab:  |
| 3 | The current database will be shown in the database field. If you want to delete another database, click Select to choose another via the SQL Server Login dialog box. |
| 4 | Click Delete Now . |

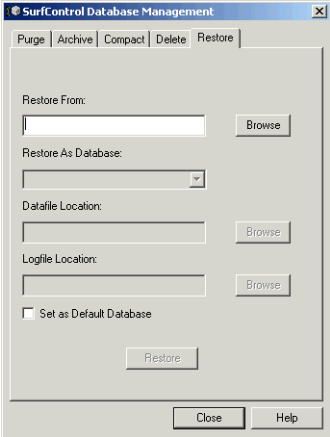
RESTORE

Restore allows you to view and report on an archived database using the SurfControl Web Filter Monitor.



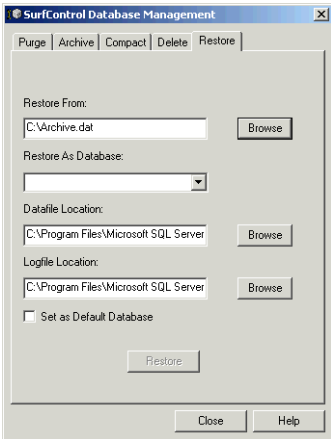
Note: You can only restore local SQL databases.

Procedure 4-5: Restoring an archived database

| Step | Action |
|------|--|
| 1 | Stop the Web Filter Service. |
| 2 | Select Database Management from the Start > Programs > SurfControl Web Filter > Database Tools menu. |
| 3 | <p>Select the Restore tab:</p>  |
| 4 | Click Browse . A Restore from Archive dialog box will appear. The default location for your archived databases is C:\. See "Archive" on page 22 for more details on archiving. If you archived your database to another location, use the dialog box to locate it. Click Open on the relevant file. |

(Sheet 1 of 2)

Procedure 4-5: Restoring an archived database (Continued)

| Step | Action |
|------|--|
| 5 | <p>The Restore tab fields will now be populated with information from the archived database.</p>  |
| 6 | Enter a name in the Restore As Database field. The Restore button becomes enabled. |
| 7 | Select Set as Default Database for the Web Filter service to use the restored database for writing to. |
| 8 | Click Restore . A message appears, confirming the restore has been successful. Click OK . |
| 9 | Start the Web Filter Service. |

(Sheet 2 of 2)

CREATE A NEW SQL SERVER DATABASE

If you wish to create a new SQL Server database for Web Filter, use the SurfControl Database Creation Wizard. Before you can use the Wizard, check the following:

- You must have installed a complete or client version of Web Filter.
- You must have installed Microsoft SQL Server (usually on its own server).
- You must have installed the SQL Server Client Connectivity Pack on the SurfControl server.
- The SurfControl server must have network access to the SQL server.
- There must be a user account on the SQL server that has a “Database Creators” role.



Note: A SurfControl database should only have one database owner.

Procedure 4-6: Create a new SQL Database

| Step | Action |
|------|---|
| 1 | Select Create SQL Server Database from the Start > Programs > SurfControl Web Filter > Database Tools menu. The Create SurfControl Web Filter Database Wizard will start. Click Next . |
| 2 | <ul style="list-style-type: none"> • Enter the name of the SQL server and the proper authentication: <ul style="list-style-type: none"> - For Windows authentication, select Use Trusted Connection. - For SQL authentication, leave Use Trusted Connection de-selected. • Enter the name of the database. • If you deselect Use Default Locations, specify the locations for the database and transaction log files. • Enter the name of the database. • If you deselect Set as SurfControl Web Filter Default, specify the new database for both the Rules and Monitor databases. • Select Populate with sample monitored data if you wish to use the database as a demo. |
| 3 | Click Next . |
| 4 | Click Finish . |

To use the new database in a multiple installation environment you must select the new database from the Web Filter Service. See “Database tab” on page 8 for more details.

UPDATING YOUR DATABASE MANUALLY

There are two methods for manually updating the database from the flat files that are created by the Monitor. You can set up a scheduled event (the recommended method. See “Database Update” on page 99), or you can perform a manual update with the Database Updater tool.



Warning: The Database Updater Tool will not run if the Web Filter Service is running and Monitor to Database is set to Automatic.

Procedure 4-7: Performing a manual database update

| Step | Action | |
|------|---|--|
| 1 | Stop the Web Filter Service. | |
| 2 | Select Database Updater from the Start > Programs > SurfControl Web Filter > Database Tools menu. | |
| 3 | From the Database Updater dialog box, click Add to select a flat file. The default location for flat files is: C:\Program Files\SurfControl\Web Filter\TMP | |
| 4 | Click Open Database . The Select Database dialog box displays, showing the default database. Click OK to update this database or select another Collector or Server and Database from the Drop down list boxes. | |
| 5 | Click Import to update the database. | |
| 6 | You can save the database updater criteria. Click the Save icon . This will save the Flat File location and Database information. You need to specify a name and a location for the update criteria file. | |

Procedure 4-7: Performing a manual database update (Continued)

| Step | Action |
|------|-------------------------------|
| 7 | Start the Web Filter Service. |

4

DATABASES *Database management*



Chapter 5

Privacy Edition

| | |
|---|---------|
| What it does | page 32 |
| Comparing the Standard and Privacy Editions | page 32 |
| Viewing User Details | page 34 |

WHAT IT DOES

In certain European countries, laws have been passed forbidding user browsing details to be seen by monitoring software without express permission from a manager and a union representative. The Privacy Edition of SurfControl Web Filter allows companies in those countries to comply with this legislation.

COMPARING THE STANDARD AND PRIVACY EDITIONS

Tables 1 to 3 outline the differences between Standard Web Filter, and the Privacy Edition of SurfControl Web Filter.

Table 5-1 Changes to the Monitor

| User Menu | Standard Editions | Privacy Edition |
|----------------------------|-------------------|-----------------|
| Rename... | Yes | No |
| Right-Click on a User Menu | Standard Editions | Privacy Edition |
| Get Friendly Name | Yes | No |
| Get User Name | Yes | No |
| View User Detail | No | Yes |
| Configure Menu | Standard Editions | Privacy Edition |
| Change Manager Password | No | Yes |
| Change Union Password | No | Yes |

Table 5-2 Changes to the Real-Time Monitor

| Options Menu | Standard Editions | Privacy Editions |
|-------------------|-------------------|------------------|
| User | Yes | Unavailable |
| Client Name | Yes | Unavailable |
| Client IP Address | Yes | Unavailable |

Table 5-3 Changes to Reports

| Quick Reports | Standard Editions | Privacy Edition |
|-----------------------------------|-------------------|-----------------|
| Top N Workstations by Connections | Yes | No |
| Summary Reports | Standard Editions | Privacy Edition |
| Top N Workstations by Connections | No | Yes |

PRIVACY EDITION FEATURES

Viewing a users' details requires the permission of both a manager and a union representative. The Privacy Edition comes with a preconfigured password for both the manager and union representative of 'admin'. SurfControl recommends that the designated manager and union representative change their password as soon as possible after installation.

Procedure 5-1: Change the Manager/Union password

| Action | Step |
|--------|---|
| 1 | From the Configure menu in the Monitor, select the Change Manager or Change Union Password option |
| 2 | Enter the old password ('admin' for the original password). |
| 3 | Enter a new password. This can be up to 40 characters long and can be alpha, numeric or a combination of both. |
| 4 | Verify the password by re-entering it. |
| 5 | Click OK to set the password. |

VIEWING USER DETAILS

The Web Filter Monitor shows users in the format ‘User X’ as in Figure 5-1:

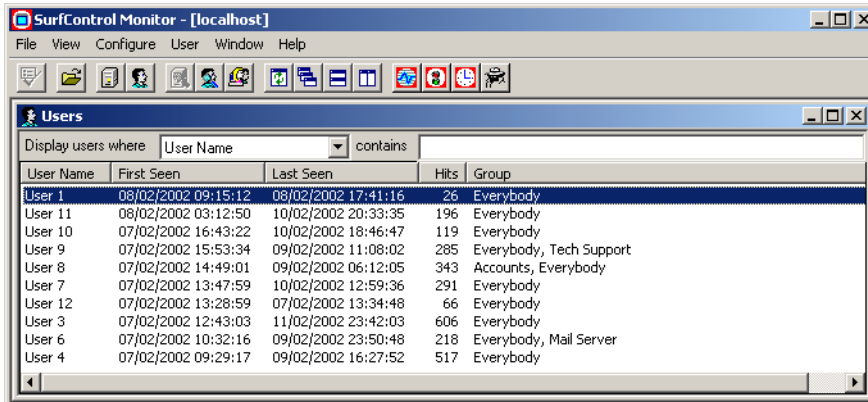


Figure 5-1 Privacy Edition Monitor - Users

| Procedure 5-2: Viewing a Users' Details | | |
|---|--|---|
| Action | Step | |
| 1 | Right-click on a User in the Monitor. | |
| 2 | Choose View User Details from the right-click menu. | |
| 3 | Have the manager enter their password. | |
| 4 | Have the union representative enter their password. | |
| 5 | Click OK . | |
| 6 | <p>The following details are then displayed in a dialog box:</p> <ul style="list-style-type: none"> • User Name • Original Detected Name • IP Address • Ethernet Address | <p>The dialog box titled 'User 7 Details' contains the following information:</p> <ul style="list-style-type: none"> User Name: QACOM1\vim Original Detected Name: QACOM1\vim Workstation Name: timpc.sample.com IP Address: 0.0.0.0 Ethernet Address: ... |
| 7 | Click OK to close the dialog box. | |



Chapter 6 Monitor

| | |
|--|---------|
| Introduction | page 36 |
| Opening the Monitor | page 36 |
| How the Monitor works | page 37 |
| Users Panel | page 37 |
| Sites Panel | page 39 |
| Right-Click Menus | page 40 |
| Submit a site to SurfControl | page 43 |
| Searching for Users and Sites | page 44 |
| Using Groups | page 45 |
| Monitored Data | page 47 |
| Printing the User and Site Panel Information | page 54 |
| Changing the Monitor Database | page 55 |

INTRODUCTION

The SurfControl Web Filter Monitor performs two functions:

- 1 Shows historic Internet activity for your users, as stored in your database. To refresh the connection between the Monitor and the database at any time, press **F5**.
- 2 Helps you determine what future Internet activity will be monitored.

OPENING THE MONITOR

Select **Monitor** from the **Start > Programs > SurfControl Web Filter** menu. From other parts of Web Filter, you can click the  icon. Figure 6-1 shows the Monitor:

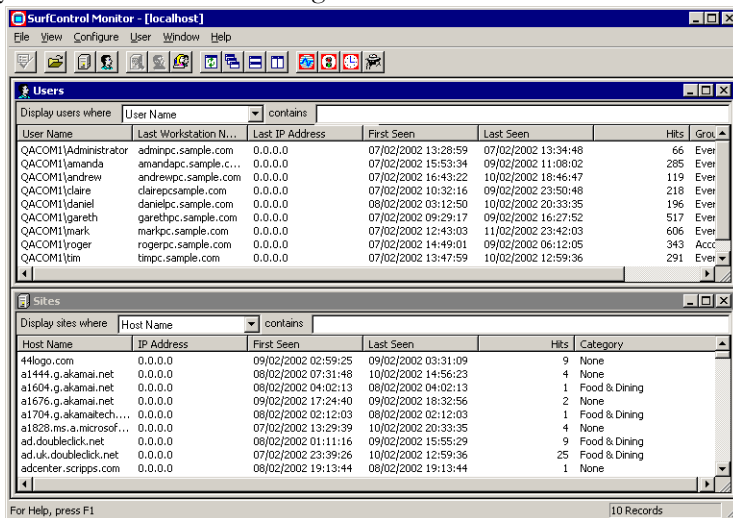



Figure 6-1 Web Filter Monitor

HOW THE MONITOR WORKS

The Monitor shows both Users and Sites in separate panels. You can arrange the panels in a variety of views. Click the Tile Horizontally button  to achieve the view in Figure 6-1.

PRIVACY EDITION FEATURES

This section applies to Web Filter for Juniper Networks Security Devices. See “Comparing the Standard and Privacy Editions” on page 32 for details on the Privacy Edition.

USERS PANEL

The Users panel displays information about the users on your network, that are being monitored by Web Filter. Figure 6-2 shows the Users panel:

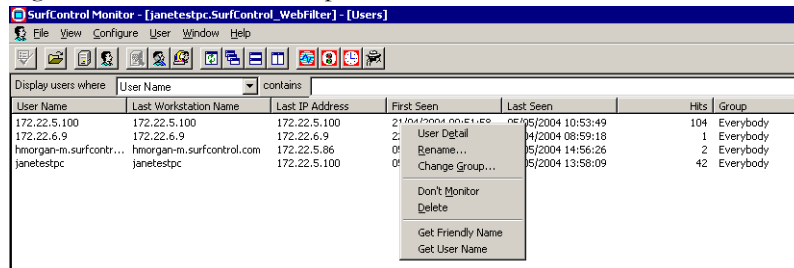


Figure 6-2 Monitor Users Panel

You can view the following Columns in the User Panel.

Table 6-1 User panel columns

| Column | Description |
|------------------------------|---|
| User Name | Identifies the user's name (in the following order of precedence): <ul style="list-style-type: none">• Novell user name• EUM user name• NetBIOS user name• workstation name• IP address |
| Last Workstation name | Identifies the name of last workstation the user was monitored on, if available. Otherwise, contains the IP address. |
| Last IP Address | The last IP address of the workstation the user was monitored on. |
| First Seen | Shows the date and time Web Filter first saw Internet activity from this user. |
| Last Seen | Shows the date and time Web Filter last saw Internet activity from this user. |
| Hits | Shows the total number of TCP (Transmission Control Protocol) transactions a user has received from the Internet. |
| Group | Identifies the group the user is assigned to. By default all users are added to a predefined group of Everybody . |
| Right Click menu | If you right click on a user, a further menu appears. See "Users" on page 40 for more details. |

SITES PANEL

| Host Name | IP Address | First Seen | Last Seen | Hits | Category |
|-------------------------|-----------------|---------------------|---------------------|------|-----------------------------------|
| 207.46.249.157 | 207.46.249.157 | 03/02/2004 13:37:24 | 03/02/2004 13:37:24 | 1 | Computing & Internet |
| 216.251.249.234 | 216.251.249.234 | 22/01/2004 10:11:04 | 10/02/2004 15:20:47 | 16 | None |
| 65.54.249.126 | 65.54.249.126 | 30/01/2004 17:28:55 | 06/02/2004 01:12:55 | 2 | Computing & Internet |
| 65.54.249.190 | 65.54.249.190 | 31/01/2004 15:17:34 | 11/02/2004 07:55:46 | 3 | Computing & Internet |
| 65.54.249.254 | 65.54.249.254 | 15/01/2004 14:19:48 | 06/02/2004 21:17:55 | 4 | Computing & Internet |
| 65.54.249.61 | 65.54.249.61 | 10/02/2004 11:03:42 | 10/02/2004 11:03:42 | 1 | Computing & Internet |
| ads.guardian.co.uk | 212.187.153.203 | 23/01/2004 18:44:59 | 10/02/2004 | | |
| c.microsoft.com | 207.46.197.85 | 13/01/2004 13:33:20 | 10/02/2004 | | Computing & Internet |
| codeventerprise.surf... | 172.22.1.16 | 16/02/2004 15:37:25 | 16/02/2004 | | Don't Monitor |
| mtas.surfcontrol.com | 192.132.210.12 | 10/02/2004 13:31:14 | 10/02/2004 | | Delete |
| news.bbc.co.uk | 212.58.240.144 | 09/02/2004 15:19:17 | 09/02/2004 | | Go to: http://ads.guardian.co.uk/ |
| rtynan:8080 | 172.22.5.9 | 21/01/2004 17:45:00 | 10/02/2004 | | Submit Site |
| time1.cyberpatrol.com | 216.251.249.227 | 07/01/2004 16:35:47 | 10/02/2004 | | Set Category... |
| time2.cyberpatrol.com | 216.251.249.228 | 12/01/2004 11:40:40 | 16/02/2004 | | |
| v4-on.windowupdate... | 207.46.134.126 | 13/02/2004 15:10:19 | 13/02/2004 | | Computing & Internet |
| v4.windowupdate.... | 207.46.134.126 | 15/01/2004 14:07:36 | 26/01/2004 10:40:39 | 27 | Computing & Internet |
| windowupdate.micr... | 207.46.134.24 | 15/01/2004 14:07:44 | 26/01/2004 10:40:02 | 2 | Computing & Internet |
| www.adobe.com | 192.150.19.61 | 26/01/2004 13:40:11 | 10/02/2004 13:49:40 | 6 | Computing & Internet |
| www.bbc.co.uk | 212.58.240.31 | 13/01/2004 13:31:58 | 12/02/2004 15:35:18 | 8 | Arts & Entertainment |
| www.dell.co.uk | 163.244.65.252 | 13/01/2004 13:35:19 | 10/02/2004 13:49:18 | 4 | Computing & Internet |
| www.dell.com | 143.166.224.230 | 13/01/2004 13:36:15 | 13/01/2004 13:36:15 | 1 | Computing & Internet |
| www.football.guardi... | 212.187.153.24 | 13/01/2004 13:32:54 | 10/02/2004 13:47:19 | 7 | Sport |

Figure 6-3 Monitor Sites Panel

You can view the following columns in the Sites panel.

Table 6-2 Sites panel columns

| Column | Description |
|------------------|--|
| Host Name | Identifies the site URL. |
| IP Address | Identifies the site's IP address. |
| First Seen | Shows the date and time Web Filter first saw this site being accessed. |
| Last Seen | Shows the date and time Web Filter last saw this site being accessed. |
| Hits | Identifies the number of times the site has been accessed. |
| Category | Identifies the Category Web Filter has assigned to the site. |
| Right Click menu | If you right click on a site, a further menu appears. See "Sites" on page 42 for more details. |

RIGHT-CLICK MENUS

Both the Users and Sites Panels have right-click menus that are available when an individual user or site is highlighted.

Users

The following right-click menu options are available in the Users panel:

Table 6-3 Users Right-Click Menu

| Menu option | Description |
|-------------------|--|
| User Detail | Displays detailed Internet activity for the user. To view further details on a site a user has visited, either double-click the site, or highlight it and right-click it. This menu is described in Table 2. |
| Rename | Allows you to rename a user in the Web Filter database. In the dialog box that appears, enter a name in the New name text box. The original information about the user is also listed. If you want to reset the user name to the one originally detected, click Reset . Note: <i>if, during a database update, a duplicate name is detected, a modified name insertion will be attempted in the following format: "Friendly Name (domain\some.user)". If this fails a second time, the name is not added.</i> |
| Change Group | See "Using Groups" on page 45 for more details on assigning users to groups. |
| Don't Monitor | Stops monitoring the user and removes their Internet activity data from the SurfControl database. |
| Delete | Removes the user and their Internet activity data permanently from the database. |
| Get Friendly Name | Shows the network name of the user as entered by the system administrator. If the friendly name is unavailable, a pop up will appear. |
| Get User Name | Show the name of the user e.g. domain1\user1 |

If you have installed the Privacy Edition, the following options are unavailable from the right-click menu:

- Rename
- Get Friendly Name
- Get User Name

In addition, the following option will be available in the Privacy Edition only:

View User Detail

User Site Detail

This right-click menu is available after selecting the User Detail menu option and the Detail for User screen appears.

