



Internet

SurfControl Mobile Filter
Administrator's Guide

NOTICES

Copyright © 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.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

This product contains work based on the wvWare program, which is licensed under the Free Software Foundation General Public License.

This product incorporates code from GoAhead Software Inc., Copyright 2003 GoAhead Software, Inc. All Rights Reserved.

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.

COMMENTS ON THIS GUIDE?

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

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

April 2005

TECHNICAL SUPPORT

- For the latest support information on SurfControl products, visit <http://www.surfcontrol.com/support>
- Read the Top Issues - This page has a quick list that covers the most common support issues with the SurfControl products. If your problem is here, you will have an immediate answer.
- Search our Knowledge Base - our new, constantly updated Knowledge Base contains articles, FAQs and glossary items to answer your questions about all SurfControl products.
- If your question or problem cannot be answered by the Top Issues or is not in the Knowledge Base, fill out an Online Support Request Form
- Telephone Support - If you would like to speak with a Technical Support Representative, our excellent SurfControl Technical Support is just a phone call away.

SURFCONTROL SALES

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

<http://www.surfcontrol.com>

CONTENTS

Notices	i
Comments on this Guide?	i
Technical Support	ii
SurfControl Sales	ii
Contents	iii

MOBILE FILTER

Introduction	2
Mobile Administrator	2
Administrator Menus	4
Filtering details	6
Selecting clients.....	6
Offline Action.....	6
Offline action issues.....	7
Dealing with unfiltered ports	7
Setting filtering sensitivity	8
User name.....	9
Host name	10
Server Settings	11
New client defaults	12
Navigating around the Mobile Administrator	13
Filter Settings	14
Setting filtering action.....	14
Ports that can be filtered.....	14
Ports that can be monitored.....	14
Filtering Status.....	15
Client Status Icons	16
Client properties	17

Contents



Chapter 1

Mobile Filter

"Introduction"	page 2
"Administrator Menus"	page 4
"Filtering details"	page 6
"Filter Settings"	page 14
"Client Status Icons"	page 16
"Client properties"	page 17

INTRODUCTION

This guide describes the features of the SurfControl Mobile Filter Administrator and how it manages the devices you have installed the Mobile Filter client software on.

For setting up rules that apply to Mobile Filter clients see Chapter 8 - Rules Administrator of the Web Filter Administrators Guide. Mobile Filter users and hosts can be selected from the Who objects tab.

MOBILE ADMINISTRATOR

The Mobile Administrator (see Figure 1-1) is the main management point for your SurfControl Mobile Filter clients. It contains a configurable description of each remote device with its settings. Once you can see your clients within the Mobile Administrator you can edit their filter settings:

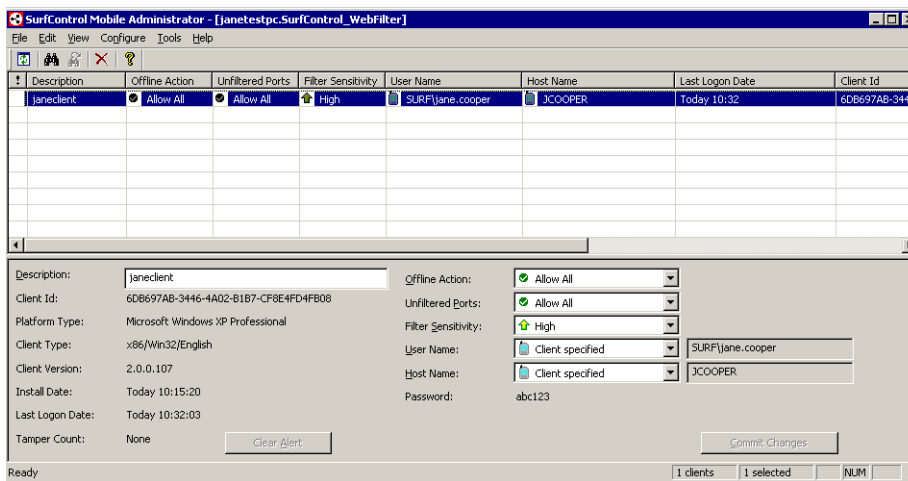


Figure 1-1 Mobile Filter Administrator

Select an individual client in the top pane of the Administrator. It's details will appear in the bottom pane.



Note: When you select multiple clients the only details that will appear in the bottom pane are those that are common to each client.

You can also select both continuous and non-continuous ranges of clients using either the SHIFT or CTRL key.

