

The logo for Mobile Filter, featuring a red swoosh that curves around the left side of the text.

# Mobile Filter

Version 5.0

## SurfControl Mobile Filter

*Administrator's Guide*

A blue-tinted background image of a globe with a grid overlay, representing global connectivity and security.

Enterprise Threat Protection™

# NOTICES

---

Updates to the SurfControl documentation and software, as well as Support information are available at [www.SurfControl.com/support](http://www.SurfControl.com/support).

Copyright ©1998-2006 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 December 2005.

# CONTENTS

---

Notices.....	i
Finding your way around.....	1
The Mobile Filter Administrator .....	1
Administrator Menus.....	3
File .....	3
Edit .....	3
View .....	4
Configure .....	5
Tools .....	9
Help .....	11
Client Details section.....	12
Client Description .....	12
Offline Action .....	13
Offline action issues .....	14
Dealing with unfiltered ports .....	14
Setting filtering sensitivity .....	15
Visibility Level .....	16
User name .....	17
Host name .....	18
Password .....	18
Other Configuration.....	19
Ports that can be filtered .....	19
Ports that can be monitored .....	19
Security and Mobile Filter .....	20
The Mobile Filter Client.....	21
Client Status Icons .....	21
Client properties .....	22
Client Security .....	24
Group Policy and client configuration .....	25
Connections between client and server using SP2 .....	26
Troubleshooting.....	27
Client not filtering .....	27
Client not picking up change to offline action .....	27



## FINDING YOUR WAY AROUND

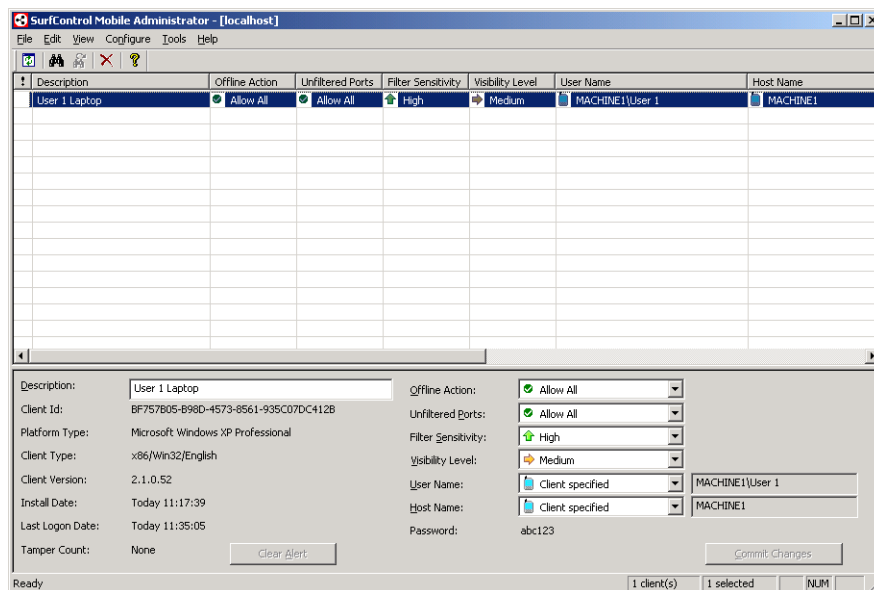
This guide describes how to configure SurfControl Mobile Filter once you have installed Service Pack 2. Service Pack 2 enhances SurfControl Mobile Filter to give you:

- Secure LDAP communication between Mobile Filter and the domain controller.
- The ability to configure the port between the client and Mobile Filter server.
- Network installation of clients via group policy.
- The ability to make the client invisible to the user.
- Secure communication between the client and the server.
- Increased client deployment security.

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.

## THE MOBILE FILTER ADMINISTRATOR

The Mobile Administrator (see Figure 1) is where you manage your SurfControl Mobile Filter clients. It contains a configurable description of each remote device with its settings.



**Figure 1** The Mobile Filter Administrator

Once you can see your clients within the Mobile Administrator you can edit their filter settings. When you select an individual client in the top pane of the Administrator, its details will appear in the bottom pane.



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

## *Finding your way around*

To see the Mobile Filter Administrator Select Start > Programs > SurfControl Web Filter > Mobile Administrator.

### **Selecting Clients to view and/or configure**

To view and configure the filtering of client devices, you need to select the client that you want to configure. Select clients 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.