Table 6-4 User Site Detail Menu

| Menu option | Description |
|------------------------|--|
| Site Detail | <p>Opens a new pane showing the following details about the site:</p> <ul style="list-style-type: none"> • User Name • Workstation Name • Activity • Protocol • Category • Allowed/Blocked • Date/Time • Duration * <p>* This column will always display zero in this release.</p> |
| Show all http activity | Shows all activity associated with a site. If not selected, only Web page activity is shown. |
| Go to: Site | Open the selected Web site in a Web browser. |
| Go to: Page | Open the specific Web site page in a Web browser. |
| Category | Manually overrides the SurfControl Category a site or page has been assigned to. |
| Copy URL | Copies the URL into another program such as a Web browser or Notepad. |

Sites

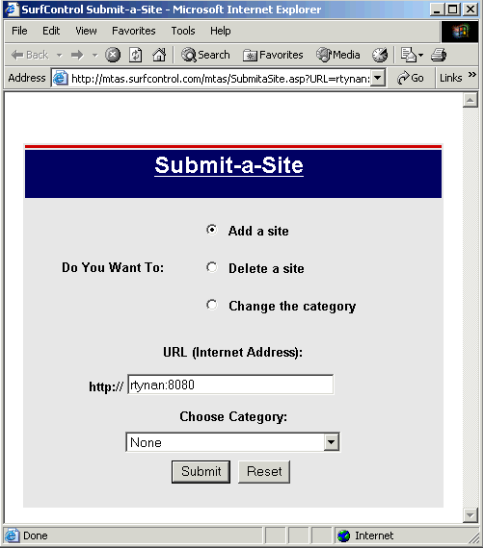
The following right-click menu is available from the Sites panel.

Table 6-5 Sites panel right-click menu

| Menu option | Description |
|------------------|--|
| Site Detail | <p>Opens a new pane showing the following details about the site:</p> <ul style="list-style-type: none"> • User Name • Workstation Name (all workstations the user has used to access the site will be listed) • Activity • Protocol • Category • Action • Date/Time • Duration * • Bytes Sent * • Bytes Received * <p>* These columns will always display zero in this release.</p> |
| Don't Monitor | <p>Stops monitoring the selected site and removes all previous data from the Web Filter database.</p> <p>Note: <i>You must stop the Web Filter Service before selecting this option.</i></p> |
| Delete | <p>Removes the selected site and all previous data from the SurfControl database.</p> <p>Note: <i>You must stop the Web Filter Service before selecting this option.</i></p> |
| Go to http://... | <p>Opens the selected site in a Web browser.</p> |
| Submit Site | <p>If you find traffic to a site with a category of None (and is not an internal site), this option allows you to submit the URL to SurfControl, along with the category you feel the site should belong to. See "Submit a Site to SurfControl" on page 43 for more details.</p> |
| Set Category | <p>This option allows you to block certain Web site pages, without blocking the whole site. From the Set Category dialog box, select the category you want to apply to the page. Click OK. Click Commit to apply the changes to the Web Filter Service.</p> <p>Note: <i>You need to have a rule applied that blocks access to the category chosen for Set Category to become effective.</i></p> |

SUBMIT A SITE TO SURFCONTROL

If you see a site in the Monitor that you feel should be included in our URL Category List, or a site you feel should be categorized differently, you can send details to SurfControl:

| Procedure 6-1: Submit a Site to SurfControl | |
|---|--|
| Step | Action |
| 1 | Highlight the site you wish to submit in the Sites panel of the Monitor. |
| 2 | <p>From the Sites right-click menu, select Submit Site. The Submit-a-Site Web page will be displayed in a browser window:</p>  |
| 3 | From the Choose Category list, select which category you want the site to be added to. |
| 4 | Click Submit . |

SEARCHING FOR USERS AND SITES

In the Users and Sites panels, you can search for users or sites by combining filtering on the column headings and entering search text.

Procedure 6-2: Using the Monitor Search facility

| Step | Action |
|------|---|
| 1 | In either the User or Sites panel, select a column from the Display users (sites) where drop-down list box. |
| 2 | To further refine the search enter some text relevant to the Column selected in the Contains field. Note: <i>You cannot use wildcards in the Contains search field.</i> |
| 3 | The data within the Users or Sites panel is automatically filtered, based on your search criteria. |

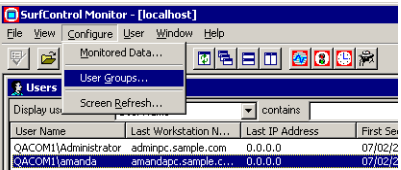

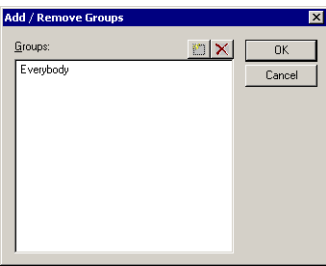
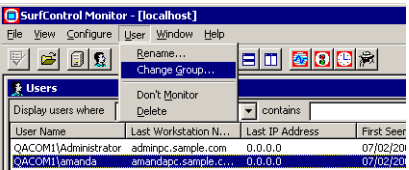
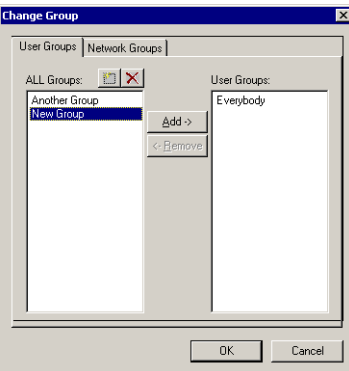
USING GROUPS

User Groups are used to reflect the structure of your organization, i.e. Sales, Accounts, Human Resources, etc.

These groups can then be used by Web Filter when running reports

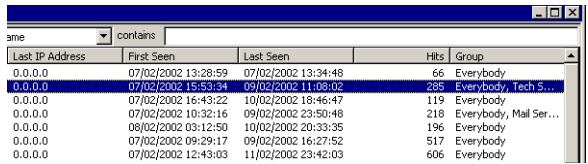
A default group of Everybody is included with Web Filter. All users are added to this group. SurfControl recommends setting up User Groups and then assigning the relevant users to those groups.

Procedure 6-3: Setting up Groups and Assigning Users

| Step | Action | |
|------|---|--|
| 1 | From the Web Filter Monitor, select User Groups... from the Configure menu. |  |
| 2 | The Add / Remove Groups dialog box will appear. The default group of Everybody can be seen in the dialog box. Click Add New Item  . |  |
| 3 | Enter a name for your new group. Click OK . Repeat this for the other groups you wish to set up. | |
| 4 | To assign users to any of the groups you have set up, highlight a user from the Users pane, right click and select Change Group from the menu. The Change Group dialog box will appear. |  |
| 5 | In the right hand pane are the groups the user is already a member of. In the left hand pane is the list of all available groups. Highlight the group in the All Groups pane you want to add the user to and click Add-> . The group will appear in the right hand User Groups pane. Network Groups are described below this procedure. |  |
| 6 | To assign multiple users to a group, highlight them holding down the Shift key for a continuous range or the Ctrl key for non-continuous range of users. | |

(Sheet 1 of 2)

Procedure 6-3: Setting up Groups and Assigning Users (Continued)

| Step | Action | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-----------------|---|---------------------|------------|------------------------|------|-------|---------|---------------------|---------------------|----|-----------|---------|---------------------|---------------------|-----|----------------------|---------|---------------------|---------------------|-----|-----------|---------|---------------------|---------------------|-----|------------------------|---------|---------------------|---------------------|-----|-----------|---------|---------------------|---------------------|-----|-----------|---------|---------------------|---------------------|-----|-----------|
| 7 | <p>In the Monitor Users panel, you will now see the additional groups the user has been assigned to in the Group column.</p>  <table border="1"> <thead> <tr> <th>Last IP Address</th> <th>First Seen</th> <th>Last Seen</th> <th>Hits</th> <th>Group</th> </tr> </thead> <tbody> <tr> <td>0.0.0.0</td> <td>07/02/2002 13:28:59</td> <td>07/02/2002 13:34:48</td> <td>66</td> <td>Everybody</td> </tr> <tr style="background-color: #e6f2ff;"> <td>0.0.0.0</td> <td>07/02/2002 15:53:34</td> <td>09/02/2002 11:08:02</td> <td>285</td> <td>Everybody, Tech 5...</td> </tr> <tr> <td>0.0.0.0</td> <td>07/02/2002 16:43:22</td> <td>10/02/2002 18:46:47</td> <td>119</td> <td>Everybody</td> </tr> <tr> <td>0.0.0.0</td> <td>07/02/2002 10:32:16</td> <td>09/02/2002 23:50:48</td> <td>218</td> <td>Everybody, Mail Ser...</td> </tr> <tr> <td>0.0.0.0</td> <td>08/02/2002 03:12:50</td> <td>10/02/2002 23:33:35</td> <td>196</td> <td>Everybody</td> </tr> <tr> <td>0.0.0.0</td> <td>07/02/2002 09:29:17</td> <td>09/02/2002 16:27:52</td> <td>517</td> <td>Everybody</td> </tr> <tr> <td>0.0.0.0</td> <td>07/02/2002 12:43:03</td> <td>11/02/2002 23:42:03</td> <td>606</td> <td>Everybody</td> </tr> </tbody> </table> | Last IP Address | First Seen | Last Seen | Hits | Group | 0.0.0.0 | 07/02/2002 13:28:59 | 07/02/2002 13:34:48 | 66 | Everybody | 0.0.0.0 | 07/02/2002 15:53:34 | 09/02/2002 11:08:02 | 285 | Everybody, Tech 5... | 0.0.0.0 | 07/02/2002 16:43:22 | 10/02/2002 18:46:47 | 119 | Everybody | 0.0.0.0 | 07/02/2002 10:32:16 | 09/02/2002 23:50:48 | 218 | Everybody, Mail Ser... | 0.0.0.0 | 08/02/2002 03:12:50 | 10/02/2002 23:33:35 | 196 | Everybody | 0.0.0.0 | 07/02/2002 09:29:17 | 09/02/2002 16:27:52 | 517 | Everybody | 0.0.0.0 | 07/02/2002 12:43:03 | 11/02/2002 23:42:03 | 606 | Everybody |
| Last IP Address | First Seen | Last Seen | Hits | Group | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 0.0.0.0 | 07/02/2002 13:28:59 | 07/02/2002 13:34:48 | 66 | Everybody | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 0.0.0.0 | 07/02/2002 15:53:34 | 09/02/2002 11:08:02 | 285 | Everybody, Tech 5... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 0.0.0.0 | 07/02/2002 16:43:22 | 10/02/2002 18:46:47 | 119 | Everybody | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 0.0.0.0 | 07/02/2002 10:32:16 | 09/02/2002 23:50:48 | 218 | Everybody, Mail Ser... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 0.0.0.0 | 08/02/2002 03:12:50 | 10/02/2002 23:33:35 | 196 | Everybody | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 0.0.0.0 | 07/02/2002 09:29:17 | 09/02/2002 16:27:52 | 517 | Everybody | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 0.0.0.0 | 07/02/2002 12:43:03 | 11/02/2002 23:42:03 | 606 | Everybody | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

(Sheet 2 of 2)

Network Groups

The Network Groups tab displays the groups as set up on your domain. You cannot change the Network Group that a user belongs to from this tab. To keep the Network Groups information up to date you need to set up a scheduled event. See “Network Group Updates” on page 100 for more details.

MONITORED DATA

You can configure the Monitor to track specific Internet traffic or users. This can help ease the load on your Web Filter server as well as producing more meaningful reports.



Warning: You must stop the Web Filter Service to apply changes to any of the Monitored Data settings. An error will display if you haven't done this.

From the **Configure** menu select **Monitored Data**. A dialog box as in Figure 6-4 will display.

You can configure the following in the Monitor:

- **Ignored Sites** – you can specify Web sites you don't want to monitor. For example, you may not want to monitor traffic to your internal sites.
- **Protocols** – you can specify which Protocols you want to monitor.
- **Ignored Users** – you can specify users you don't want to monitor.
- **Default Audit Level** – you can specify what type of Internet traffic you want to monitor. Web Filter only monitors Web page traffic by default. You can also create custom audit levels.
- **User Specific Audit Level** – you can specify what type of Internet traffic you want to monitor specific users on. All users are monitored on the Default Audit Level (Web pages), by default.

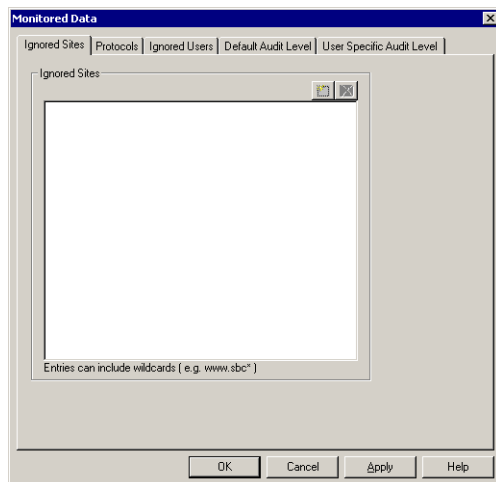



Figure 6-4 Monitored Data dialog box

Procedure 6-4: Ignoring sites in the Monitor

| Step | Action |
|------|---|
| 1 | Stop the Web Filter Service |
| 1 | From the Monitored Data dialog box, select Ignored Sites . |
| 2 | Click Add New Item .  |
| 3 | You can enter the following data: <ul style="list-style-type: none"> • URLs • IP addresses - if sites are being accessed using their IP address as apposed to their URL. <p>Note: <i>when entering IP addresses, do not include the <code>http://</code> prefix. If this is added the site will still be monitored.</i></p> <ul style="list-style-type: none"> • wild card entries. For example <code>*.yourcompany.*</code>. will ignore all your corporate sites. |
| 4 | Click Apply to save the changes. Click OK to close the dialog box. |
| 5 | Start the Web Filter Service. |

To edit an entry, select it and press **F2**.

Monitoring Specific Protocols

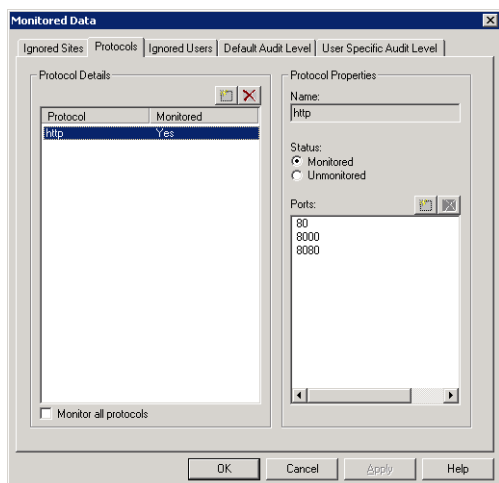



Figure 6-5 Monitored data Protocols tab

The Protocols tab shows the following data:

- Protocol (only HTTP is monitored)
- Monitored Status
- Associated ports for the HTTP protocol.

The following ports are monitored by default:

- 80, 8080, 8000


| Procedure 6-5: Add a new Port | |
|-------------------------------|--|
| Step | Action |
| 1 | Stop the Web Filter Service. |
| 2 | Select the HTTP protocol and from Ports click Add New Item .  . |
| 3 | Enter the new port numbers associated with the HTTP protocol. Note: <i>Port numbers must be between 1 to 65535</i> |
| 4 | Click Apply to save the changes. Click OK to close the dialog box. |
| 5 | Start the Web Filter Service. |

To edit an entry, select it and press **F2**.

Ignoring Users

If you have users whose Internet traffic you don't want to monitor, you can set up a list in the Ignored Users tab. Ignored Users are not excluded from your rules.

Procedure 6-6: Setting up Ignored users

| Step | Action |
|------|---|
| 1 | Stop the Web Filter Service. |
| 2 | From the Monitored Data dialog box, select Ignored Users . |
| 3 | Click Add New Item .  . |
| 4 | Enter the network name for the user. Wildcards can be used. For example to add a whole domain enter YOURDOMAIN*. |
| 5 | Click Apply to save the changes. Click OK to close the dialog box. |
| 6 | Start the Web Filter Service. |

Setting a Default Audit Level

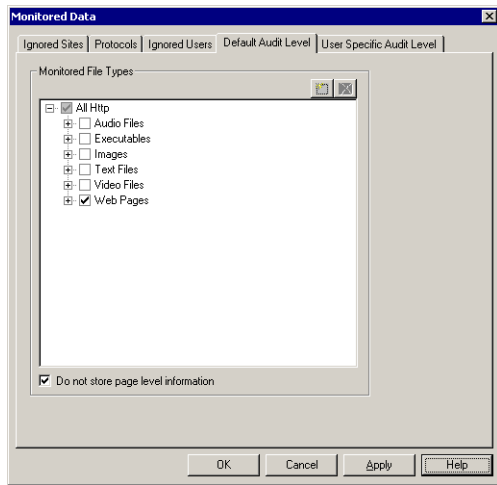


Figure 6-6 Default Audit Level tab

The Monitor only tracks Web page traffic following installation. You can change this setting in the Default Audit Level tab.

For example if you want to monitor the downloading of potentially illegal mp3 files (which can also take up considerable bandwidth), you can select mp3 from the Audio Files list. Any mp3 downloads will then be tracked in the monitor.

This can be useful when enforcing your Acceptable Use Policy.

The **Do not store page level information** setting enables all allowed pages to be stored in the database as the root, i.e., `www.bbc.co.uk/weather/5day.shtml` will be stored as `www.bbc.co.uk`. All blocked pages will be stored with the full path. This setting is selected by default for new Web Filter installations. It is not selected if you have upgraded from a previous version.

Table 6-6 Monitored File Types

| File Type | File Extensions |
|-------------|----------------------------------|
| Audio Files | aif, au, mid, mp3, wav |
| Executables | dll, exe, ocx, zip |
| Images | bmp, gif, jpeg, jpg, pcx |
| Text Files | doc, pdf, txt, xls |
| Video Files | avi, mov, mpeg, mpg, qt, ram, rm |
| Web Pages | asp, aspx, htm, html,.shtml |

You have the following options when selecting Monitored File Types:



- Select the File Type. All file extensions associated with this File Type are monitored.
- Select a specific file extension. The File Type entry this extension belongs to will be grayed out, indicating a partial selection for this File Type.



Warning: The monitoring of too many File Types can impact on the performance of Web Filter. If you suspect certain file types are being accessed significantly, select the file type and monitor it for a set period of time.

You can also add your own custom File Types and add new File Extensions, to create your own custom default audit level. These then can be applied to your users.

Procedure 6-7: Create Custom File Types and Extensions

| Step | Action |
|------|---|
| 1 | Stop the Web Filter Service. |
| 2 | Select the All HTTP entry in the Default Audit Level tab. |
| 3 | Click Add New Item .  . This will create a new file type |
| 4 | Enter a name for your file type. Press Enter . |
| 5 | Now select your newly created file type and click Add New Item .  . This will create a new file extension. |
| 6 | Enter a file extension name, minus the leading '.' and press Enter . Note: <i>a file extension can only exist in one file type group. An error message is returned if the extension already exists in another group.</i> |
| 7 | Add further file extensions by repeating steps 4 and 5. |
| 8 | Click Apply to save the changes. Click OK to close the dialog box. |
| 9 | Start the Web Filter Service. |

To edit an entry, select it and press **F2**.

User Specific Audit Levels

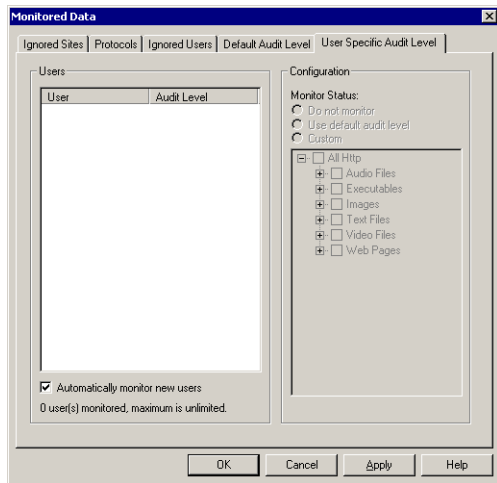


Figure 6-7 User Specific Audit Level tab

If you want to set an audit level for a specific individual, rather than change the Default Audit Level for everyone, you can do so in the User Specific Audit Level tab. The following configurations are available:

- **Do not monitor** – the user is not tracked in the monitor. You can also set this from the **Users > Don't Monitor** menu option.
- **Use default audit level** – the setting you have configured in the Default Audit Level tab is used. See “Setting a Default Audit Level” on page 51 for more details.
- **Custom** – set an audit level specific to a highlighted user. When selected, the Monitored File Types box becomes active. You can select the same file types as in “Setting a Default Audit Level” on page 51.
- **Automatically monitor new users** - as new users are added to the network, their activity is automatically monitored. This is selected by default in a new installation. It is not selected if you have upgraded from a previous version.
- The number of monitored users is shown, with your user licence limit.