To make it easier to identify your clients, it is recommended that you put in a brief description of each one. The initial description in this field is the one that was added during the installation of the client. Beneath the 'Description' text box there is a list of properties relating to the client (see Table 1-1). These are specified by the client and cannot be edited in the Mobile Administrator:

Table 1-1 Mobile Administrator fields

Field	Description
Client ID	Unique ID that helps locate a specific client installation. This ID is also visible in the client. See "Client properties" on page 17 for more details.
Platform Type	The client operating system. It is useful when locating and/or grouping installations.
Client Type	Identifies the Processor, Operating System Description and Language variant of a Mobile Filter client.
Client Version	Identifies the version number of the Mobile Filter client and indicates whether an upgrade is available.
Install Date	Date on which the Mobile Filter client software was installed on the selected device.
Last Logon Date	Date the client last made an Internet request that was logged by the Mobile Administrator.
Tamper Count	Should the client detect an unauthorized change to any of the offline log files, it will increase the tamper count when the log files are deleted. At the same time, it will inform the Mobile Filter server that the logs have experienced some tampering and may not be correct.
Password	Password that was supplied during the client's installation process and is required if you uninstall the client.

ADMINISTRATOR MENUS

The following menu options are available in the Mobile Filter Administrator:

File

- **Open...** - open a database of Mobile Filter clients to be administered by the Mobile Administrator. Only Mobile Filter compatible databases can be opened in the Administrator.
- **Exit** - close the Mobile Administrator.

Edit

- **Find** - use a keyword search to locate particular clients. See “Navigating around the Mobile Administrator” on page 13 for further details.
- **Find Next** - find the next Mobile Filter client that matches the search criteria. See “Navigating around the Mobile Administrator” on page 13 for further details.
- **Select All** - selects all clients in the Administrator.
- **Invert Selection** - reverses the selection status of the clients in the Administrator. For example if clients 2, 4 and 6 are selected and 1, 3 and 5 are not, selecting Invert Selection will deselect clients 2, 4 and 6 and select clients 1, 3 and 5.
- **Delete Client** - remove the client from the Mobile Administrator and prevents that client from using the Mobile Filter Server.

View

- **Toolbar** - show or hide the Mobile Filter toolbar buttons.
- **Status bar** - show or hide the status bar.
- **Columns** - this menu contains two sub-menus:
 - **Reset Positions** - if you have moved columns to different places in the table select this to restore all columns to their original positions.
 - **Reset Width** - restores the column widths to their default setting.
- **Refresh** - update the information in the Mobile Administrator by refreshing the details.

Tools

- **Password Bypass Generator** - enables you to still uninstall the client should the password not be accepted when you try to uninstall the client. See the Troubleshooting section for more details.

Configure

- **Server Settings** - enables you to specify whether the Mobile Filter server is accepting new clients, and what the global default user name and host name are. You can also set the number of concurrent client sessions available for uploading of log files after a period of offline action. See “Offline action issues” on page 7, for more details.
- **New Client Defaults** - configure the settings that were initially given to a Mobile Filter client as it was installed. These default settings will include:
 - Offline Action.
 - Unfiltered Ports action.
 - Filter Sensitivity.
 - User Name setting.
 - Host Name setting.
- **Client Upgrade Details** - specify whether there is an upgrade available for Mobile Filter clients. See ‘The Mobile Filter client - Upgrading your Mobile Filter clients’ in the Installation Guide for more details.
- **Corporate Web Filters** - enables you to specify the location and scope of your corporate Web Filter installations. See ‘Corporate Web Filters’ in the Installation Guide for more information.

Help

- **About SurfControl Mobile Administrator** - the About box containing information such as the version number of the Mobile Filter installation, the name of the category database and how many days are left on your subscription.

FILTERING DETAILS

SELECTING CLIENTS

You can select client individually or in multiples, using the SHIFT or CTRL key.

- Click the **Find First** button to find one client of a particular type.
- Click the **Find All** button to find a group of clients of a particular type.

When selecting multiple client the property panel at the bottom of the Administrator shows values that are consistent between the selected clients.

Procedure 1-1: Changing the properties of multiple clients

Step	Action
1	Select the clients that need changing.
2	Change the properties in the Properties panel and click the Commit Changes button.