#### **Procedure 1 Changing client properties**

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

# ADMINISTRATOR MENUS

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

## FILE

The **File** menu enables you to open databases and close the Administrator.

## Open...

The **Open...** menu enables you to 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

Enables you to close the Mobile Administrator.


## EDIT

The **Edit** menu enables you search, select and delete clients.

## Find

**Find** enables you to use a keyword search to locate particular clients. If you have a lot of clients and only want to configure those of a certain type, you can use **Find** to select only those clients that contain the criteria that you are looking for.

### Procedure 2 Searching for clients

Step	Action
1	Choose <b>Find...</b> from the <b>Edit</b> menu or click  on the toolbar.
2	The <b>Find</b> dialog box will appear.
	<div data-bbox="317 1360 890 1591" data-label="Image"> </div> <div data-bbox="927 1346 1249 1375" data-label="Caption"> <p><b>Figure 2</b> The Find dialog</p> </div> <div data-bbox="933 1404 1402 1558" data-label="List-Group"> <ul style="list-style-type: none"> <li>• <b>Find what:</b>- enter the text you want to find.</li> <li>• <b>Search Columns</b> - select the check-boxes that correspond to the columns that you want to search.</li> </ul> </div>
3	Enter the text or characters that you want to be included in the search into the 'Find what:' text box.
4	Indicate which column you want to search by selecting the relevant 'Search Columns' check boxes.
5	Click <b>Find First</b> to have the first client that fulfills this criteria highlighted or <b>Find All</b> to have every client highlighted.

### **Find Next**

The **Find Next** menu item enables you to find the next Mobile Filter client that matches the search criteria.

### **Select All**

Choosing **Select All** selects all of the clients in the Administrator.

### **Invert Selection**

This 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**

**Delete Client** removes the client from the Mobile Administrator. If you have not selected 'Reject new client installs' in the Server Settings dialog, the client will reappear the next time the Mobile Administrator opens.

## **VIEW**

The **View** menu enables you to specify how you want the Mobile Administrator to look by adding or hiding toolbar buttons and the status bar. You can also use the **View** menu to change the columns within the Administrator:

### **Toolbar**

Select **Toolbar** to show the Shortcut buttons or deselect it to hide them.

### **Status Bar**

Select **Status Bar** to show the status values at the bottom of the Administrator or deselect it to hide them.

### **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. 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. 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 Positions**.
- **Reset Widths** - Selecting Reset Widths restores the column widths to their default setting

### **Refresh**

Selecting **Refresh** updates the information in the Mobile Administrator by refreshing the details.

## CONFIGURE

The **Configure** menu enables you to specify global attributes for clients as well as the location and scope of your corporate Web Filter installations.

### Server Settings

**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. See “Offline action issues” on page 14, for more details.

Most of the settings available 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 3 Configuring Server settings

Step	Action
1	Select <b>Server Settings</b> from the <b>Configure</b> menu to see the Server Settings dialog.
2	<p>Enter the following information:</p> <ul style="list-style-type: none"> <li>• <b>User Name</b> - Enter or edit a system value which can be used for the ‘Server default’ user name.</li> <li>• <b>Host Name</b> - Enter or edit a system value which can be used for the ‘Server default’ host name.</li> <li>• <b>Offline Log Synchronization</b> - 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 &amp; 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. Select ‘Maximum concurrent client sessions’ to limit the number of clients that can connect at one time.</li> <li>• <b>Server Lockdown</b> - Select the ‘Reject new client installs’ check-box called to specify whether new clients can or cannot be installed to the Mobile Filter server.</li> </ul>
	<div data-bbox="316 1423 708 1745" data-label="Image"> </div> <p><b>Figure 3</b> The Server Settings dialog</p> <ul style="list-style-type: none"> <li>• <b>User Name</b> - The ‘Server default’ user name.</li> <li>• <b>Host Name</b> - The ‘Server default’ host name.</li> <li>• <b>Offline Synchronization</b> - Deals with how many client log files can be uploaded onto the server at any one time (see Step 2 for more details).</li> <li>• <b>Server Lockdown</b> - Rejects new client installs if selected.</li> </ul>
3	Click <b>OK</b> .