Procedure 6-8: Setting a User Specific Audit Level

| Step | Action |
|------|--|
| 1 | Stop the Web Filter Service. |
| 2 | Select the User from the Users section. |
| 3 | From the Configuration section, select the Monitor Status you want to apply. |
| 4 | If using the Custom audit level, select a Monitored File Type. |
| 5 | Click Apply to save the changes. Click OK to close the dialog box. |
| 6 | Start the Web Filter Service. |


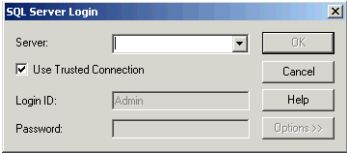
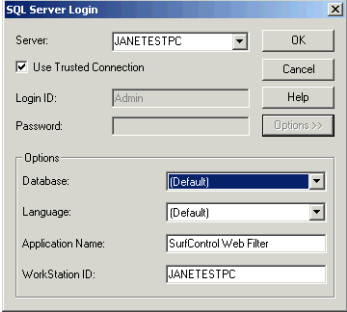
PRINTING THE USER AND SITE PANEL INFORMATION

To print out the contents of the Users and Sites Panels, select **File > Print**.

CHANGING THE MONITOR DATABASE

You can change the default database that Web Filter writes its monitored traffic to from the Web Filter Service settings tab (See “Database tab” on page 8 for more details). To view a different database in the Monitor, while still writing traffic to the default database, follow Procedure 9.

Procedure 6-9: Changing the Monitor Database

| Step | Action | |
|------|---|---|
| 7 | <p>Click .</p> <p>A SQL Server Login dialog box appears.</p> <p>The Use Trusted Connection option is selected by default. If you want to use a SQL Server Login ID and Password, clear this option and enter the details in the relevant fields.</p> |  |
| 8 | <p>From the drop-down list box, select the server you want to connect to. The Options button will then be enabled. Click Options to expand the login dialog box.</p> |  |
| 9 | Select the database you want to connect to. | |
| 10 | Add an Application Name to identify the database. Click OK . | |

6

MONITOR

Changing the Monitor Database



Chapter 7

Real Time Monitor

| | |
|-------------------|---------|
| Introduction | page 58 |
| Display Columns | page 59 |
| Category Color | page 60 |
| Collector Details | page 61 |

INTRODUCTION

The Real-Time Monitor shows Internet activity on your network as it is happening. This is different from The Monitor, which displays historic information as stored in your database.

From the **Start > Programs > SurfControl Web Filter** menu, select **Real-Time Monitor**. From other parts of Web Filter you can click the  icon. The Real-Time Monitor will appear as in Figure 7-1:



Figure 7-1 Real-Time Monitor

The following columns are visible by default in the Real-Time Monitor.

Table 7-1 Real-Time Monitor Columns

| Column | Description |
|------------------|---|
| URL | Identifies the site URL. |
| Category | Identifies the Category Web Filter has assigned to the site. |
| User | Identifies the user. |
| Action | Indicates whether the site was Allowed or Blocked by Web Filter. |
| Right Click menu | If you right click on a site, a button appears that allows you to view the selected site in your Web browser. |

Other columns can be configured via the **Options** menu. Select **General** from the Options menu. The Real-Time Monitor Options dialog box appears as in Figure 7-2:

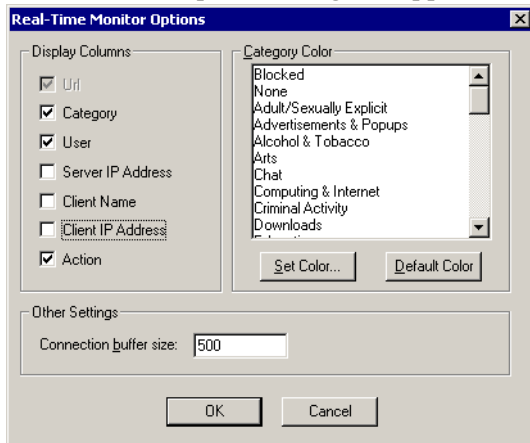


Figure 7-2 Real-Time Monitor Options dialog box



Note: Changes made in the Real-Time Monitor Options dialog box clear the existing Real-Time Monitor buffer.

From the dialog box, you can configure the following:

DISPLAY COLUMNS

This controls the columns displayed in the Real-Time Monitor window.

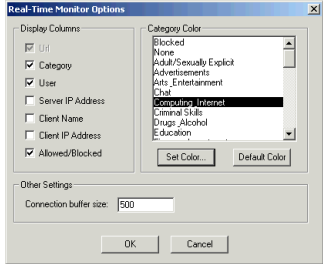
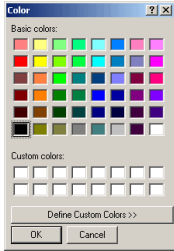
Table 7-2 Real-Time Monitor Options

| Column | Description | Default Option |
|---------------------|---|--------------------------------------|
| URL | Shows the page being visited | Yes (this option cannot be cleared.) |
| Category | Shows the SurfControl category assigned to the URL. If a site has not been categorized it will be shown as 'None' | Yes |
| User * | Shows the user name of the person accessing the site. | Yes |
| Server IP Address | Shows the IP Address for the server hosting the URL. | No |
| Client Name * | The name of the client computer accessing the site. | No |
| Client IP Address * | The IP Address of the client computer accessing the site. | No |
| Action | Shows whether the URL was Allowed or Blocked by a SurfControl Web Filter rule. | Yes |

* These columns are unavailable in the Privacy Edition.

CATEGORY COLOR

This option allows you to assign a color to a SurfControl Category. This can aid you in spotting trends in surfing habits in the Real-Time Monitor.

| Procedure 7-1: Assigning a Category Color | | |
|---|--|---|
| Step | Action | |
| 1 | Select a Category from the from the Real-Time Monitor Options dialog box. |  |
| 2 | Click Set Color... A color palette will appear. |  |
| 3 | Either select a basic color from the chart or click Define Custom Colors to select a color using HSL or RGB values. Click OK . | |
| 4 | The Category definition will now be highlighted in the color chosen. | |

COLLECTOR DETAILS

You can view information about the collector the Real-Time Monitor is connected to (see Figure 7-3). Select **Collector Details** from the **Options** menu. See Table 7-3.

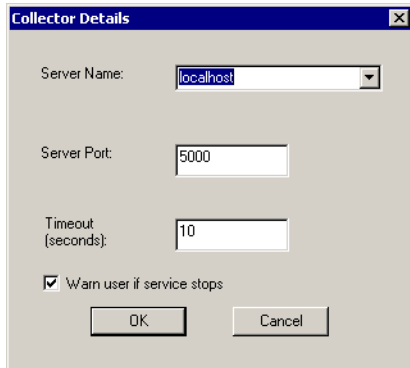


Figure 7-3 Collector Details

Table 7-3 Collector Details Options

| Option | |
|----------------------------|--|
| Server Name | The name of the server the Real-Time Monitor is connected to. You can enter the name of a new server into the drop-down list box. This server is then stored in the drop-down list. You can store up to ten servers. The first time you connect to the Real-Time Monitor, the Collector Details dialog box will display, with localhost as it's default Server Name. If you change the Server Name, the Real-Time Monitor will attempt to connect to this collector when subsequently accessed. If it cannot connect to this collector, a warning is displayed. |
| Server Port | Port number the Real-Time Monitor connects to the Web Filter Service on. The default is 5000. |
| Timeout (seconds) | The time that the Real-Time Monitor will wait before reporting an error if connection with the Server is lost. |
| Warn user if service drops | If selected, an error message will display if connection to the server is lost. |



REAL TIME MONITOR
Introduction



Chapter 8 Rules Administrator

| | |
|---|---------|
| Introduction | page 64 |
| Rule Objects | page 66 |
| Who Objects | page 67 |
| Where Objects | page 72 |
| When Objects | page 81 |
| Allowance Objects | page 85 |
| Notify Objects | page 87 |
| HTTP Deny Page Objects | page 89 |
| Changing the Rules Administrator Database | page 92 |

INTRODUCTION

In the Getting Started Guide, you enabled the supplied Adult/Sexually Explicit rule in the Rules Administrator. This rule then blocks any request to sites listed in this category from the SurfControl URL Category List.

This chapter covers the rule objects in more detail. This will enable you to configure rules more accurately, to meet your organization's requirements. The Rule object tabs are only visible if you have selected the default Advanced view in the Rules Administrator. If you can't see the Object tabs below the Rules panel, select **Advanced** from the **View** menu.

To open the Rules Administrator choose **Start > Programs > SurfControl Web Filter > Rules Administrator** or click the shortcut button in the toolbar of one of the Web Filter components.

There are three types of rules:


- **Allow** – uses positive filtering to give access. This is the default setting for any new rule you create.
- **Disallow** – uses negative filtering to deny access.
- **Allowance** – uses a combination of positive and negative filtering to set up limits for internet access. The allowance value is time based (allowing access for a predefined time limit). Once this limit has been reached, access is blocked.

GUIDELINES FOR RULE CREATION

For best results, follow these guidelines:

- Rules are processed from the top of the list in the Rule Panel downwards. Place rules to be applied to individuals or small groups near the top of the list.
- Use When and Allowance objects carefully. Use the Protocol Time Analysis report to narrow down who these rules should apply to, before creating them. See the SRC Administrators Guide for more details.
- Keep the number of rules to a minimum, to ensure the maximum efficiency of Web Filter.
- Create, test and activate any global rules you create before creating user or group specific rules.
- Ensure that only one person modifies rules at a time.
- To enable user based rules, ensure that the Monitor recognizes user names.
- If a site specific rule isn't working, ensure auto-categorization is turned on in the Web Filter Service Settings Advanced tab.

Procedure 8-1: Creating rules


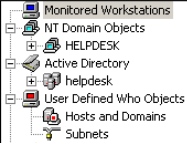
| Step | Action |
|------|--|
| 1 | Select New Rule  . New rules are always checked as enabled by default; however the rule will not be active until changes are committed to the database. |
| 2 | Choose a Who object (if required) and drop the object onto the Who section of the rule. |
| 3 | Choose a Where object (if required) and drop the object onto the Where section of the rule. |
| 4 | Choose a When object (if required) and drop the object onto the When section of the rule. |
| 5 | Choose an Allowance object (if required) and drop the object onto the Allowance section of the rule. |
| 6 | Choose a Notify object (if required) and drop the object onto the Notify section of the rule. |
| 7 | Choose a HTTP Deny Page object (if required) and drop the object onto the HTTP Deny Page section of the rule. |
| 8 | Move the rule to the appropriate level in the Rule List Panel. |
| 9 | Commit the changes to enable the rule. New rules are always checked as enabled by default; however the rule will not be active until changes are committed to the database. |
| 10 | Test the rule. |
| 11 | Make any changes if needed. |
| 12 | Commit the changes again. |

RULE OBJECTS

You can create the following Rule Objects:

- Who – see page 67 for more details.
- Where – see page 72 for more details.
- When – see page 81 for more details.
- Allowance – see page 85 for more details.
- Notify – see page 87 for more details.
- HTTP Deny Page – see page 89 for more details.

Procedure 8-2: Creating a new Rule Object

| Step | Action | |
|------|--|---|
| 13 | Select a rule object tab. |  |
| 14 | Highlight an individual object component from the left-hand pane below the tabs. |  |
| 15 | In the right-hand pane, right-click and select New . | |
| 16 | Fill in the details on the dialog box that appears. | |
| 17 | Click OK . The object can now be used in any rule you create. | |

WHO OBJECTS

Who objects are used to apply rules to certain individuals or groups.

The default for Who objects is **Anyone**.

The following objects are included in the Who tab, as in Figure 8-1:

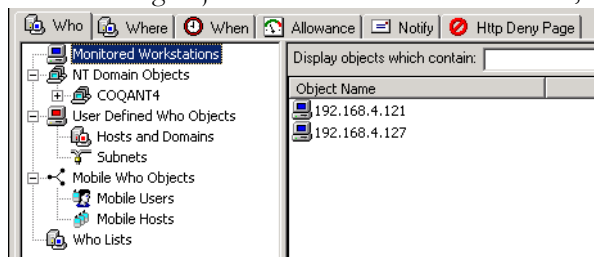


Figure 8-1 Who Objects tab

- **Monitored Workstations** - shows a list of workstations as identified in the database and seen by the Monitor and the Rules Administrator. Refresh this list with F5. You cannot manually add Monitored Workstations to this list. If workstations appear as IP addresses, you need to select Enable Workstation name resolution on the Advanced Settings tab in the Web Filter Services Settings. See “Advanced tab” on page 5 for more details.
- **Active Directory, NT and NetWare Domain Objects** -lists objects taken from the domain. These only apply to local Active Directory, NT, or Novell NetWare networks. Refresh this list with F5. You cannot manually add Active Directory or NT Domain Objects to this list. Depending on where Web Filter is installed you will see the objects as described in Table 8-1:

Table 8-1 Active Directory, NT and NetWare Domain objects

| Where Installed | Objects seen |
|---------------------------------|---|
| Workgroup | NT Domain objects: Workgroup. |
| NT Domain | NT Domain objects: Workgroup, Domain object. |
| Active Directory | NT Domain objects: Workgroup, Domain object. Active Directory objects: Domain object: Note: <i>Only the currently logged on Active Directory forest will be seen by the Who Object. All trusted NT domains can be seen. SurfControl recommends using the Active Directory objects. if Web Filter has been installed in this environment.</i> |
| NetWare Domain/NT Workgroup | NT Domain objects: Workgroup. NetWare objects: Domain object. |
| NetWare Domain/NT Domain | NT Domain objects: Workgroup, Domain object. NetWare objects: Domain object. |
| NetWare Domain/Active Directory | NT Domain objects: Workgroup, Domain object. Active Directory objects: Domain object: NetWare objects: Domain object. |

- **User-defined Who Objects** - These have to be created manually and can consist of the following:
 - Hosts and Domains
 - Subnets
- **Who Lists** - Who Lists are a combination of Monitored Workstations, NT Domain and User Defined Who Objects. Who lists are a convenient way of grouping Who objects together to share common rules.

The list of workstations available in the Administrator are the same as you see in the Web Filter Monitor, in addition to the Novell NetWare and Windows NT users defined for the network. As Web Filter detects new users, it updates both the Monitor and the Rules Administrator. To refresh the display with the most current contents of the database, press F5.

CREATING USER DEFINED WHO OBJECTS

Hosts and Domains

The Hosts and Domains object is used to apply a rule to a particular IP address, Host name or Domain on your network.

A host is a computer that is connected to a TCP/IP network which can include the internet. Each host has a unique IP address.

A domain is a group of computers on a network that are administered as a unit.

Figure 8-2 shows the Hosts and Domain object properties:

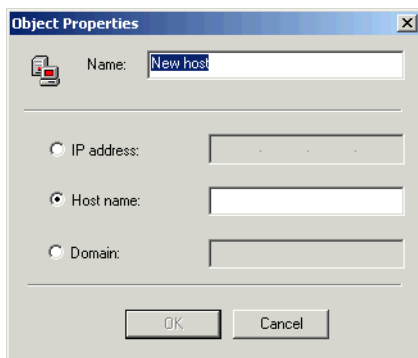


Figure 8-2 Hosts and Domain object properties

Table 8-2 Hosts and Domains object fields

| Field | Description |
|------------|--|
| Name | Enter a name for your object |
| IP address | Select the IP address and enter the IP address for the workstation the rule will be applied to. |
| Host name | The default option. Enter the Workstation name. You must have Enable Workstation name resolution selected in the Advanced Settings to be able to see Host names in the Monitor. See "Advanced tab" on page 5 for more details. |
| Domain | Enter a name for a network Domain the rule will be applied to. |

Subnet Object

A subnet allows you to take a single IP network address and split it up so that it can be used on several interconnected local networks.

A subnet mask determines the maximum number of hosts on a subnetwork.

To obtain the IP address and Subnet Mask for a particular computer on your network, run the following command from a Command Prompt window:

```
ipconfig/all
```

Make a note of the **IP Address** and **Subnet Mask** entries.

Figure 8-3 shows the Subnet object properties:

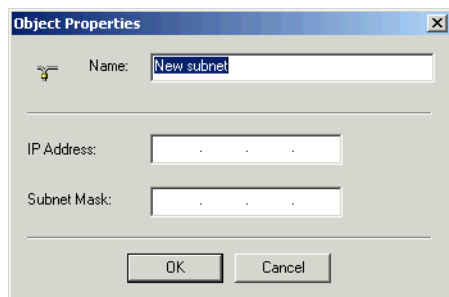


Figure 8-3 Subnet object properties

Table 8-3 Subnet object properties

| Field | Description |
|-------------|--------------------------------------|
| Name | Enter a name for your Subnet object. |
| IP Address | Enter the IP address. |
| Subnet Mask | Enter the Subnet Mask. |

Who List Objects

A Who list object can comprise of several specific Objects from the Who Object list. This provides a convenient way of grouping objects to share a set of rules. To create a Who List, drag individual Who Objects (Monitored Workstations, NT Domain Objects and User-Defined Who Objects) from the bottom right-hand pane to the bottom left-hand pane in the Who List dialog box as in Figure 8-4:

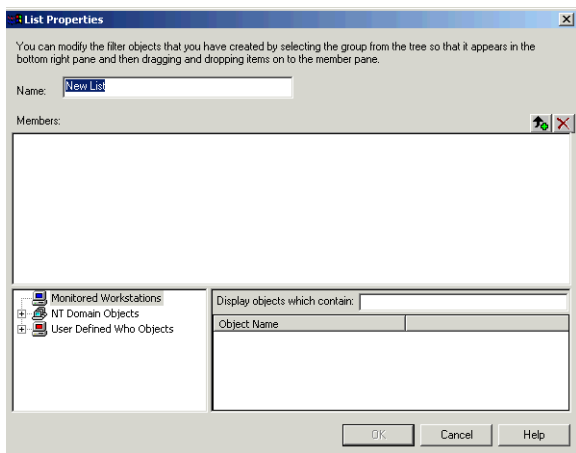


Figure 8-4 Who List dialog box

Table 8-4 Who List dialog box

| Field | Description |
|---------|---|
| Name | Enter a name for your Who List object |
| Members | This panel will show the individual objects that make up your list. |

WHERE OBJECTS

Where objects are used to identify the destinations that a rule should apply to.

The default for Where objects is **Anywhere**.

The following objects are included in the Where tab, as in Figure 8-5:

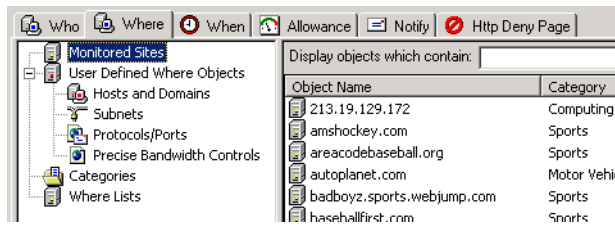


Figure 8-5 Where Objects tab

- **Monitored Sites** – the list of all sites currently seen by the Monitor and stored in the database. Refresh this list with F5. You cannot manually add a site to the Monitored Sites list.
- **User Defined Where Objects** – These have to be created manually and can consist of the following:
 - Hosts and Domains
 - Subnets
 - Protocols and Ports
 - Precise Bandwidth Controls
- **Categories** – the list of the SurfControl URL List categories and any custom categories.
- **Where Lists** – Where Lists are a combination of Monitored Sites, User Defined Where Objects and Categories. Where lists are a convenient way of grouping Where objects together to share common rules.

CREATING USER DEFINED WHERE OBJECTS

Hosts and Domains

The Hosts and Domains object is used to apply a rule to a particular IP address, Host name or Domain on your network.

A host is a computer that is connected to a TCP/IP network which can include the internet. Each host has a unique IP address.

A domain is a group of computers on a network that are administered as a unit.