OFFLINE ACTION

There may be times when the Mobile Filter server is not available to the client, perhaps because of connection difficulties or maintenance. When this happens the client will try to contact the server on a regular basis (every five minutes) while connected to the Internet, until it can re-connect to the server. If the server is busy this can take between ten to sixty minutes. While the server is unavailable the client will be unable to send Web requests to the server for categorization so must deal with these requests itself. The client can be set to perform any of the following:

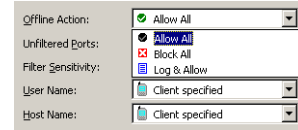
- **Allow All** - every Web request will be allowed (the default).
- **Block All** -every Web request will be blocked.
- **Log & Allow** - every Web request will be allowed but each request will be written to a log file. The Mobile Filter client will indicate to the end user their filtering status so the user of the filtered device could be aware when their activity is being logged but not filtered. However, any attempt by the user to delete any of these log files will be detected. See the next section, 'Offline Action Issues' for more information.

Procedure 1-2: Setting offline action

Step	Action
1	Open the Administrator and select the client/s that you want to set the filtering level for.

Procedure 1-2: Setting offline action

Step	Action
2	Click the arrow on the Offline Action: list to expand it:
3	Choose the type of Offline Action that you require, from the list.
4	Click Commit Changes to add the new Offline Action setting to the client in the Mobile Filter client Administrator.



OFFLINE ACTION ISSUES

When a server is offline the client repeatedly polls the server until it can re-connect to it. As soon as the client establishes a successful connection, any offline logs are sent to the Mobile Filter server.

This is a good way to keep a record of users' activities while the server is unavailable but it can cause problems if too many clients attempt to upload their log files at one time. To stop this from happening the Server Settings dialog box can be edited. 'Maximum concurrent client sessions' enables you limit the number of clients that can upload their log files at any one time. See "Server Settings" on page 11 for more information.

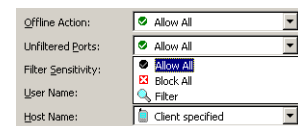
DEALING WITH UNFILTERED PORTS

Filtering of ports depends on what rules you have created and what ports are available to be monitored. There are three ways in which these unknown ports can be dealt with:

- **Allow All** - allow access to all unfiltered ports without contacting the Mobile Filter server to see if there is a rule set up for the port (this is the default).
- **Block All** - block access to any unfiltered ports without contacting the Mobile Filter server to see if there is a rule set up for the port.
- **Filter** - contact the Mobile Filter Server to see if any rules are set to apply to all ports.

Procedure 1-3: Setting unfiltered port action

Step	Action
1	Open the Mobile Administrator and select the client/s that you want to set the filtering level for.
2	Click the arrow on the Unfiltered ports: list to expand it:



Procedure 1-3: Setting unfiltered port action

Step	Action
3	Choose the type of action that you require for unfiltered ports, from the list.
4	Click Commit Changes to save the new Unfiltered Ports: setting.

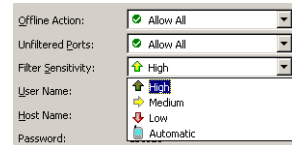
SETTING FILTERING SENSITIVITY

Filtering sensitivity enables you to set how much filtering is carried out by Mobile Filter clients. Reducing the level of filtering can speed up performance on slow connections, but of course at the same time less traffic is filtered. Priority can be assigned on four levels:

- **High** - all non-HTTP ports and all HTTP requests are categorized. There may be a performance impact if the client is making a lot of requests on a slow internet connection.
- **Medium** - all non-HTTP ports are categorized but only HTTP page requests are categorized while Images/sounds/style sheets, and XML requests are not categorized.
- **Low** - all non-HTTP ports are categorized. For HTTP requests, the URL will be categorized and, if allowed the domain level part of the URL is cached for 3 minutes. There is a potential loophole with this setting. Please see “Loophole with Low Filtering Sensitivity” in Chapter 12 - Troubleshooting for more information.
- **Automatic** - the client chooses High, Medium or Low based on the average Mobile Filter server response times and pre-configured thresholds.

Procedure 1-4: Setting filtering sensitivity

Step	Action
1	From the Mobile Administrator select the client/s that you want to set the filtering level for.
2	Click the arrow on the Filter Sensitivity: list to expand it:
3	Choose the level of filtering from the list.
4	Click Commit Changes to save the new Filter Sensitivity setting.