Figure 8-6 shows the Hosts and Domain object properties:

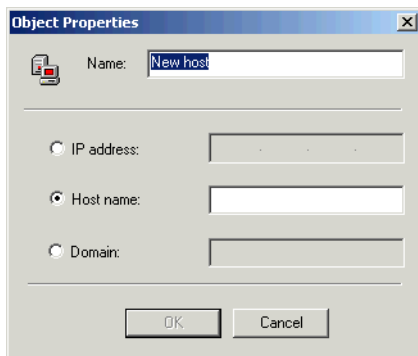


Figure 8-6 Hosts and Domain object properties

Table 8-5 Hosts and Domains dialog box fields

| Field | Description |
|------------|--|
| Name | Enter a name for your object |
| IP address | Select IP address and enter the IP address for the workstation the rule will be applied to. |
| Host name | The default option. Enter the Host name in the following format: www.yoursite.com |
| Domain | Enter a name for a network Domain the rule will be applied to. |

Subnet Object

A subnet allows you to take a single IP network address and split it up so that it can be used on several interconnected local networks.

A subnet mask determines the maximum number of hosts on a subnetwork.

To obtain the IP address and Subnet Mask for a particular computer on your network, run the following command from a Command Prompt window:

```
ipconfig/all
```

Make a note of the **IP Address** and **Subnet Mask** entries.

Figure 8-7 shows the subnet object properties:

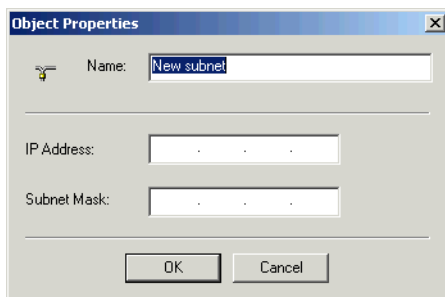


Figure 8-7 Subnet object properties

Table 8-6 Subnet object dialog box

| Field | Description |
|-------------|--|
| Name | Enter a name for your Subnet object. |
| IP Address | Enter the IP address for the computer. |
| Subnet Mask | Enter the Subnet Mask. |

Protocols/Ports Object

The only protocol monitored is HTTP.

Figure 8-8 shows the Protocol/Port object properties:

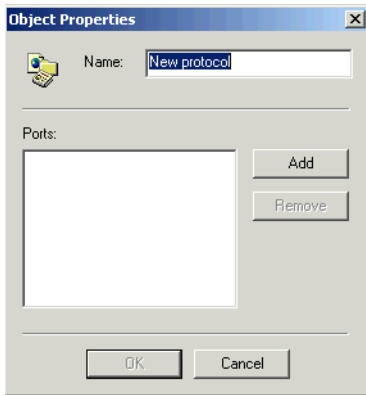


Figure 8-8 Protocol/Port object properties

Table 8-7 Protocol/Port dialog box

| Field | Description |
|-------|--|
| Name | Enter the new protocol name. |
| Port | Click Add to assign a port number to your protocol. Add again if there is more than one port associated with the protocol. Use Remove to remove a port number. |

Precise Bandwidth Controls Object

With a Precise Bandwidth Control, you can accurately define what content you want to allow or block. By creating rules with Precise Bandwidth Controls, you can block pages or files that contain precise prefixes, suffixes, or word patterns. These rules operate by identifying the contents within the URL rather than just the top-level domain name.

Precise Bandwidth Control objects are “if” statements, which means that if you apply more than one Precise Bandwidth Control object to the rule, the rule only applies if both conditions are met.

Figure 8-9 shows the Precise Bandwidth Control object properties:

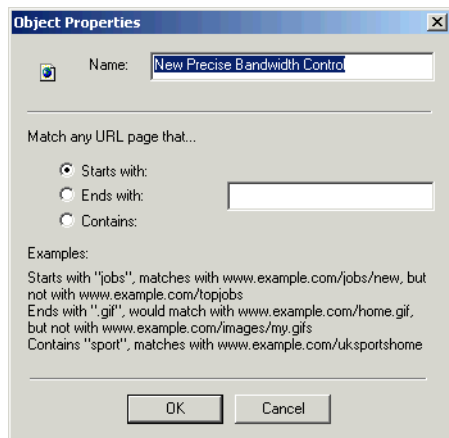


Figure 8-9 Precise Bandwidth Control object properties

Table 8-8 Precise Bandwidth Control dialog box

| Field | Description |
|----------------------------|---|
| Name | Enter a name for your Precise Bandwidth Control |
| Match any URL page that... | <p>You have three options for your control:</p> <ul style="list-style-type: none"> • Starts with: - for instance the word 'jobs' means any URL that starts with the word jobs: i.e www.jobserve.co.uk will match, but www.topjobs.co.uk will not. • Ends with: - if you specify the word '.gif' i.e. www.example.com/home.gif will match, but www.example.com/my.gifs will not. • Contains: - if you specify 'jobs' in the field both www.jobserve.co.uk and www.topjobs.co.uk will match. <p>Note: You can enter multiple selections by using a comma to separate the selections. I.e. .gif,.bmp,.jpg</p> |

CATEGORY OBJECT

SurfControl's URL Category List contains over 9 million Web sites and over 1.7 billion Web pages. These sites and pages are allocated to one of SurfControl's forty seven categories as in Table 8-9:



Note: As the SurfControl content team can dynamically add new categories, this list is subject to change. For the latest list and detailed explanation of each category, visit www.surfcontrol.com.


Table 8-9 SurfControl Categories

- | | |
|---|---|
| <ul style="list-style-type: none"> • Adult/Sexually Explicit • Advertisements & Popups • Alcohol & Tobacco • Arts • Business • Chat • Computing & Internet • Criminal Activity • Downloads • Education • Entertainment • Finance & Investment • Food & Dining • Forums & Newsgroups • Gambling • Games • Glamour & Intimate Apparel • Government & Politics • Hacking • Health & Medicine • Hobbies & Recreation • Hosting Sites • Illegal Drugs • Intolerance & Hate | <ul style="list-style-type: none"> • Job Search & Career Development • Kids Sites • Motor Vehicles • News • Personals & Dating • Phishing & Fraud • Photo Searches • Proxies & Peer-to-Peer • Real Estate • Reference • Religion • Search Engines • Sex Education • Shopping • Society & Culture • Sports • Spyware • Streaming Media • Tasteless & Offensive • Travel • Violence • Weapons • Web-based E-mail |
|---|---|



Note: You will receive an e-mail informing you of any changes made to the SurfControl URL Category List.

SurfControl Categories

SurfControl's content team have the ability to dynamically add new categories via a URL Category List update. For this reason SurfControl categories are read only, and appear in the Category Object list with the following icon: 

You cannot re-name or delete them from within SurfControl Web Filter.

SurfControl categories do not support SmartScan. You must create a custom category to use this functionality.

Custom Categories

The Category Object allows you to create custom categories, which can contain any of the following:

- One or more of the pre-defined SurfControl categories.
- Keywords that are matched against the domain level of a URL, using SmartScan.

Custom categories you create will appear in the Category object list with the following icon: 

Custom categories can be re-named and deleted from within Web Filter via a right-click menu from a selected category. If a SurfControl category is added or re-named identically to a custom category you created, your custom category will be amended with brackets containing a number, i.e. custom(1).

Figure 8-10 shows the Category List object properties:

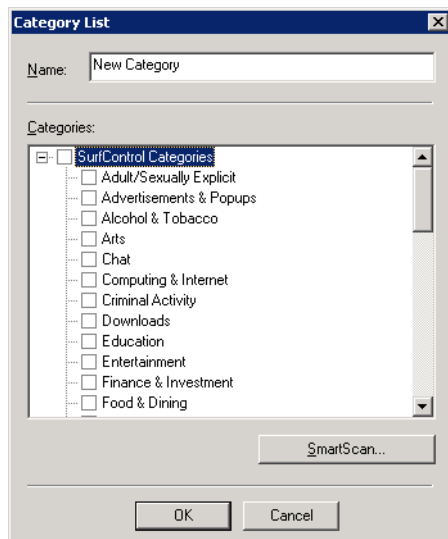


Figure 8-10 Category List object dialog box

Table 8-10 Category List dialog box

| Field | Description |
|------------------|---|
| Name | Enter a name for your new category |
| Categories | Select one or more of the SurfControl Categories you want to include in your new category. |
| SmartScan button | <p>If you want to refine the category match, select a category you are including in the object and click SmartScan. Enter the keywords that you wish to match for any domains that will be allocated to the category. The keyword must form all or part of the domain level URL.</p> <p>Example: Entering 'football' will match the following URLs: www.football365.com www.football.guardian.co.uk It will not return www.bbc.co.uk/football as 'football' is not part of the domain level URL.</p> |

Your new category will now be seen in the Where tab Categories pane. It is important that you move this custom category to the top of the list, so it is applied before the standard categories. From the **Tools** menu, use **Set Category Object Order** to do this.

WHERE LISTS

A Where list object can comprise of several specific Objects from the Where Object list (see Figure 8-11). This provides a convenient way of grouping objects to share a set of rules. To create a Who List, drag individual Where Objects (Monitored Workstations, NT Domain Objects and User-Defined Where Objects) from the bottom right-hand pane to the upper left-hand pane in the Where List dialog box.

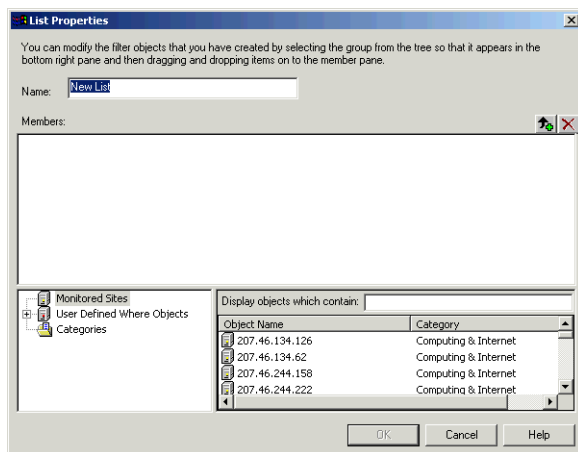


Figure 8-11 Where List dialog box

Table 8-11 Where List dialog box

| Field | Description |
|---------|---|
| Name | Enter a name here for your Where List object |
| Members | This panel will show the individual objects that make up your list. |

WHEN OBJECTS

When objects are used to define the time and date when a rule will be applied.

The default setting for When objects is **Anytime**.



Note: When objects use 24-hour clock.

SurfControl Web Filter is supplied with three pre-defined When Objects as in Figure 14:

- After Work
- Weekends
- Worktime

The following objects are included in the When tab, as in Figure 8-12:

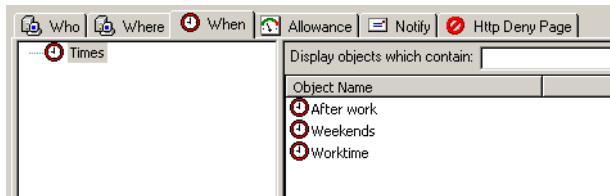


Figure 8-12 When objects tab

You can either create a new When object if necessary, or change the default properties of the supplied objects to suit your purposes.

After work

The After work object has the following default properties. Right-click the object and select **Properties** to view. Figure 8-13 shows the After Work object properties:

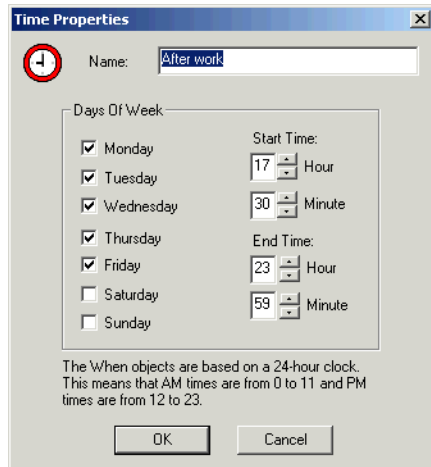


Figure 8-13 After work object properties

- **Days of the Week** – Monday to Friday.
- **Start Time** – 17:30.
- **End Time** – 23:59.

Weekends

The Weekends When object has the following default properties. Right-click the object and select **Properties** to view. Figure 8-14 shows the Weekend object properties:

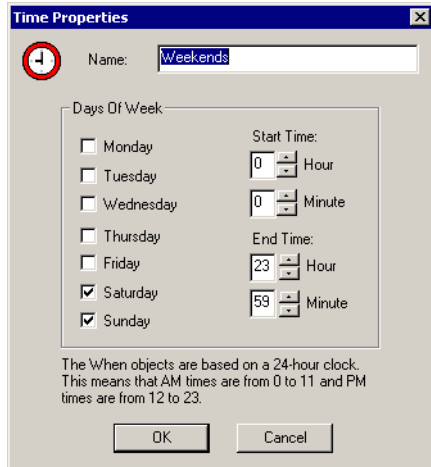


Figure 8-14 Weekend object properties

- **Days of the Week** – Saturday & Sunday.
- **Start Time** – 0:00.
- **End Time** – 23:59.

Worktime

The Worktime When object has the following default properties. Right-click the object and select **Properties** to view. Figure 8-15 shows the Worktime object properties:

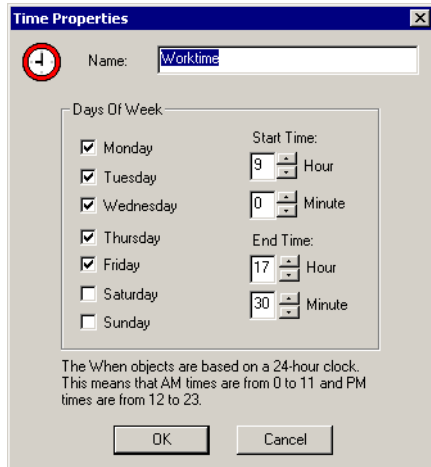


Figure 8-15 Worktime object properties

- **Days of the Week** – Monday to Friday.
- **Start Time** – 09:00.
- **End Time** – 17:30.

ALLOWANCE OBJECTS

Allowance objects are used to permit Internet access for a specified period of time. Once this limit has been reached, access is blocked.

The default for Allowance objects is **None**.

Web Filter is supplied with one pre-defined Allowance Object as in Figure 8-16:

- 30 minutes time value object

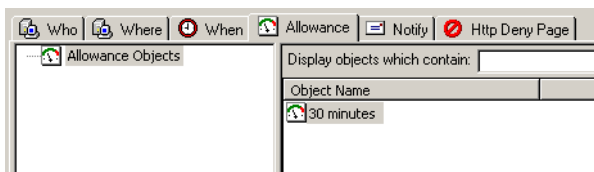


Figure 8-16 Allowance object tab

You can either create a new Allowance object if necessary, or change the default properties of the supplied object to suit your purposes.

30 MINUTE TIME OBJECT

The 30 Minute Allowance object has the following default properties. Right-click the object and select **Properties** to view. Figure 8-17 shows the 30 minute object properties:

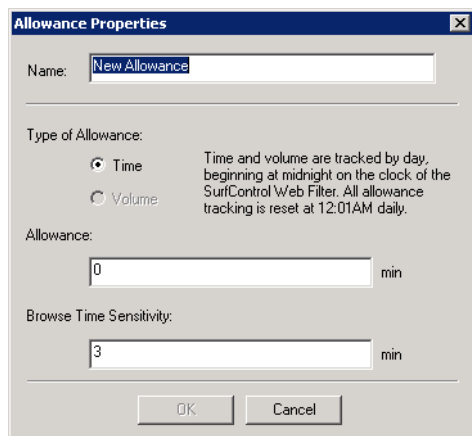


Figure 8-17 30 Minute object properties

Table 8-12 30 Minute object properties

| Type of Allowance | Allowance Limit |
|-------------------------|-----------------|
| Time | 30 min |
| Browse Time Sensitivity | 3 min |

About Browse Time Sensitivity

Browse Sensitivity refers to the maximum amount of time Web Filter presumes a user to be actively engaged with a site. Browse sensitivity is also used to offset the uncertainty about how much actual time a user is engaged in browsing. By default, Browse Sensitivity is set to three minutes.

Browse Sensitivity comes into play every time a user launches a browser. However, the way in which Web Filter attributes Browse Sensitivity depends on whether the browsing takes place as a stand-alone occurrence or in a sequence of connections.

Stand-alone browsing. Stand-alone browsing is a single connection to the Internet. For example, stand-alone browsing occurs when a user opens their browser and makes a connection to a site, does not go to any subdirectories of the site, then either closes their browser or makes no more connections.

When a user browses in a stand-alone occurrence, Web Filter calculates the browse time to be equal to the Browse Sensitivity (by default, three minutes).

Example

A user opens a connection to CNN.com. Technically, they spend forty-five minutes at the site, because even though they stop browsing and are working on other tasks, the browser is left open.

The browse time to CNN.com is calculated to be three minutes because the Browse Sensitivity is set to three.

Continuous browsing. Continuous browsing occurs when there is a sequence of connections, each one made within three minutes of the last. SurfControl Web Filter automatically adds the Browse Sensitivity value to the last connection in the sequence.

Example

A user opens their browser and makes a connection to ebay.com for two minutes, connects to ebay.com\ebaymotors for one minute, then opens ebay.com\ebaymotors\motorcycles for one minute. Web Filter records the browse time as in Table 8-13:

Table 8-13 Example Continuous Browsing Recording

| From | To | + Browse Time Sensitivity | Duration |
|--------------------------|-------|---------------------------|------------------|
| 10:00 | 10:02 | | 2 minutes |
| 10:02 | 10:03 | | 1 minute |
| 10:03 | 10:04 | 3 minutes | 4 minutes |
| Total Browse Time | | | 7 minutes |

NOTIFY OBJECTS

Notify objects allow you to inform by e-mail specified people within the organization that a rule has been broken (see Figure 8-18).

Notify objects work in a different way, depending on what type of rule has been broken.

- **Allow rule** – one message will be sent once per hour per user.
- **Disallow rule** – one message will be sent per user each time a rule is triggered.
- **Allowance rule** – After the Allowance limit is exceeded, one message per user is sent each time the rule is triggered.

There is no default Notify object

Figure 8-18 Notify Objects tab

.Figure 8-19 shows the SMTP e-mail Notification object properties:

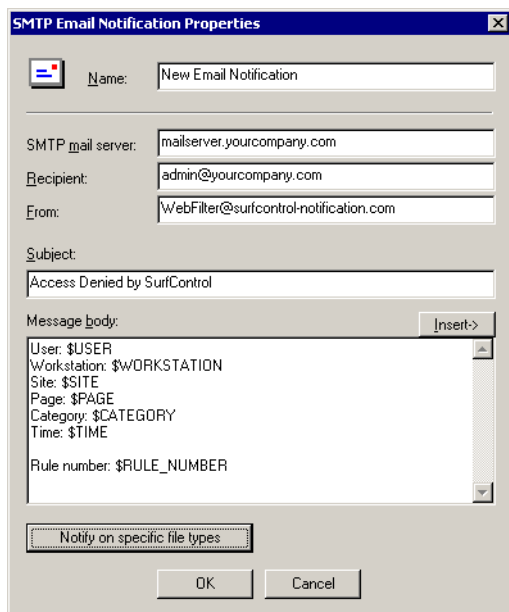


Figure 8-19 SMTP e-mail Notification Properties

Table 8-14 SMTP e-mail Notification dialog box


| Field | Description |
|-------------------------------|---|
| Name | Enter a name for your new Notify object. |
| SMTP mail server | Enter the address of your mail server. This information can be obtained from the E-mail Notification tab in the Web Filter Service Settings dialog box. Right-click the SurfControl icon in the status area of the taskbar.  |
| Recipient | Enter the e-mail address of the person you want to receive the notification. If you want to send the message to multiple recipients, make sure there is a space between each e-mail address. |
| From | You can either leave the default address in this field, or enter a suitable address for your own organization. |
| Subject | Enter a relevant subject for your e-mail object. |
| Message body | The object comes with pre-defined data that you can include in the construction of your notification object. Click Insert to select any of the following: <ul style="list-style-type: none"> • User • Workstation • Site • Category • Protocol • Time • Rule Number • Page |
| Notify on Specific File Types | By default, the notification object is only triggered if the base Web page is blocked. You can use this option to specify which file types you want to send notifications on. Click the button and select the file type from the dialog box. The available file types are shown in Table 8-15. |

Table 8-15 Notification File Types

| File Type | File extensions |
|-------------|----------------------------------|
| Audio Files | aif, au, mid, mp3, wav |
| Executables | dll, exe, ocx, zip |
| Images | bmp, gif, jpeg, jpg, pcx |
| Text Files | doc, pdf, txt, xls |
| Video Files | avi, mov, mpeg, mpg, qt, ram, rm |
| Web Pages | asp, aspx, htm, html, shtml |

HTTP DENY PAGE OBJECTS

HTTP Deny Page objects are Web pages that a user will see when they have triggered a rule, e.g. if they try to access a site that is blocked (see Figure 8-20).

The default setting for HTTP Deny Page objects is **Default**.

Web Filter is supplied with a pre-defined HTTP Deny Page Object:

- Default

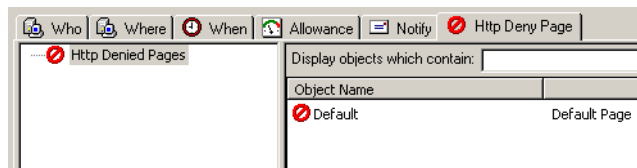


Figure 8-20 HTTP Deny Page object tab

DEFAULT

The Default HTTP Deny Page object has the following default properties. Right-click the object and select **Properties** to view. Figure 8-21 shows the Default HTTP Deny Page object properties:

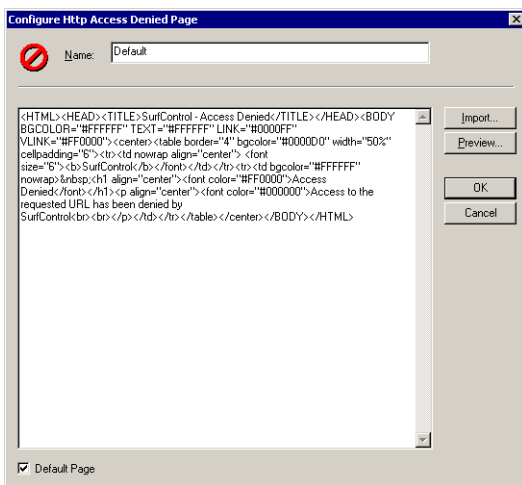


Figure 8-21 Default HTTP Deny Page object properties

This produces the Web page as in Figure 8-22:

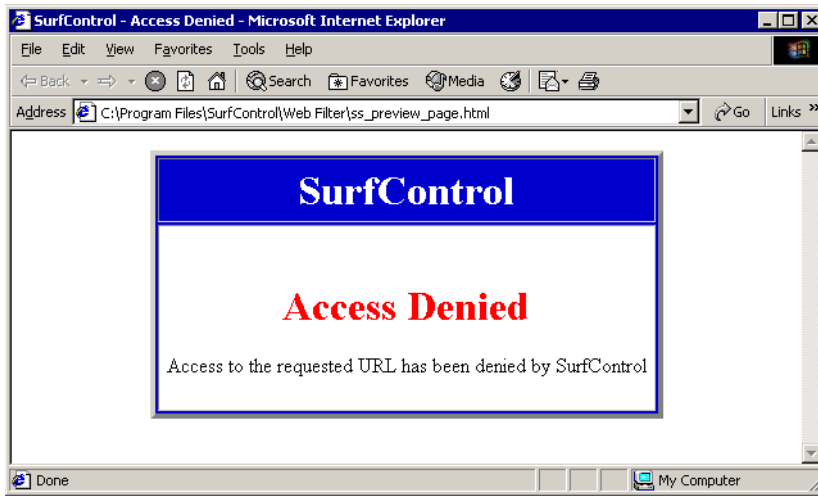


Figure 8-22 Default HTTP Deny Web Page

You can edit the text from within the object. See “Constructing HTTP Deny Pages” on page 91 for restrictions applying to editing or constructing deny pages.

From the dialog box you have the following options:

Table 8-16 Default HTTP Deny Page object dialog box options

| Option | Description |
|--------------|---|
| Import | You can import HTML code you have created in a file elsewhere, or you can re-import the default deny page text from the following location: C:\Program Files\SurfControl\Web Filter\Sample Denied Text\Default_Denied.html |
| Preview | Use this option to see how your deny page will look in a browser. |
| Default Page | This option is selected as this is the default page supplied by SurfControl. |

OTHER HTTP DENY PAGE OBJECTS

SurfControl have supplied the following html pages which you may find useful when creating custom deny pages:

- `Redirect_Denied.html`
- `Refresh_to_AUP.html` – this allows you to redirect a user to your Acceptable Use Policy.

These pages can be found in the following location in a default installation:

`C:\Program Files\SurfControl\Web Filter\Sample Denied Text\`

CONSTRUCTING HTTP DENY PAGES



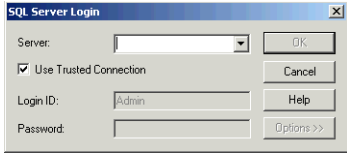
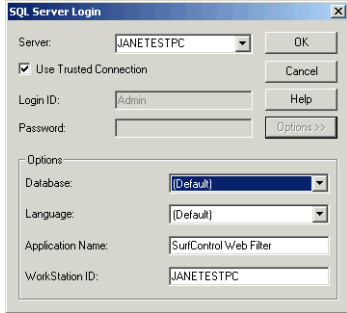
When constructing your own HTTP Deny Pages, you are restricted to using 4950 characters or less, including the HTML tags, when building your deny page. In addition there are the following objects you can insert into your HTTP Deny Page objects:

- User
- Client_IP
- Site
- Category
- Page

CHANGING THE RULES ADMINISTRATOR DATABASE

You can change the database that Web Filter stores its rules to both from The Web Filter Service settings tab (See “Database tab” on page 8 for more details), or from the Rules Administrator itself. Procedure 8-3 shows how to change the database from within the Rules Administrator.

Procedure 8-3: Changing the Rules Administrator Database

| Step | Action | |
|------|---|---|
| 1 | Stop the Web Filter service. Right Click the SurfControl Web Filter icon  in the status area on the task bar and select Stop Web Filter Service from the SurfControl Web Filter Service Settings dialog box. | |
| 2 | Click  . A SQL Server Login dialog box appears. The Use Trusted Connection option is selected by default. If you want to use a SQL Server Login ID and Password, clear this option and enter the details in the relevant fields. |  |
| 3 | From the drop-down list box, select the server you want to connect to. The Options button will then be enabled. Click Options to expand the login dialog box. |  |
| 4 | Select the database you want to connect to. | |
| 5 | Add an Application Name to identify the database. Click OK . | |
| 6 | Start the Web Filter Service. | |



Chapter 9

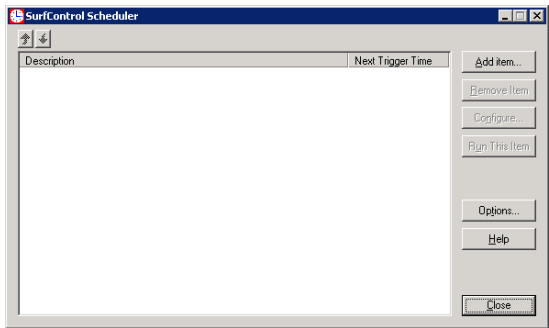
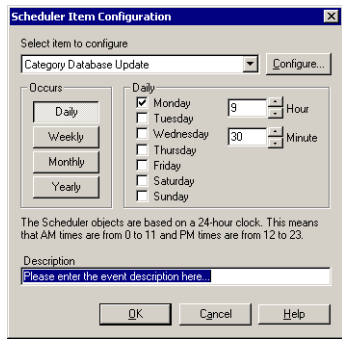
Scheduler

| | |
|-----------------------|----------|
| Introduction | page 94 |
| Available Events | page 95 |
| URL Category List | page 95 |
| Command Line | page 95 |
| Database Management | page 96 |
| Database Update | page 99 |
| Network Group Updates | page 100 |

INTRODUCTION

You can schedule certain events that consume high bandwidth or that need users to be logged off the network to take place at a convenient time.

Procedure 9-1: Scheduling an Event

| Step | Action | |
|------|---|---|
| 1 | Select Scheduler from the Programs > SurfControl > Web Filter menu. |  |
| 2 | Click Add Item . The Scheduler Item Configuration dialog box will appear. |  |
| 3 | From the Select item to configure drop-down list box select the event you want to configure. | |
| 4 | Select when you want the event to occur – Daily, Weekly, Monthly or Yearly. Further options are available depending on the frequency chosen. | |
| 5 | Enter a name for the event in the Description field. | |
| 6 | Click Configure . Depending on the event chosen, a dialog box will appear. Once you have completed the details in the dialog box, Click OK . Click OK in the Item Configuration dialog box and your event should now be listed in the Scheduler main dialog box. | |

AVAILABLE EVENTS

You can set up the following events in the Scheduler:

URL CATEGORY LIST

Your URL Category List is important in helping you to identify the nature of Web sites being accessed on your network.

URL Category List updates are produced daily and can vary in size. SurfControl recommends that you schedule this event to take place every day at a time when Internet traffic is low.

When you installed SurfControl Web Filter you were asked to register for updates. If you did not register during installation, you will be asked to fill in the registration form again before you can schedule a URL Category List update.



Warning: URL Category List Updates are only available to registered product users or products within the 30 day evaluation.

COMMAND LINE

Command line items such as batch routines can be scheduled to run. The following dialog box appears when you click **Configure** from the Scheduler Item configuration dialog box as in Figure 9-1:

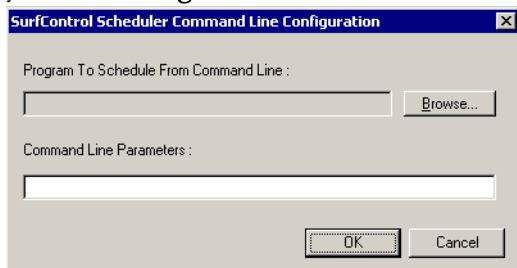


Figure 9-1 Command Line Configuration dialog box

Click Browse to locate the required file. Enter any required Parameters in the Command Line Parameter field and Click **OK**.

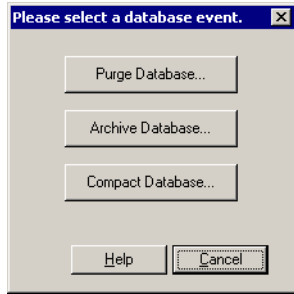
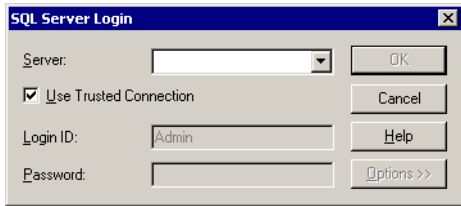
DATABASE MANAGEMENT

You can schedule the following database routines:

- Purge
- Archive
- Compact

For more details on these routines, see “Database management” on page 20.

Procedure 9-2: Select a Database for Events

| Step | Action |
|------|--|
| 1 | Select Database Management Tasks from the Select Item to Configure drop-down list box |
| 2 | Click Configure .  |
| 3 | Select the Database task from the dialog box. |
| 4 | Click Select to choose a database. A SQL Server Login dialog box appears. Choose an available Server from the drop-down list box.  |
| 5 | Click Options and select the database you want to use from the drop-down list box. Note: <i>The database selected will be retained by the Database management settings.</i> |
| 6 | Click OK . |

Purge

Figure 9-2 shows the Select purge criteria dialog box:

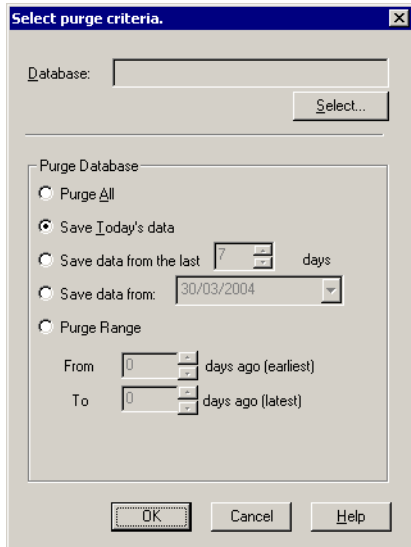


Figure 9-2 Select purge criteria

Table 9-1 Select Purge Criteria options

| Option | Description |
|----------------------------------|---|
| Purge All | Removes all connection details from the database. |
| Save Today's data | Removes all but the current day's connection details. |
| Save data from the last "N" days | "N" is the number of days to retain connection details. |
| Save data from DD/MM/YY | Removes all connection details before the specified date. |
| Purge Source Database | Removes connection details from a specific range of days. |

Archive

Figure 9-3 shows the Select archive criteria dialog box:

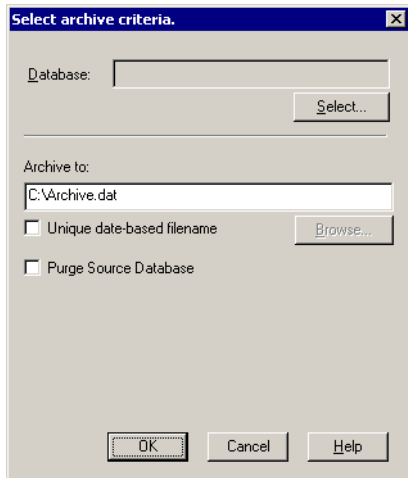


Figure 9-3 Select Archive Criteria

Table 9-2 Select archive criteria options

| Option | Description |
|----------------------------|--|
| Archive to | Location and name of the archived database. In a default installation this is C:\Archive.dat on the server where the database is hosted. |
| Unique date-based filename | Gives the archived database a unique name, which will prevent it being overwritten, the next time the scheduled event is run. |
| Purge Source Database | Removes all connection details apart from the current day's data. |

Compact

Over time your database will become fragmented, increasing in size and making it less efficient. Compacting shrinks your database, removing redundant space without removing any data.

Once you have selected the database to compact, click **OK**.

DATABASE UPDATE

If you have selected to update the flat files into your database manually, you can schedule this at a time that best suits your network. See the “Advanced tab” on page 5 for more details on database update settings.



Warning: Do not schedule flat file updates from multiple collectors to take place at the same time. This can corrupt your database.

Figure 9-4 shows the DBUpdater for SurfControl Scheduler dialog box:

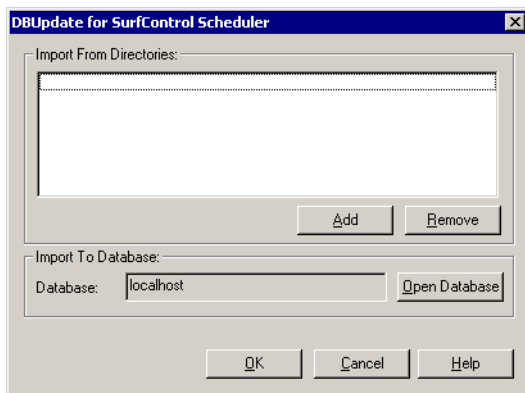


Figure 9-4 DBUpdate for SurfControl Scheduler dialog box

Table 9-3 DBUpdate Fields

| Field | Description |
|-------------------------|---|
| Import From Directories | Click Add to navigate to the directory where your flat files are located. Click Remove if you want to delete a location. Flat files are stored in the following directory by default: C:\Program Files\SurfControl\Web Filter\tmp |
| Import To Database | Click Open Database. You have two choices: <ul style="list-style-type: none"> Choose a SurfControl Collector from the drop-down list box then click Connect to SQL Server to select a SQL Server Database resident on the Collector. Click Connect to SQL Server if using a database on the local computer. Select Use Trusted connection for Windows Authentication (the default option), or deselect this option and use a valid SQL Login ID and Password. |

NETWORK GROUP UPDATES

Make sure you have set up the occurrence options first. Then click **Configure**. A Network Group Lookup Configuration dialog box will appear as in Figure 9-5. You have the following option:

Automatic Removal of Inactive Users

If you enable this option, users who no longer belong to any network group, and whose last monitored connection was more than ‘N’ days ago will be removed from the database along with their connection information.

‘N’ is the figure set in the Removal Time Period (days) field. The default setting is 90 days.

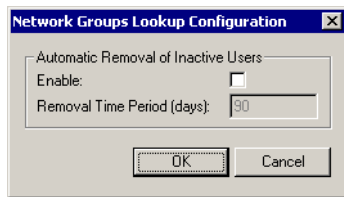


Figure 9-5 Network Group Lookup Configuration dialog box

Click **OK** to confirm the network Group Update.

SCHEDULER OPTIONS

Figure 9-6 shows the Scheduler Options dialog box:

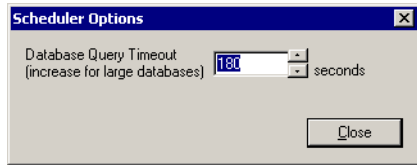


Figure 9-6 Scheduler Options

The Scheduler Options allow you to set a timeout value in seconds for your database. If the Scheduler cannot establish a query to the database within the time set, the scheduled event will be cancelled. For larger databases SurfControl recommends setting this value to 3600 seconds.

9

SCHEDULER *Available Events*



Chapter 10 Virtual Control Agent

| | |
|-----------------------------------|----------|
| Introduction | page 104 |
| How it Works | page 104 |
| Using the VCA | page 105 |
| VCA List of Sites tab | page 105 |
| VCA Settings tab | page 107 |
| VCA Results tab | page 109 |
| The VCA Control Panel application | page 111 |


INTRODUCTION

The Virtual Control Agent (VCA) evaluates unknown web sites, reading and analyzing content page by page. It then uses cutting-edge artificial intelligence algorithms to study and classify each Web page into one of the SurfControl Web Filter categories. This allows sites initially categorized as ‘None’ in the Monitor to be categorized more meaningfully.

HOW IT WORKS

- 1 The VCA collects a representative number of pages and analyzes their content.
- 2 The VCA's Neural Network compares the page and site with other sites in the SurfControl Web Filter categories.
- 3 It then puts the site into the category that it most resembles. For more details on SurfControl's URL Category List, see “SurfControl Categories” on page 140.

USING THE VCA

You can open the VCA from the **Start > Programs > SurfControl Web Filter** menu, or from a shortcut button  within the other SurfControl Web Filter components. The default view is the List of Sites tab as in Figure 10-1.