USER NAME

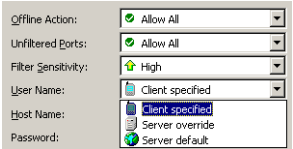
The User Name specifies the name used by the Mobile Filter server for all categorizations for the client device. This name will then be checked against the rules in the Rules Administrator to see if it appears in a rule. This name can be either be the system user name or a name you have created for this user. There are three types of User Name that can be used:

- **Client specified** - when the user logs into their remote device, for example a laptop computer, they will have to log into the operating system using a user name and password. **'Client specified'** sends this user name to the server and this is used in subsequent filtering.
- **Server override** - this is a user name that you specify to identify this user as a member of the organization without specifically defining them as an individual. It is particularly useful for devices that cannot supply a user name. A cell phone would be such a device though Mobile Filter does not support the use of cell phones as yet. You could enter a user name such as 'remote_user' for each cell phone that you are going to use. This would enable any user of this cell phone to be filtered regardless of who they were.
- **Server default** - this is a user name that will be used in the absence of a 'Client specified' or 'Server override' user name, thus enabling the device to still be filtered.

Procedure 1-5: Setting the type of User Name

Step	Action
1	Open the Mobile Administrator and select the client(s) that you want to set the user name for.

Procedure 1-5: Setting the type of User Name

Step	Action	
2	Click the arrow on the User Name: list to expand it:	
3	Choose the type of User Name that you require from the list.	
4	Click Commit Changes to save the new User name specification setting.	

HOST NAME

The Host name specifies the actual device itself rather than the person who is using the device. It means that devices or groups of devices can be recognized and filtered regardless of who is actually using them. This is divided into three types of host name:

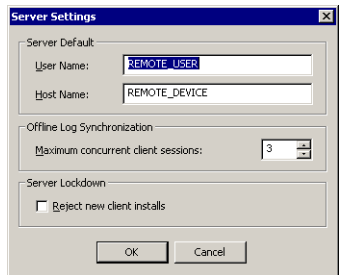
- **Client specified** - when the user logs into their remote device, for example a laptop computer, the network name of the device is sent to the Mobile Filter server and is used in subsequent filtering. When this device is added to a rule as a Who object, the rule can be applied to the device as if it were a user irrespective of the user using it.
- **Server override** - this is a host name that you specify to identify this device as a member of a particular group. It is particularly useful for devices that cannot supply a host name. You could enter a host name such as 'remote_device' for each device that you are going to use. This would enable any device thus named to be filtered.
- **Server default** - this is a host name that will be used in the absence of a 'Client specified' or 'Server override' hostname, thus enabling the device to still be filtered.

SERVER SETTINGS

Most of the settings available for configuration within the Administrator are specific to the clients that are installed to the server. However, there are some settings that are global to the server which can be configured in the Administrator.

These include the default User name and Host name. The User name is a ‘catch-all’ name given to a client in the event that a client name is not specified. It enables SurfControl Mobile Filter to apply settings to the client even without a specified name. One reason you might want to change this is if you already have a user account set up that is used by a low privileged user in the absence of their own account. Setting the User name to this account name will make sure that anyone using this account will be filtered automatically.

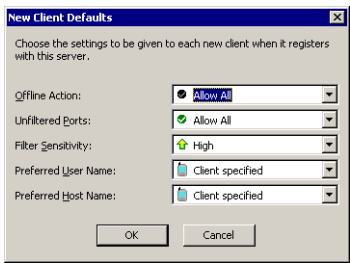
Procedure 1-6: Configuring server settings

Step	Action
1	<p>Select Server Settings from the Configure menu. The Server Settings dialog box will appear:</p> 
2	<p>Enter the following information:</p> <ul style="list-style-type: none">• User Name - the system value used for the ‘Server default’ user name• Host Name - the system value used for the ‘Server default’ host name• Maximum concurrent client sessions - if the server goes offline, the clients will not be able to connect to verify whether a Web page should be allowed or not. If you have set your clients to ‘Log & Allow’ then all Web pages will be allowed but a log will be kept as to what pages are being visited. Once the server is back on-line these logs will be uploaded onto the server. However, if too many clients attempt to do this at one time it can result in the server becoming less responsive to client filter requests. ‘Maximum concurrent client sessions’ enables you limit the number of clients that can connect at one time. <p>There is also a check-box called ‘Reject new client installs’. Select this to specify whether new clients can or cannot be installed to the Mobile Filter server.</p>
3	<p>Click OK.</p>

NEW CLIENT DEFAULTS

When a client is installed to the Mobile Filter server certain default settings are used. You can change these default values by setting up the New Clients Defaults dialog box. Any clients that are installed after this point will contain these settings.