VCA LIST OF SITES TAB

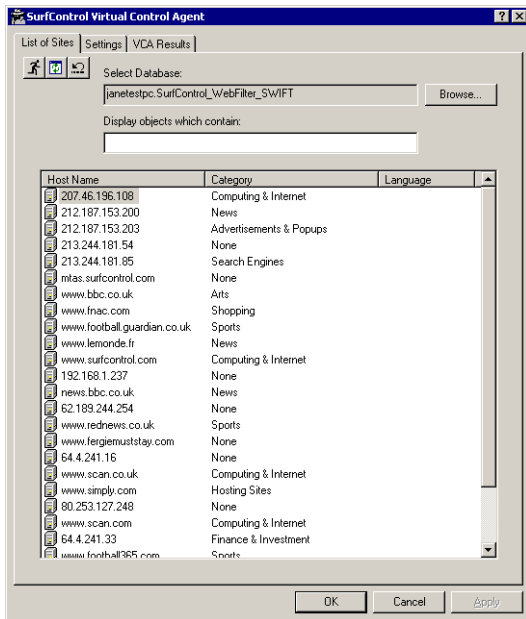





Figure 10-1 VCA List of Sites tab

Table 10-1 VCA List of Sites tab properties

| Item | Description |
|---|--|
| List of Sites tab | Shows the current list of sites in the Monitor database. Click the Host Name column heading to sort sites by name or the Category column heading to sort sites by category. |
| Categorize all 'None' Sites button.  | Starts the VCA categorization process. |
| Refresh List.  | Used to refresh the site list in the VCA |
| Set all sites back to unchecked.  | In each run the VCA attempts to categorize all 'None' unchecked sites. However if the sites have already been checked in a former run the VCA will not attempt to re-categorize these sites. Use Set All Sites back to Unchecked to set sites back to the 'unchecked' state that they were in previously. The VCA will then attempt to categorize the 'None' sites again in the next run. This action only applies to 'None' sites. |
| Select Database | The field shows the database currently in use for VCA runs. Browse to connect to another SurfControl Web Filter computer (Collector), or Connect to SQL Database to select a Server and Database. |
| Display objects which contain | Enter part or all of a URL to search the VCA List of Sites for a particular Web site or group of sites. |
| Host Name column | Shows the URL for a categorized site. |
| Category column | Shows the VCA category for the URL. |
| Language column | The following language dictionaries are installed in the VCA: <ul style="list-style-type: none"> • Dutch • English • French • German • Spanish If the VCA cannot categorize a site against any of these dictionaries, It will show the appropriate Language in this column and 'None (Checked)' in the Category column. |
| Settings tab | Shows the VCA configuration settings. See "VCA Settings tab" on page 107 for more details. |
| VCA reports | Shows results for either specific VCA runs or all runs in total. See "VCA Results tab" on page 109 for more details. |

Right-clicking any site in the List of Sites dialog box brings up a menu with the following options:

Table 10-2 List of Sites Right-Click menu

| Menu Option | Description |
|----------------------|--|
| Categorize Selection | Perform a VCA run on the selected site. |
| Set Category | Manually set the category from the SurfControl Category list. |
| Uncheck Selection | Removes the Checked status from a site, which will then be checked again in a VCA run. |
| Go To HTTP: | Opens the selected site in a Web browser. |
| Find Site | Allows you to search for a URL in the List of Sites. |

VCA SETTINGS TAB

Figure 10-2 shows the VCA Settings tab:

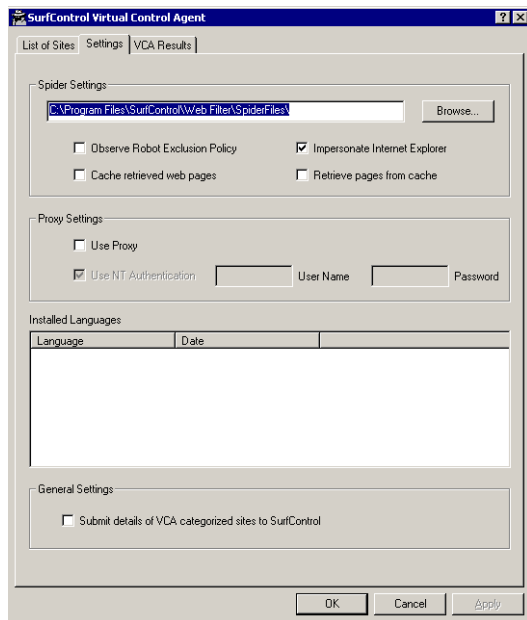


Figure 10-2 VCA Settings tab

Table 10-3 VCA Settings dialog box

| Field | Description |
|--------------------------------|---|
| Spider Settings | The location of the Spider Files. In a default installation the location will be: C:\Program Files\SurfControl\Web Filter\SpiderFiles Note: <i>This setting can also be changed via the VCA Control Panel application. See page 111 for more details.</i> |
| Observe Robot Exclusion Policy | Some sites contain a text file that describes exactly what each spider (or robot) can access on the site. If you choose to ignore this policy then the spider will try to access unauthorized areas on the site. This may result in your IP address being banned by the site. |
| Cache Retrieved Web Pages | Adds any pages directly retrieved during the VCA run to the local web page cache, if available. |
| Impersonate Internet Explorer | The VCA will identify itself as Internet Explorer when making requests to servers. If you clear this item the VCA will identify itself as SurfControl. Some sites are inaccessible unless you impersonate Internet Explorer. Alternatively, sites can also ignore requests that originate from Internet Explorer. This option is selected by default. |
| Retrieve pages from cache | Enables the VCA to use locally cached versions of pages of a site, rather than having to retrieve current versions from the Internet. |
| Use Proxy | Select this option, if you are using a Proxy server. |
| Use NT Authentication | Enables you to access the Proxy server as part of an NT Domain. This option is selected as default if the Proxy Server option is selected. |
| User Name & Password | Used if NT Authentication is not selected. |
| Installed Languages | Displays the languages that the VCA can categorize in. |
| General Settings | Select the Submit details of VCA categorized sites to SurfControl checkbox if you want to send your results to SurfControl's Content Team for analysis and possible inclusion in the SurfControl URL Category List. |

VCA RESULTS TAB

Figure 10-3 shows the VCA Results tab:

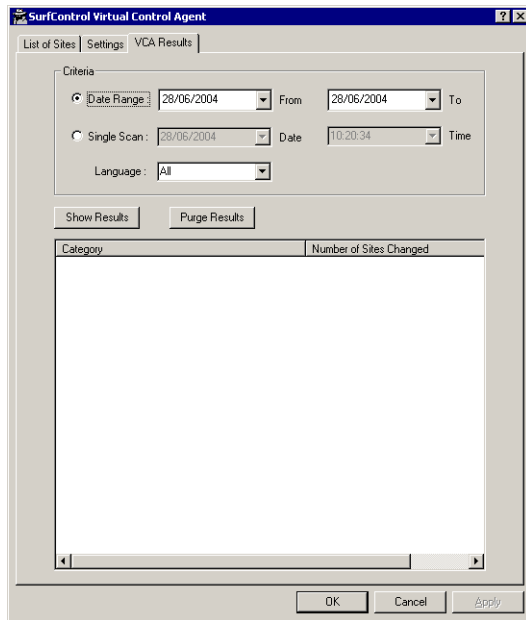

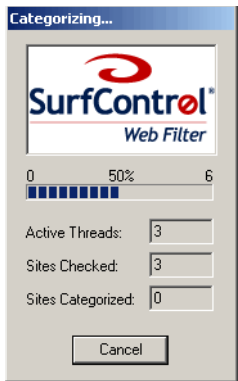
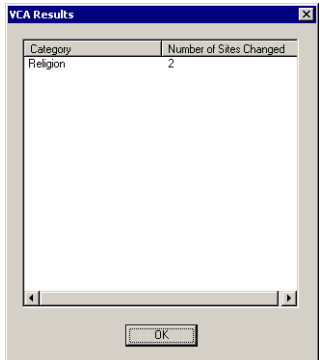
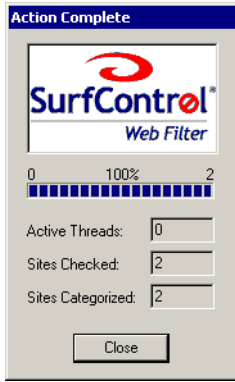


Figure 10-3 VCA Results tab

Table 10-4 VCA Results tab

| Field | Description |
|---------------|--|
| Date Range | Choose a From and To date to report on a range of days. |
| Single Scan | Select this option and choose a single date and a time to run a scan on from the drop-down list boxes. |
| Language | Choose a specific language to run reports on from the drop-down list box. This will return URL's in the language specified. The default setting is All. These are: <ul style="list-style-type: none"> • Dutch • English • French • German • Spanish |
| Show Results | Select this to view the results in the window below. |
| Purge Results | Removes the results from the window below. |

Procedure 10-1: Performing a VCA run

| Step | Action | |
|------|---|---|
| 1 | From the VCA List of Sites tab, click the Categorize all 'None' Sites button:  | |
| 2 | <p>A Categorizing dialog box will display with the following information:</p> <ul style="list-style-type: none"> • A Progress bar showing the number of 'None' sites being categorized on the right and the percentage of those sites processed. • Active Threads - the number of pages being categorized at any one time. You can limit the amount of active threads being used for this in the Virtual Control Agent Control Panel application. • Sites Checked - counts the number of sites checked during the VCA run. • Sites Categorized - the number of sites that have been categorized by the VCA during this run. <p>Click Cancel to stop the VCA run at any time.</p> |  |
| 3 | <p>On completion of the run a VCA Results dialog box displays showing the VCA categorized sites and the category to which they have been assigned.</p> <p>Click OK.</p> |  |
| 4 | <p>An Action Complete dialog box appears, confirming the number of sites checked and Categorized.</p> <p>Click Close.</p> |  |

THE VCA CONTROL PANEL APPLICATION

The VCA Control Panel application enables you to stop and start the VCA service, as in Figure 10-4. You can also configure the VCA settings as in Figure 10-5:

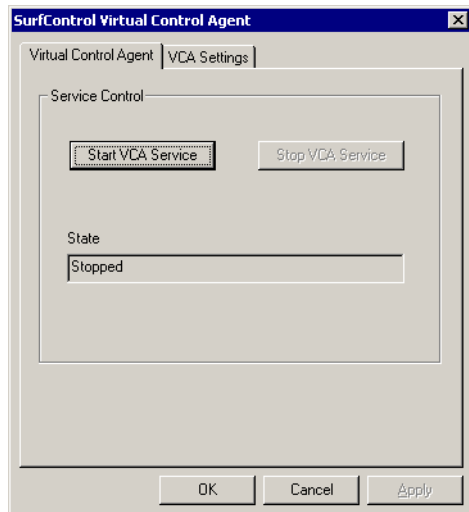


Figure 10-4 VCA Service Control tab



Warning: The VCA service does not function if you are using a 30 day evaluation version of Web Filter.

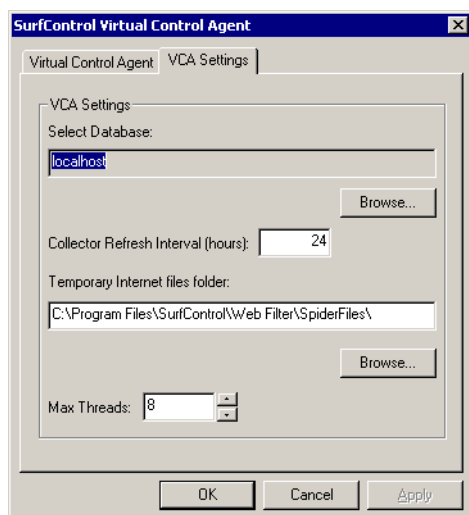


Figure 10-5 VCA Settings tab

Table 10-5 VCA Settings tab

| Field | Description |
|---------------------------------|--|
| Select Database | Select the database you want the VCA to save its categorizations to. |
| Collector Refresh Interval | You can configure the time in hours before the VCA will commit changes to the selected database and flush its cache. |
| Temporary Internet files folder | The VCA spiders will download up to 10 pages of a site it is categorizing. It downloads them to the folder specified in this field. By default this location is: C:\Program Files\SurfControl\Web Filter\SpiderFiles Once the spiders have finished categorizing the site, the pages are deleted from the folder. This setting can also be changed from within the VCA. See page 107 for more details. |
| Max Threads | This controls the maximum number of spiders that can be categorizing sites at any one time. The default number is 8. The maximum is 32. Increasing the number of spiders can use up your available bandwidth. For this reason SurfControl recommends you keep this setting at its default number. |



Chapter 11 Help Desk

| | |
|--------------------------|----------|
| Introduction | page 114 |
| Setting up the Help Desk | page 115 |
| Using the Help Desk | page 127 |

INTRODUCTION

The SurfControl Web Filter Help Desk allows an administrator to check the category of a URL in the URL Category List and, if necessary, re-categorize it.

The advantage of using the help desk is that the category changes can be made remotely from the Web Filter server.

HOW IT WORKS

A Web page connects to the Web Filter Database. You enter a URL and its current categorization is shown. You can then choose another category from a list. You then save and commit the changes back to the database.

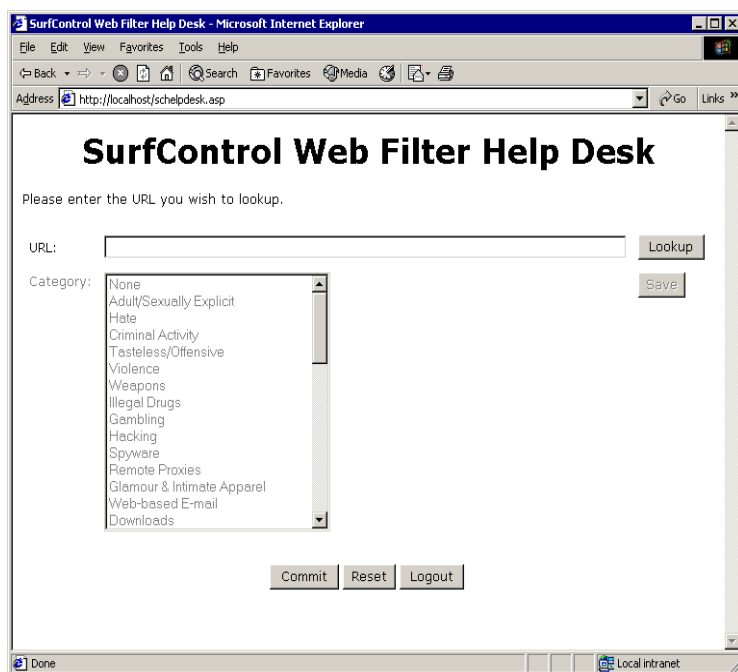


Figure 11-1 Web Filter Help Desk

SETTING UP THE HELP DESK

To set up the help desk you need to have Microsoft Internet Information Services (IIS) installed on the server.

To install IIS, follow Procedure 11-1:

| Procedure 11-1: Installing IIS | |
|--------------------------------|--|
| Action | Step |
| 1 | From the Control Panel, select Add or Remove Programs . |
| 2 | Click the Add/Remove Windows Components icon on the left hand side of the dialog box. |
| 3 | Select the Internet Information Services (IIS) check box |
| 4 | Click Next and follow the on-screen instructions. |

Once IIS is installed, you will note the following directory has been installed on your C: drive:

Inetpub

If you expand the Inetpub folder you will see a folder called **wwwroot**.

You need to copy the help desk Web page - **schelpdesk.asp** from the **Program Files > SurfControl > Web Filter > Tools** folder to the **wwwroot** folder.

If you want you can create a new folder under the wwwroot folder and copy the file to that location.

CONFIGURING IIS

IIS must be configured in a certain way to enable the help desk to work properly. The following settings apply to both IIS 5 and 6.

To configure IIS, select Internet Information Services from the **Programs > Administrative Tools > Internet Services Manager**. You can also access this via the Administrative Tools folder in the Control Panel. The Internet Information Services Manager opens as in Figure 11-2:

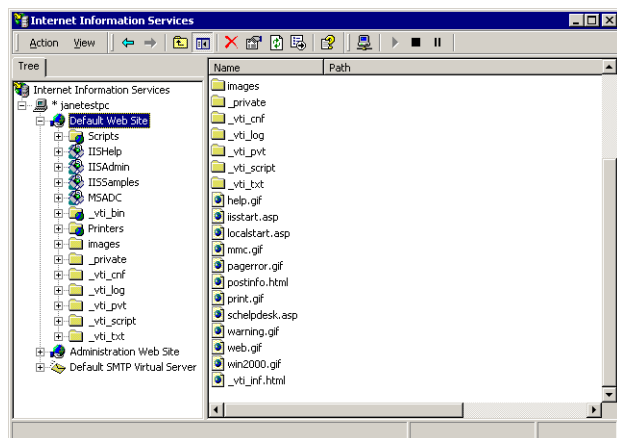


Figure 11-2 Internet Services Manager dialog box

If you expand the server you are logged on to in the left-hand column and select the Default Web Site, you will see the `schelpdesk.asp` file in the list of files and folders.

If you don't want to change the settings on the Default Web Site, you can create a new Virtual Directory, copy the help desk file to it and then configure that directory. See the IIS documentation for details on setting up a new Virtual Directory.

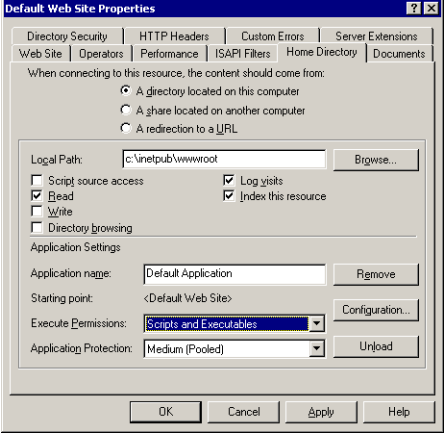
You must configure the Default Web Site in the following ways.

- Enable both scripts and executables to be run.
- Change the Directory Security Settings from Anonymous Access to Basic and Integrated Windows Authentication.

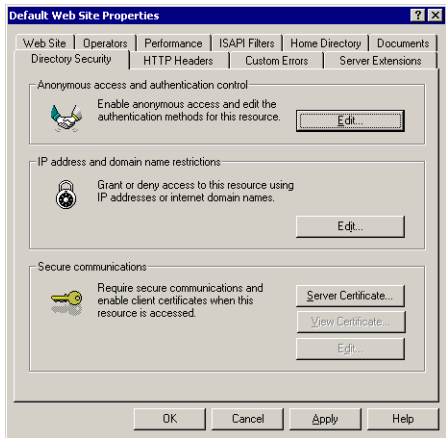
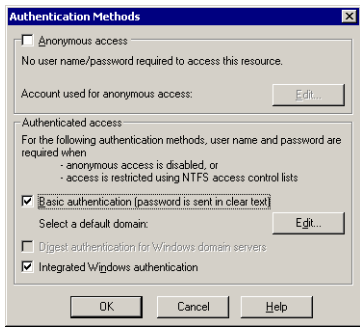
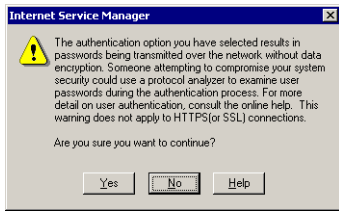
If you don't want to change the settings on the Default Web Site, you can create a new Virtual Directory, copy the help desk file to it and then configure that directory. See the IIS documentation for details on setting up a new Virtual Directory.

Procedures 11-2 and 11-3 assume you have used the Default Web Site.

Procedure 11-2: Run Scripts and Executables

| Step | Action | |
|------|--|--|
| 1 | Select the Default Web Site. Right-click and select Properties from the menu. The Properties dialog box for the Default Web Site appears. |  |
| 2 | Select the Home Directory tab. | |
| 3 | Select Scripts and Executables from the Execute Permissions drop-down list box. | |
| 4 | Click Apply . | |

Procedure 11-3: Change the Directory Security Settings

| Step | Action | |
|------|--|--|
| 1 | Select the Default Web Site. Right-click and select Properties from the menu. The Properties dialog box for the Default Web Site appears. |  |
| 2 | Select the Directory Security tab. | |
| 3 | Click the Anonymous and authentication control Edit button. An Authentication Methods dialog box appears. |  |
| 4 | Clear the Anonymous access check box. | |
| 5 | Select the Basic authentication check box. The following warning will appear. Click Yes to continue. |  |
| 6 | Ensure the Integrated Windows authentication check box is selected. | |
| 7 | Click OK . Click Apply . | |

OTHER CONFIGURATION CHANGES

There are three other configuration changes that you need to perform, depending whether you have IIS 5 (Windows 2000) or IIS 6 (Windows Server 2003) installed.

IIS 5 only

- The identity of the IIS user must be the same as the SurfControl Web Filter user. See Procedure 11-4.

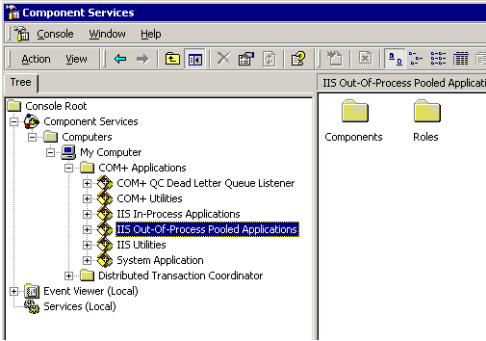
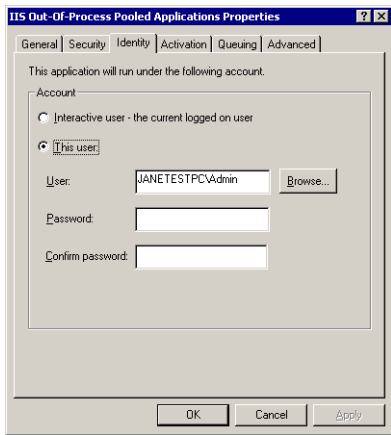
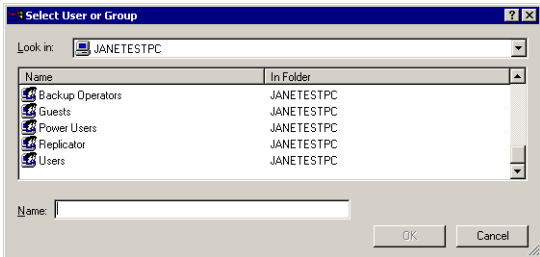
IIS 6 only

- Configure IIS to allow Active Server Pages (ASP) extensions. See Procedure 11-5.
- Set an Application name and Identity. See Procedure 11-6.