Procedure 1-7: Setting new client defaults

Step	Action
1	<p>Select New Client Defaults from the Configure menu. The New Client Defaults dialog box will appear.</p> 
2	<p>Enter the following information:</p> <ul style="list-style-type: none"> • Offline Action: - set how the client will behave if the Mobile Filter server becomes unavailable. See "Offline Action" on page 6 for more details. The default is Allow All. • Unfiltered Ports: - set how the client should behave towards ports that are not included for filtering. See "Dealing with unfiltered ports" on page 7. The default is Allow All. • Filter Sensitivity: - set how much filtering is carried out. See "Setting filtering sensitivity" on page 8 for more details. The default is High. • Preferred User Name: - set the name for the user of the device that is being filtered. See "User name" on page 9 for more details. The default is client specified. • Preferred Host Name: - set the name for the device that is being filtered. See "Host name" on page 10 for more details. The default is client specified.
3	Click OK .

NAVIGATING AROUND THE MOBILE ADMINISTRATOR

Within the Mobile Administrator interface you can sort columns and perform searches on the contents to find clients more easily. You can also rearrange columns to reflect your preferred view of the data.

Sorting columns

To sort client data click the Heading at the top of the column. The data will be sorted into alphabetical order. Clicking the column again will reverse the order of the sort.


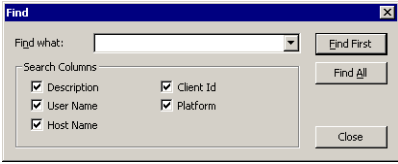
Moving columns

To move a column to a different position, select the column heading then drag and drop it into its new position. You can return it to its original position at any time by choosing **Columns > Reset order** from the View menu.

Finding clients

If you have a lot of clients and only want to administer those of a certain type you can use Find to select only those clients that contain the criteria that you are looking for.

Procedure 1-8: Searching for clients of a particular type

Step	Action
1	Choose Find... from the Edit menu or click  on the toolbar.
2	The Find dialog box will appear. 
3	Enter the text or characters that you want to be included in the search in the 'Find what:' text box.
4	Indicate which column you want to search by selecting the relevant 'Search Columns' check boxes.
5	Click Find First to have the first client that fulfills this criteria highlighted or Find All to have every client highlighted.

FILTER SETTINGS

Once you can see your clients within the Mobile Administrator you can select any of these and use the bottom half of the Administrator to change their filter settings.

SETTING FILTERING ACTION

- **Offline Action** - select an option from the list to state how the client should behave in the event of the Mobile Filter Server been unavailable.
- **Unfiltered Ports** - use the drop-down list to set how the client should behave with ports that are not specifically identified as filtered.
- **Filter Sensitivity** - set how sensitive you want filtering to be.

PORTS THAT CAN BE FILTERED

To reduce the amount of communication between Mobile Filter clients and servers the clients only communicate activity on those TCP ports of interest.

To perform filtering on a specific port, an appropriate protocol/port Where object must be applied to rules. Those rules that do not contain a protocol/port Where object are assumed to apply to HTTP ports only. The SurfControl Mobile client only filters ports that appear in active rules.

PORTS THAT CAN BE MONITORED

You can set the protocols to be monitored or unmonitored (see “Monitoring Specific Protocols” in Chapter 6 of the Web Filter Administrator’s Guide for more information).

The SurfControl Mobile client both filters and intercepts activity on those ports chosen to be monitored with the SurfControl Monitor and informs the Mobile Filter server.

Monitoring issues with Mobile Filter

You should be aware of the following when using the Monitor with Mobile Filter:

- In the Site Details and User Details panes, the ‘Bytes Sent’, ‘Bytes Received’ and ‘Duration’ fields will not display data because of the way in which the Mobile Filter client and server communicate.
- The ‘Allowed/Blocked’ status of off-line traffic will display as ‘Allowed’ in the Monitor. This is because at the time the Mobile Filter server was off-line and the client device was not being filtered by Mobile Filter. This is only applicable when the status of off-line traffic is set to ‘Log and Allow.’

FILTERING STATUS

The client will inform any user of any change in the way it is filtering. If a request is denied the user will see an appropriate Deny page corresponding to the rule that has been triggered. Non-HTTP requests (including HTTPS) will show a pop-up window containing a message. These will also be recorded in a Message history window with the most recent messages at the top, as in Figure 1-2:



Note: These messages are not permanently stored.