CREATING A DSN (IIS 5 & 6)

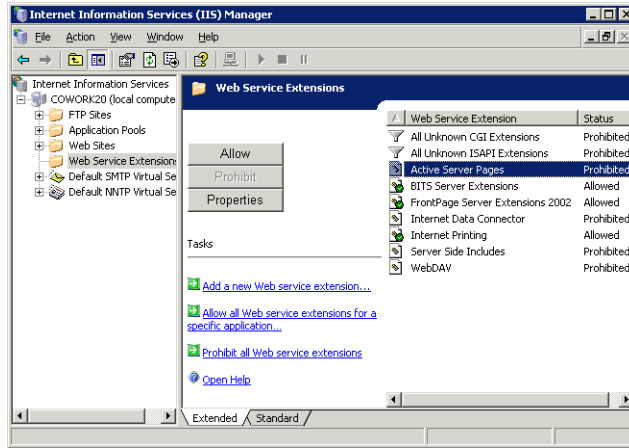
You need to create a DSN to connect to the SurfControl Web Filter database. See Procedure 11-7.

Procedure 11-4: Configure the identity of the IIS 5 user

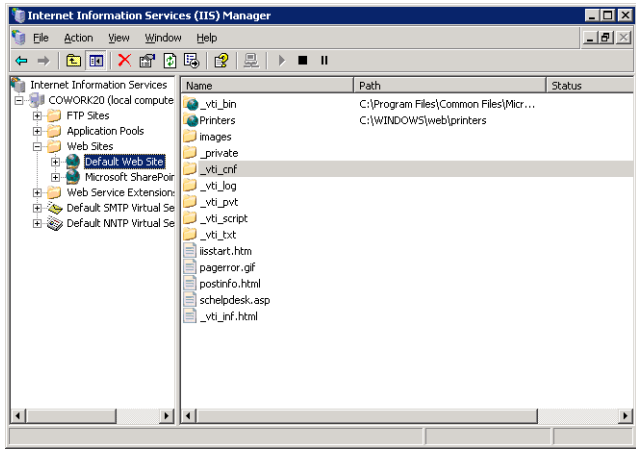
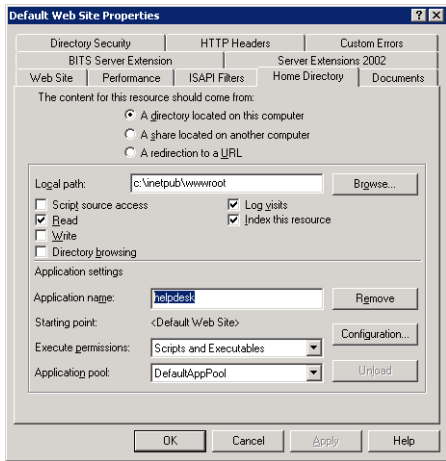
| Step | Action | |
|------|--|--|
| 1 | Select Component Services from the Programs > Administrative Tools menu. You can also access this via the Administrative Tools folder in the Control Panel. |  |
| 2 | Expand the Component Services, Computers, My Computer and COM+ Application folders. | |
| 3 | Select IIS Out-of-Process Pooled Applications from the COM+ Application folder and right-click. Select Properties from the menu. An IIS Out-of-Process Pooled Applications Properties dialog box appears. Click the Identity tab. |  |
| 4 | Select This User and Browse . A Select User or Group dialog box will appear. Select the User that also logs on as the Web Filter administrator. |  |
| 5 | Click OK . Click Apply . | |

Procedure 11-5: Configure IIS 6 to allow ASP extensions

| Step | Action |
|------|---|
| 1 | Select Internet Information Services from the Programs > Administrative Tools > Internet Services Manager . You can also access this via the Administrative Tools folder in the Control Panel. |
| 2 | Select the Web Service Extensions folder. |
| 3 | Select Active Server Pages . By default IIS 6 prohibits the use of ASP pages. You need to set the status to Allowed for the Help Desk to work. |
| 4 | Click Allow . |

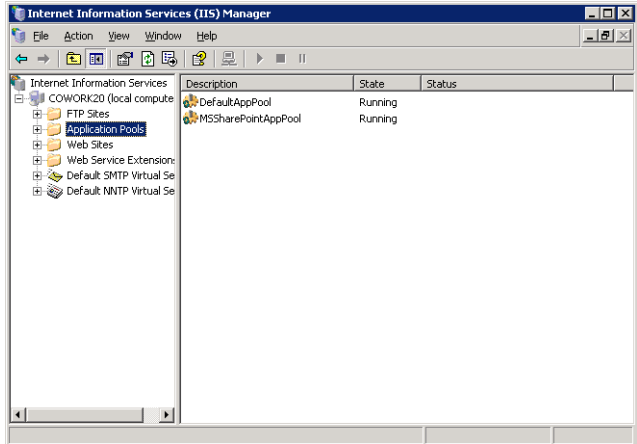
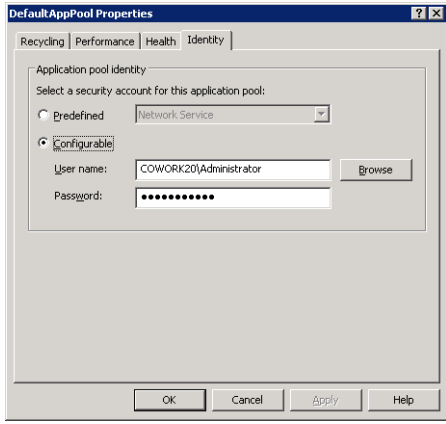


Procedure 11-6: Setting an Application name and Identity in IIS 6

| Step | Action | |
|------|---|--|
| 1 | Select Internet Information Services from the Programs > Administrative Tools > Internet Services Manager . You can also access this via the Administrative Tools folder in the Control Panel. | |
| 2 | Expand the Web Sites folder |  |
| 3 | Select the Default Web Site . From the right-click menu, select Properties . | |
| 4 | Select the Home Directory tab |  |
| 5 | Enter a name for the Help Desk in the Application name field. Ensure that Execute Permissions is set to Scripts and Executables (you should have done this already in Procedure 11-2). | |
| 6 | Click Apply . | |
| 7 | Click OK . | |

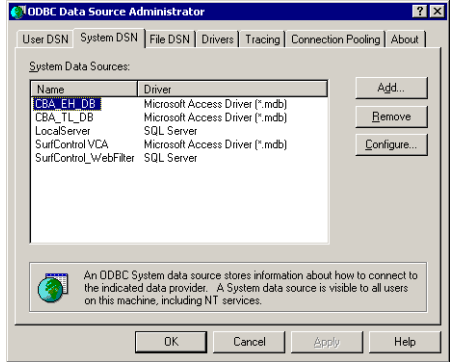
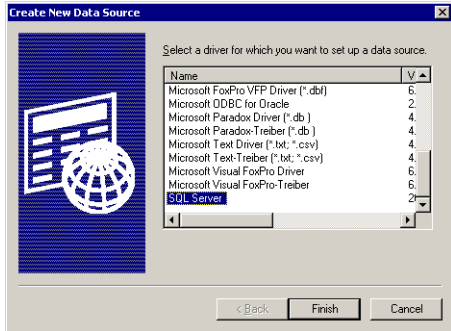
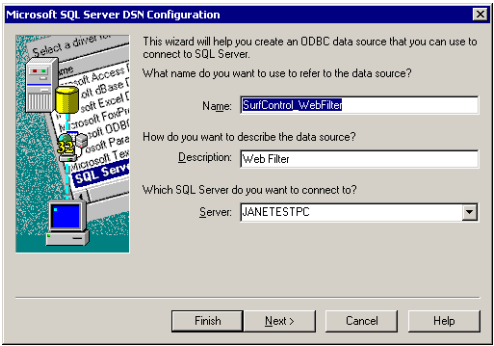
(Sheet 1 of 2)

Procedure 11-6: Setting an Application name and Identity in IIS 6

| Step | Action | | | | | | | | | | |
|---------------------|---|---|-------------|-------|--------|----------------|---------|--|---------------------|---------|--|
| 8 | From the main IIS screen, select the Application Pools folder. From the right-click menu, select Properties . |  <p>The screenshot shows the 'Internet Information Services (IIS) Manager' window. In the left-hand tree view, the 'Application Pools' folder is selected and highlighted. The main pane on the right shows a table of application pools:</p> <table border="1"> <thead> <tr> <th>Description</th> <th>State</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>DefaultAppPool</td> <td>Running</td> <td></td> </tr> <tr> <td>MSSharePointAppPool</td> <td>Running</td> <td></td> </tr> </tbody> </table> | Description | State | Status | DefaultAppPool | Running | | MSSharePointAppPool | Running | |
| Description | State | Status | | | | | | | | | |
| DefaultAppPool | Running | | | | | | | | | | |
| MSSharePointAppPool | Running | | | | | | | | | | |
| 9 | Select the Identity tab |  <p>The screenshot shows the 'DefaultAppPool Properties' dialog box with the 'Identity' tab selected. Under 'Application pool identity', the 'Configurable' radio button is selected. The 'User name' field contains 'COWORK20\Administrator' and the 'Password' field is masked with dots. There is a 'Browse' button next to the user name field.</p> | | | | | | | | | |
| 10 | Select Configurable and enter the user name and password of the Web Filter administrator. | | | | | | | | | | |
| 11 | Click Apply . Click OK . | | | | | | | | | | |

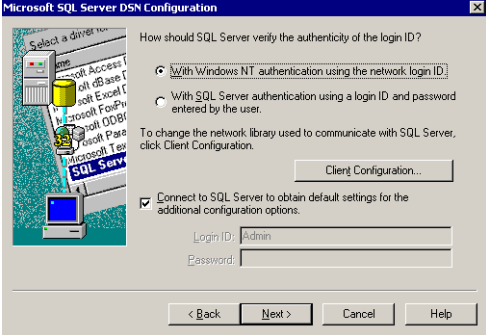
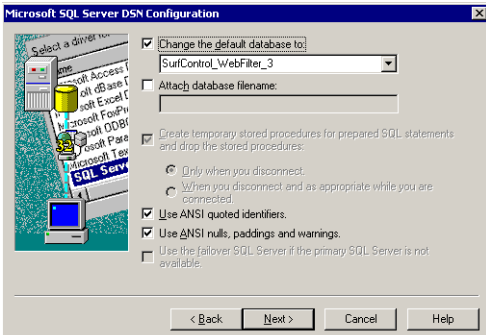
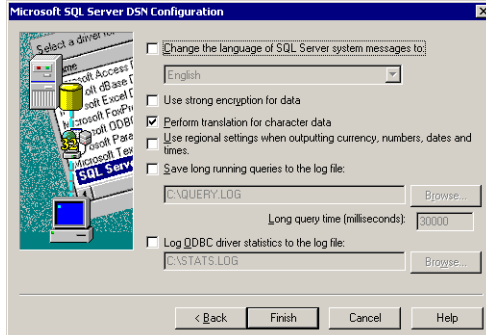
(Sheet 2 of 2)

Procedure 11-7: Create a DSN for the Help Desk (IIS 5 & 6)

| Step | Action | |
|------|---|--|
| 1 | Select Data Sources (ODBC) from the Programs > Administrative Tools menu. You can also access this via the Administrative Tools folder in the Control Panel. |  |
| 2 | Select the System DSN tab. | |
| 3 | Click Add . Select SQL Server from the list of available drivers. Click Finish . The wizard continues. |  |
| 4 | From the next screen enter the following information: <ul style="list-style-type: none"> • Name - a name for your DSN. • Description - brief details about your DSN. • Server - select the SQL server where your database is located. Click Next . |  |

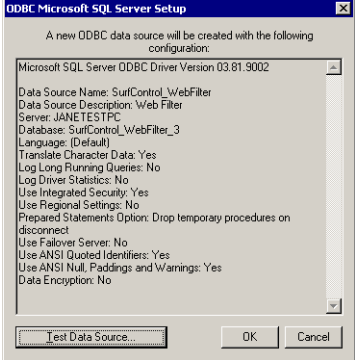
(Sheet 1 of 3)

Procedure 11-7: Create a DSN for the Help Desk (IIS 5 & 6)

| Step | Action | |
|------|---|--|
| 5 | <p>From the next screen in the wizard make sure the following authentication options are selected:</p> <ul style="list-style-type: none"> With Windows NT authentication using the network login ID. Connect to SQL Server to obtain default settings for the additional configuration options. <p>Click Next.</p> |  |
| 6 | <p>From the next screen, select the SurfControl database from the drop-down list box, ensuring the Change the default database to: check box is selected. The default SurfControl Web Filter database is called SurfControl_WebFilter. The other settings on this dialog box can be ignored.</p> <p>Click Next.</p> |  |
| 7 | <p>The final screen can remain unchanged.</p> <p>Click Finish.</p> |  |

(Sheet 2 of 3)

Procedure 11-7: Create a DSN for the Help Desk (IIS 5 & 6)

| Step | Action | |
|------|---|--|
| 8 | <p>You can now test your connection. If the test is unsuccessful, try to reconfigure your connection, checking the options you selected.</p> <p>If the test is successful, click OK.</p> |  |
| 9 | Your DSN connection is now available for use with the Help desk. | |

(Sheet 3 of 3)

USING THE HELP DESK

Assuming you have setup the help desk in the Default Web Site, and you are using the server you set the help desk application up on, open the page by typing the following address in your Web browser:

`http://localhost/schelpdesk.asp`

When using the help desk from a remote location, you will need to replace 'localhost' with the IP address of the server.

The following page will appear as in Figure 11-3:

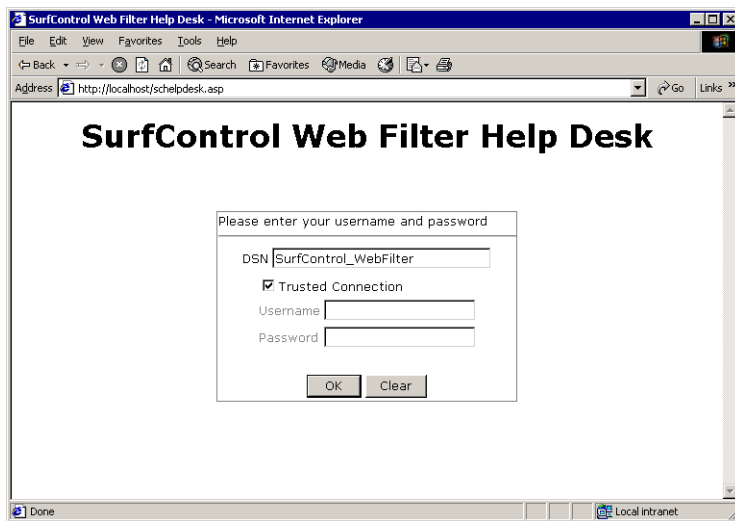


Figure 11-3 Help Desk login screen

You need to enter the DSN name you created in Procedure 11-5.

Click **OK**.

The Help Desk main page will appear as in Figure 11-4:

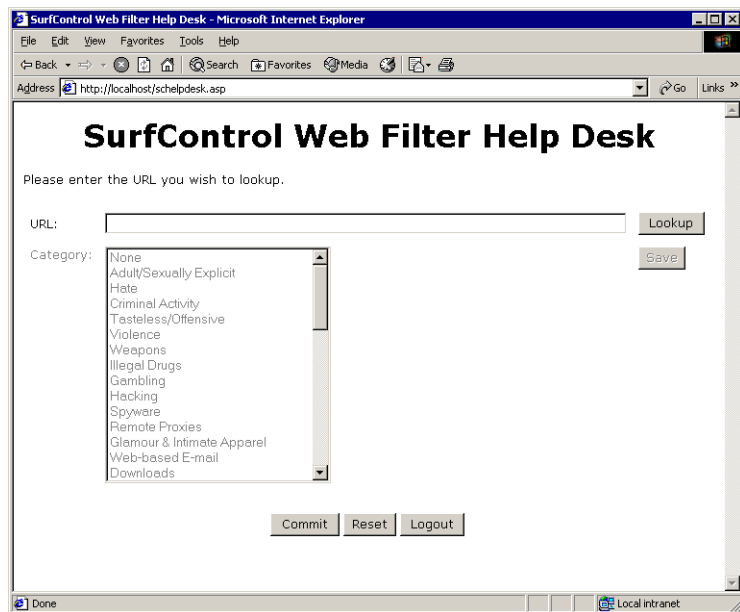


Figure 11-4 Help Desk main page

| Procedure 11-8: Re-categorizing a URL | |
|---------------------------------------|---|
| Step | Action |
| 1 | Type the URL in the URL field. Note: <i>Wildcard entries cannot be used.</i> |
| 2 | Click Lookup . The current category assigned to the URL will be highlighted in the Category list box. |
| 3 | Select the new category you want to assign to the URL. |
| 4 | Click Save . |
| 5 | If you have multiple URLs you want to change, repeat steps 1 to 4 for each URL. |
| 6 | After making all your changes, click Commit . This updates the URL Category List with your re-categorizations. |
| 7 | Click Logout to exit the help desk. |



Chapter 12 Troubleshooting

| | |
|--|-----------------|
| The Monitor | page 130 |
| All Editions | page 130 |
| The Monitor does not display traffic | page 130 |
| ("\") Appears in the Users Pane of the Monitor | page 132 |
| Databases | page 133 |
| Create SQL Database Utility Error Message | page 133 |
| Database Tools Fail with MSDE Database | page 133 |
| Report Central | page 136 |
| Uninstalling the JRE v1.4.2 | page 136 |
| VCA | page 136 |
| VCA results not shown in the Monitor | page 136 |

THE MONITOR

ALL EDITIONS

THE MONITOR DOES NOT DISPLAY TRAFFIC

CAUSE

This problem can occur for the following reason:

- You did not select Monitor all connections during installation.

RESOLUTION

If you did not select Monitor all connections:

- Re-install SurfControl Web Filter, or
- Edit the registry. (Note: The registry contains information vital to your system. SurfControl strongly recommends that only someone with registry experience edit the registry. For information from Microsoft on editing the Registry, consult Microsoft Knowledge Base article 322755 – How to Backup, Edit, and Restore the Registry in Windows 2000.)

- 1 Click **Start** and select **Run**.

- 2 Enter “regedit.”

- 3 Change the following registry key from 0x0 to 0x1:

```
HKEY_LOCAL_MACHINE / SOFTWARE/ JSB / surfCONTROL Scout /ProxyServerMonitoring
```

- 4 Change the following registry key from 0x0 to 0x1:

If Winsock Proxy is being used, enable **Access Control for Winsock Proxy**, and ensure specific **Access Control Groups** are empty. With **Access Control** selected in the Winsock Properties Permissions tab, ensure that no groups or users are in the following protocols' Access Control group lists:

- Unlimited Access.
- HTTP.
- HTTPS.
- FTP.

To Ensure that no groups or users are in these Access Control group lists:

- 1 Right click the SurfControl icon in the status area of the task bar and select Stop Web Filter Service from the menu.
- 2 Open the Proxy Management Console (MMC.)
- 3 Right-click Winsock/Web proxy access and select **Properties**.
- 4 Click **Permissions** to ensure that Access Control is enabled.
- 5 Make sure that no users or groups are listed in the Access Control Groups for any of the above protocols. If you see any users or groups in these Access Control Groups, remove them.



Note: In the Unlimited Access group, only the NT/System should be granted access. For all other protocols, grant access as needed by users or groups for client applications. Once this change is made, any service not using Web proxy will require protocol permissions to access the internet via Winsock Client.

- 6 Stop and re-start the Winsock Proxy service within the MMC.

("\\") APPEARS IN THE USERS PANE OF THE MONITOR

Cause

This can happen with the Enterprise User Monitor (EUM) for Windows 2000 domain controllers or Windows NT domains. In some cases, a log on event appears with a blank user name and domain value. Web Filter resolves this blank user name and domain value with a backslash ("\\") character.



Note: These log on events are NOT associated with a valid user.

Resolution

Configure SurfControl Web Filter to omit the backslash "user" from the Users pane.

To omit the backslash:

- 1 Open the `scua.ini` file located on each domain controller. By default, this file is located in `C:\SurfControl User Agent\`.
- 2 Create an `[ignored_users]` section at the end of the file (if one does not exist already).
- 3 Add the string `\=1`
- 4 **Save** and **close** the file.
- 5 If the Domain Controller is Windows 2000, reboot the Domain Controller. If the Domain Controller is Windows NT, go into the Services utility and re-start the SurfControl User Agent service.

To remove the backslash character's history in the Monitor:

- 1 Open the SurfControl Web Filter Monitor.
- 2 Locate the backslash in the User pane.
- 3 Highlight the backslash, right-click and select **Delete**.

DATABASES

CREATE SQL DATABASE UTILITY ERROR MESSAGE

Symptom

When you try to use the Create SQL Database utility in SurfControl Web Filter, you receive one of the following error messages:

CreateTables.exe – Unable to Locate DLL

or

The dynamic link library `ntwdblib.dll` could not be found

Cause

A client installation of SQL server must be installed on the SurfControl server. There is a tool (`ntwdblib.dll`) that is installed with the SQL server client application, and is necessary for the Create SQL Database utility.

Resolution

Install the client version of SQL server on the SurfControl server.

DATABASE TOOLS FAIL WITH MSDE DATABASE

Symptom

You are unable to archive, delete, or restore your MSDE database using SurfControl Web Filter's database tools, and you receive one of the following error messages:

Failed to delete database. Line 1: Incorrect syntax near (database name).

or

Error archiving database: SQL Server archive database failed.

Error archiving database: SQL Server archive database failed

Cause

This issue occurs when the name of your MSDE database does not conform to one of the following SQL naming conventions:

- The database starts with a number (for example, “10-1-03WebFilter”).
- The database starts with a non-alpha-numeric character (other than “_”).
- The database includes the word “unique,” or any other SQL-reserved word.

Resolution

If you have a licensed version of SQL on your network, use SQL Enterprise Manager to archive, restore, or delete the database.

Or, you can use the OSQL command line utility to:

- Archive the non-conforming database.
- Restore the database using a conforming database name.
- Delete the original database.

Procedure 12-1: Using the OSQL Utility

| Step | Action |
|------|---|
| 1 | Stop the Web Filter service. |
| 2 | Click Start and select Run . |
| 3 | Type "cmd." |
| 4 | <p>Enter one of the following MSDE commands:</p> <p>Note: <i>The command switches (i.e., -E, -P, -U) are case-sensitive.</i></p> <ul style="list-style-type: none"> • If you are using a trusted connection, type: <code>OSQL -E</code> • If you are using SQL authentication, type: <code>OSQL -Usa -Pabc123</code> <p>Where:</p> <ul style="list-style-type: none"> • "-U" and "-P" represent respective switches. • "sa" represents your SQL account. • "abc123" represents your SQL account password. |
| 5 | Archive, restore, and delete a database using one of the following commands, making sure that (1) brackets (" []") are included in the command, and (2) your restored database conforms to the SQL naming standards noted above. |
| 6 | <p>To archive your non-conforming database, type:</p> <pre>Backup database [database name] to disk = 'c:\backup\new_database_name.bak'</pre> <p>Then</p> <p>Go</p> <p>If no path is specified, the default is "winnt\system32." Quotes are required around the path and/or backup database file name.</p> |

(Sheet 1 of 2)

Procedure 12-1: Using the OSQL Utility (Continued)

| Step | Action |
|------|---|
| 7 | <p>To restore your database and re-name it in accordance with SQL naming standards, type:</p> <pre>Use master restore database new_database_name = 'c:\backup\database_name.bak' with replace</pre> <p>Then</p> <p>Go</p> <p>Replace "new_database_name" with a name that adheres to SQL naming standards.</p> <p>If no path is specified, the default is "winnt\system32." Quotes are required around the path and/or backup database file name.</p> <p>Note: <i>Include brackets around the database name only if the name does not adhere to SQL naming standards</i></p> |
| 8 | <p>To delete your original database, type:</p> <pre>Drop database [database_name]</pre> <p>Then</p> <p>Go</p> |
| 9 | <p>After completing this process, you will be able to use the SurfControl Database Management utility to archive, restore, or delete your database.</p> |

(Sheet 2 of 2)

REPORT CENTRAL

UNINSTALLING THE JRE v1.4.2

Symptom

Having un-installed the Java 2 Runtime Environment (JRE) via Add Remove Programs in the Control Panel, Selecting Repair from the SurfControl Report Central setup does not re-install the JRE.

Resolution

You have two options:

- 1 Uninstall SurfControl Report Central and then re-install.
- 2 Download and install the JRE from the following location:

<http://java.sun.com/j2se/1.4.2/download.html>

VCA

VCA RESULTS NOT SHOWN IN THE MONITOR

Symptom

The Web Filter Monitor does not display VCA categorized sites in the Monitor.

Cause

You are monitoring the server where the VCA is installed.

Resolution

Stop monitoring the VCA server.

Procedure 12-2: Stop monitoring VCA Server - Windows Edition

| Step | Action |
|------|--|
| 1 | Double-click the SurfControl Web Filter icon in the task bar. Stop the Web Filter Service. |
| 2 | Select the Subnets tab. |
| 3 | In the Subnets Settings section, click Add . |
| 4 | Enter the IP address of the VCA server. |
| 5 | Enter 255.255.255.255 as the subnet mask. |
| 6 | Click OK . |
| 7 | Make sure Monitor Everything Except These Subnets is selected. |
| 8 | Click OK . |



Appendix A

Custom Reports
Table details

page 140
page 141

CUSTOM REPORTS

Using SQL queries you can create custom reports from your database. A reporting utility is required to compile custom reports. SurfControl recommends Crystal Reports V8. To create custom reports you will need to re-create the database schema in Figure 1:

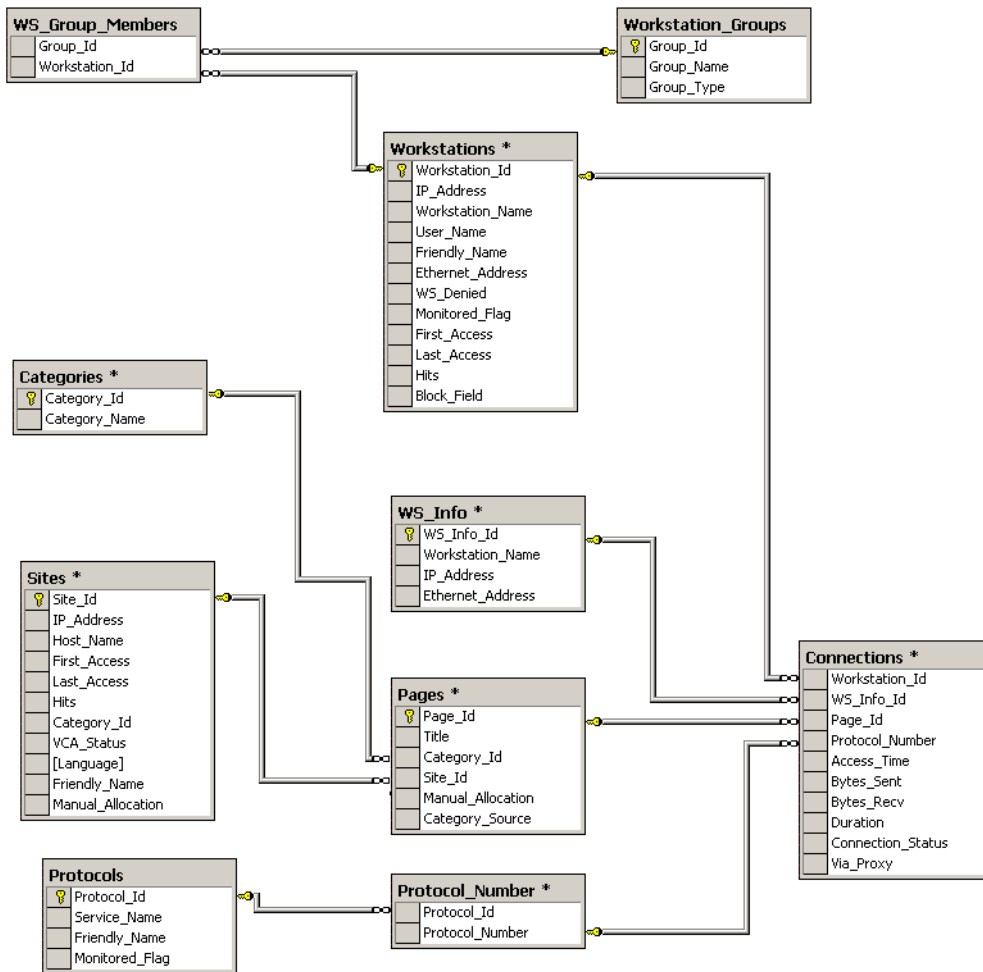


Figure 1-1 Custom Reports database schema

TABLE DETAILS

The tables comprising the schema are as follows:

- Categories - see page 142.
- Connections - see page 142.
- Pages - see page 142.
- Protocols - see page 144.
- Protocol_Number - see page 144.
- Sites - see page 145.
- Workstations - see page page 145.
- Workstation_Groups - see page page 147.
- WS_Group_Members - see page 147.
- WS_Info - see page 147.

APPENDIX A

Table details

CATEGORIES

Table 1-1 Categories table

| Field | Data Type | Example | Description |
|---------------|--------------|-------------------------|----------------------------|
| Category_ID | Integer | 9 | ID number of the category. |
| Category_Name | Varchar (70) | Adult/Sexually Explicit | Name of the category. |

CONNECTIONS

Table 1-2 Connections table

| Field | Data Type | Example | Description |
|-------------------|-----------|-----------------------|--|
| Access_Time | Date/Time | 26/05/1999 3:53:32 | Date & Time of connection. |
| Bytes_Recv * | Integer | 2068 | Number of bytes received. |
| Bytes_Sent * | Integer | 563 | Number of bytes sent. |
| Connection_Status | Integer | 0 or 1 or 2 | Status of the connection: 0 = Allowed. 1 = Override. 2 = Blocked. |
| Duration | Integer | 10 | Length of connection time in seconds. |
| Page_ID | Integer | 5 | ID of Web page or file accessed or downloaded during the connection. |
| Protocol_Number | Integer | 8 | number of protocol being used. |
| Via_Proxy | Bit | 0 | How connection is made: 0 = Direct. 1 = Via Proxy. |
| Workstation_ID | Integer | 1 | ID number of user making request. |
| Ws_info_id | Integer | 1 | ID number of workstation. |

* These fields are not used in this release and will always return a value of zero.

PAGES

Table 1-3 Pages table

| Field | Data Type | Example | Description |
|-------------|-----------|---------|-----------------------------|
| Category_ID | Integer | 1 | ID of SurfControl category. |

Table 1-3 Pages table

| Field | Data Type | Example | Description |
|-------------------|---------------|---------|--|
| Manual_Allocation | Integer | 1 | ID if site categorized manually or by VCA: 1 = re-categorized. 0 = not re-categorized. |
| Page_ID | Integer | 1 | ID number of requested page. |
| Title | Varchar (255) | a | Title of requested page. |
| Site_ID | Integer | 1 | ID of requested site. |

APPENDIX A

Table details

PROTOCOLS

Table 1-4 Protocols table

| Field | Data Type | Example | Description |
|----------------|---------------|---------|--|
| Friendly_Name | Varchar (100) | HTTP | 'Friendly' name of protocol. |
| Monitored_Flag | Integer | 0 or 1 | indicates whether protocol monitored or not: 0 = monitored. 1 = not monitored. |
| Protocol_ID | Integer | 1 | ID of requested protocol. |
| Service_Name | Varchar (50) | HTTP | Protocol name. |

PROTOCOL_NUMBER

Table 1-5 Protocol_Number table

| Field | Data Type | Example | Description |
|-----------------|-----------|---------|-------------------------------|
| Protocol_ID | Integer | 1 | ID of requested protocol. |
| Protocol_Number | Integer | 80 | Port number used by protocol. |

SITES

Table 1-6 Sites table

| Field | Data Type | Example | Description |
|-------------------|--------------|---------------------|--|
| Category_ID | Integer | 4 | ID of SurfControl category. |
| First_Access | Date/Time | 02/07/2001 3:53:32 | Date & time site first accessed. |
| Friendly_Name | Varchar (70) | www.surfcontrol.com | 'Friendly' name of site. |
| Sites_ID | Integer | 1 | ID of site. |
| Hits | Integer | 3 | Number of times page requested. |
| Host_Name | Varchar (70) | www.surfcontrol.com | Host name of site. |
| IP_Address | Varchar (15) | 208.1.9.11 | IP address of site. |
| [Language] | Varchar (50) | Dutch | Language of site. |
| Manual_Allocation | Integer | 0 | ID if site categorized manually or by VCA: 1 = re-categorized. 0 = not re-categorized. |
| Last_Access | Date/Time | 02/07/2001 3:53:32 | Date & time site last requested. |
| VCA_Status | Integer | 1 | Whether site has been checked by VCA: 0 = Unchecked. 1 = Checked. |

WORKSTATIONS

Table 1-7 Workstations table

| Field | Data Type | Example | Description |
|--------------------|---------------|--------------------|--|
| Block_Field | Integer | 0, 1, 2 or 3 | How workstation is blocked: 0 = Global Default. 1 = Workshop name. 2 = IP address. 3 = Ethernet address. |
| Ethernet_Address * | Varchar (25) | 123456789ABC | Ethernet address of last used workstation |
| First_Access | Date/Time | 02/07/2001 3:53:32 | Date & time user first accessed the Internet. |
| Friendly_Name | Varchar (250) | "John Smith" | 'Friendly' name of user. |

APPENDIX A

Table details

Table 1-7 Workstations table (Continued)

| Field | Data Type | Example | Description |
|------------------|---------------|-----------------------|---|
| Hits | Integer | 54 | Number of times workstation accessed the Internet. |
| IP_Address | Varchar (255) | 127.0.0.1 | IP address of last user to connect to the Internet. |
| Last_Access | Date/Time | 02/07/2001 3:53:32 | Date & time user last accessed the Internet. |
| Monitored_Flag | Integer | 0 or 1 | The audit level of the user. |
| User_Name | Varchar (250) | QACOM1\john | Network name of user. |
| Workstation_ID | Integer | 1 | ID number of user making request. |
| Workstation_Name | Varchar (255) | jspc.example.com | Name of last user to connect to the Internet. |
| WS_Denied | Integer | 0 or 1 | Not used. |

WORKSTATION_GROUPS

Table 1-8 Workstation_Groups table

| Field | Data Type | Example | Description |
|------------|---------------|-----------|--|
| Group_ID | Integer | 1 | ID of the user group. |
| Group_Name | Varchar (250) | Everybody | Name of the user group. |
| Group_Type | Integer | 1 | Type of group: 0= Web Filter defined group. 1 = Network Group. |

WORKSTATION_GROUP_MEMBERS

Table 1-9 Workstation_Group_Members table

| Field | Data Type | Example | Description |
|----------------|-----------|---------|-----------------------------------|
| Group_ID | Integer | 1 | ID of the user group. |
| Workstation_ID | Integer | 1 | ID number of user making request. |

WS_INFO

Table 1-10 WS_Info table

| Field | Data Type | Example | Description |
|--------------------|---------------|------------------|--|
| WS_Info_Id | Integer | 1 | ID of the workstation. |
| Workstation_Name | Varchar (255) | jspc.example.com | Name of last workstation to connect to the Internet. |
| IP_Address | Varchar (15) | 1 | Workstation IP address. |
| Ethernet_Address * | Varchar (25) | 123456789ABC | Workstation's ethernet address. |

* These fields are not used in this release and will always return a value of zero.

APPENDIX A
Table details

Index

A

- Add new Protocol 49
- Allowance Objects
 - 30 Minute Time Object 85
 - Browse Time Sensitivity 86
- Archiving a database 22

B

- Browse Time Sensitivity
 - Continuous browsing 86
 - Stand-alone browsing 86

C

- Category Object
 - Custom Categories 78
 - Set Category Object Order 79
 - SurfControl Categories 77
- Change the Manager/Union password 33
- Changing Rules Administrator Database 92
- Changing Web Filter Database 9
- Compacting a database 23
- Create a new SQL Database 27
- Creating new Rule Object 66
- Custom File Types and Extensions 52
- Custom Report Tables
 - Categories 142
 - Connections 142
 - Pages 142
 - Protocol_Number 144
 - Protocols 144
 - Sites 145
 - Workstation_Group_Members 147
 - Workstation_Groups 147
 - Workstations 145
 - WS_Info 147

D

- Database Management
 - Archive 22
 - Compact 23
 - Create a new SQL Database 26
 - Delete 24
 - Purge 21
 - Restore 25
- Default audit level 53
- Deleting a database 24

F

- Flat Files
 - Manual Update 28

H

- Heartbeat Interval 10
- Help desk
 - Change the Directory Security Settings 118
 - Configure IIS 6 to allow ASP extensions 121
 - Configure the identity of the IIS 5 user 120
 - Configuring IIS 116
 - Create a DSN for the Help Desk (IIS 5 & 6) 124
 - Installing IIS 115
 - Re-categorizing a URL 128
 - Setting an Application name and Identity in IIS 6 122
- HTTP Deny Page Objects
 - Constructing HTTP Deny Pages 91
 - Default 89
 - Other HTTP Deny Page objects 91

I

- Ignoring Users 50

L

- Licensing
 - Mobile Filter 18
 - Web Filter 18

INDEX

M

- Manual database update 28
- Mobile Filter
 - Databases 28
- Monitor
 - Ignoring sites in 48
 - Opening 36
 - Privacy Edition Features 37
 - Search facility 44
 - Sites Panel 39
 - Users Panel 37
 - View a different database 55
- Monitor to Database
 - Automatic 5
 - Manual 5
 - Database Updater tool 5
 - Scheduled Event 5
- Monitored File Types 51
- Monitoring Specific Protocols 48

N

- Network Groups 46
- Notify Objects
 - Notification File Types 88

O

- OSQL tool 134

P

- Performing VCA run 110
- Privacy Edition
 - Changes to Monitor 32
 - Changes to Real-Time Monitor 32
 - Changes to Reports 32
 - Features 33
 - Viewing User Details 34
- Purging a database 21

R

- Real-Time Monitor
 - Collector Details 61
 - Options 59
- Remote Service Control
 - Open 15
 - Options 15
- Remotely accessing another server 15
- Restoring an archived database 25
- Rule creation 65
- Rule Types
 - Allow 64
 - Allowance 64
 - Disallow 64
- Rules Administrator
 - Open 64

S

- Scheduled Events
 - Archive 98
 - Compact 98
 - Database Management 96
 - Database Update 99
 - Network Group Updates 100
 - Purge 97
 - URL Category List 95
- Scheduler
 - Open 94
 - Options 101
- Setting Default Audit Level 51
- Setting up Groups Assigning Users 45
- SmartScan 6, 78
- SQL Server Client Connectivity Pack 26
- Submit site to SurfControl 43
- SurfControl icon 2

T

- Troubleshooting
 - Databases 133
 - Report Central 136
 - The Monitor 130
 - VCA 136

U

- User Groups 45
- User Site Detail 41
- User Specific Audit Levels 53
- Username resolution
 - NetBIOS queries 6

V

VCA

- Control Panel application 111
- List of Sites tab 105
- Results tab 109
- Settings tab 107

W

Web Filter Service

Advanced

- Categorization Settings 6
- Monitor to Database 5
- TCP/IP Name Resolution
6

Current Database settings 8

E-mail Notification

- Catch up mode notifications 7
- Scheduled task failures 7
- Service status changes 7
- URL Category List License reminders 7

Open 2

Real-Time Monitor

- Heartbeat Interval 10
- Maximum Clients 10
- Port Number 10
- Timeout 10

Start/Stop Service 4

When Objects

- After work 82
- Weekends 83
- Worktime 84

Where Objects

- Categories 72
- Category Object 77
- Hosts and Domains 73
- Monitored Sites 72
- Precise Bandwidth Controls Object 76
- Protocols/Ports Object 75
- Subnet Object 74
- SurfControl Categories 77
- User Defined Where Objects 72
- Where Lists 72, 80

Who Objects

- AD, NT, NetWare Domain 67
- Hosts and Domains 69
- Subnet Object 70
- User-defined Who Objects 68
- Who List Objects 71

INDEX