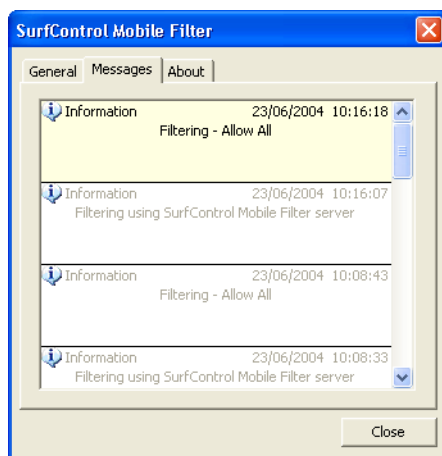








Figure 1-2 Filtering Status dialog box

CLIENT STATUS ICONS

Once the Mobile Filter client is installed on the mobile device your users will see an icon in the status area. The available icons are described in Table 1-1:

Table 1-2 Client Icons

Icon	Description
	The Mobile Filter Server is offline, and offline action is set to Allow All.
	Server is offline, and offline action is set to Block All.
	Server is offline, and offline action is set to Log & Allow.
	The client has switched off as a local Web Filter is already filtering the device.
	The product Icon. This is used while the client is using the Mobile Filter Server for filtering.
	The client is waiting for the user to access the Internet before trying to log on to the Mobile Filter server.

CLIENT PROPERTIES

Mobile Filter client properties can be seen by double-clicking the Mobile Filter system tray icon (see Figure 1-3). You can also right-click the icon and select **Open** from the pop-up menu. This will launch the Mobile Filter dialog box which contains the following tabs:

- General
- Messages
- About

General

The General tab contains three sections:

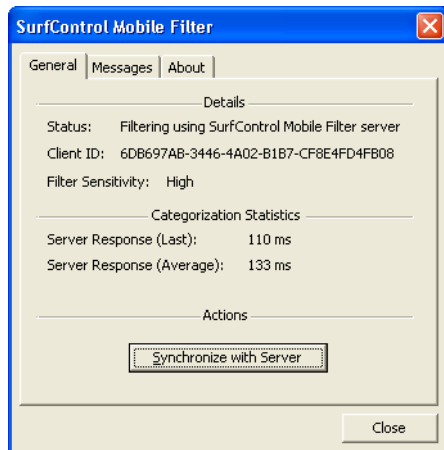


Figure 1-3 Mobile Filter General tab

- **Details** - this shows a summary of the Mobile Filter client settings, showing how filtering is set up, the client ID (this can be given by the user to an administrator or Technical Support so that they can identify the device within the Mobile Administrator) and the level of filtering sensitivity. See “Setting filtering sensitivity” on page 8 for more information on this setting.
- **Categorization Statistics** - every time an Internet request is made the Mobile Filter client contacts the Mobile Filter server to have the request categorized and have any appropriate rules applied. ‘Server Response (Last):’ shows how quickly the server responded to the client’s last request while ‘Server Response (Average):’ gives an average of the speed of communication based on the response times it has collected. If the last categorization failed the last response time will be preceded by the word ‘Failed’.

1

MOBILE FILTER *Client properties*

For example

- If the last categorization took 10 ms: Server Response (Last) 10ms.
- If the last categorization failed: Server Response (Last) Failed 65000ms.
- **Actions** - clicking **Synchronize with Server** immediately updates the client with any client side changes made on the Mobile Filter server.



Note: Clicking **Synchronize with Server** will not update the last response time.

Messages

Every time there is a change in the way the Mobile Filter client is filtering it will display a message relating to what has occurred (see Figure 1-4). These messages are stored in the Messages pane with the most recent at the top:

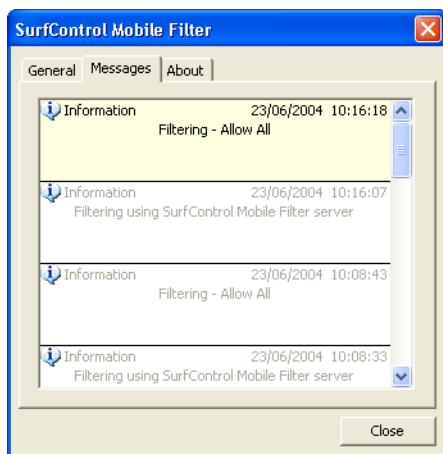


Figure 1-4 Mobile Filter Messages tab

About

The About tab (see Figure 1-5) tells you the version number of the product and can be used as a reference for upgrading etc:



Figure 1-5 Mobile Filter About tab

1

MOBILE FILTER *Client properties*