## 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 4 Configuring New Client Defaults.

Step	Action
1	Select <b>New Client Defaults</b> from the <b>Configure</b> menu.
2	<p>In the the New Client Defaults dialog box, enter the following information:</p> <ul style="list-style-type: none"> <li>• <b>Offline Action:</b> - set how the client will behave if the Mobile Filter server becomes unavailable. See “Client Details section” on page 12 for more details. The default is <b>Allow All</b>.</li> <li>• <b>Unfiltered Ports:</b> - set how the client should behave towards ports that are not included for filtering. See “Dealing with unfiltered ports” on page 14. The default is <b>Allow All</b>.</li> <li>• <b>Filter Sensitivity:</b> - set how much filtering is carried out. See “Setting filtering sensitivity” on page 15 for more details. The default is <b>High</b>.</li> <li>• <b>Visibility Level</b> - set how much of Mobile Filter the user sees. The default is Medium: <ul style="list-style-type: none"> <li>- Full - all features and pop-ups will be visible to the user.</li> <li>- Medium - the Client UI will be available but pop-ups will be disabled.</li> <li>- Stealth - no features will be available to the user. Only pop-ups containing a critical message will be shown.</li> </ul> </li> <li>• <b>Preferred Host Name:</b> - set the name for the device that is being filtered. See “Host name” on page 18 for more details. The default is <b>client specified</b>.</li> <li>• <b>Preferred User Name:</b> - set the name for the user of the device that is being filtered. See “Visibility Level” on page 16 for more details. The default is <b>client specified</b>.</li> </ul>
	<div data-bbox="311 1171 805 1558" data-label="Image"> </div> <div data-bbox="874 1150 1423 1600" data-label="Text"> <p><b>Figure 4</b> New Client Defaults</p> <ul style="list-style-type: none"> <li>• <b>Offline Action:</b> - How clients will behave if the server goes offline.</li> <li>• <b>Unfiltered Ports:</b> - How Mobile Filter treats ports that are not included for filtering.</li> <li>• <b>Filter Sensitivity:</b> - The strength of filtering.</li> <li>• <b>Visibility Level:</b> - How much of the client interface the user sees. The default is medium.</li> <li>• <b>Preferred Host Name:</b> - The name of the device being filtered.</li> <li>• <b>Preferred User Name:</b> - The name of the user of the device being filtered.</li> </ul> </div>
3	Click <b>OK</b> .

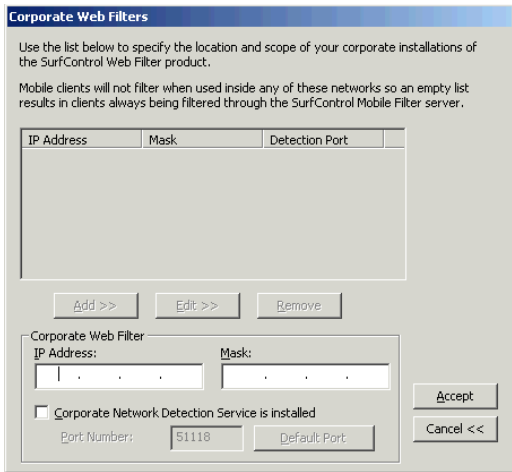
## Client Upgrade Details

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.

## Adding Corporate Web Filters

Mobile Filter has the ability to recognize when it is in the vicinity of an installation of the corporate Web Filter product, which will then take over filtering of the client.

### Procedure 5 Adding a corporate Web Filter server

Step	Action
1	Select <b>Corporate Web Filters</b> from the <b>Configure</b> menu. You will see the Corporate Web Filters dialog.
2	Click <b>Add&gt;&gt;</b> to expand the dialog box and enter the IP address of the Web Filter server along with a subnet mask to show the range of IP addresses that Mobile Filter has to look for.
	<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;">  </div> <div style="width: 45%;"> <p><b>Figure 5</b> Corporate Web Filters dialog</p> <ul style="list-style-type: none"> <li>• <b>Add&gt;&gt;</b> - Add a new IP address.</li> <li>• <b>Edit&gt;&gt;</b> - Edit an existing IP address.</li> <li>• <b>Remove&gt;&gt;</b> - Remove an existing IP address.</li> <li>• <b>IP Address</b> - The IP address of the Web Filter server.</li> <li>• <b>Mask</b> - The subnet mask for this network.</li> <li>• <b>Corporate Network Detection Service is installed</b> - indicate whether CNDS is installed. See your Mobile Filter Installation Guide for more details.</li> <li>• <b>Port Number</b> - The port number that the connection to CNDS will use.</li> <li>• <b>Default Port</b> - Sets the port number to the default.</li> </ul> </div> </div>
3	Once you have added all of the details that you need, click <b>Accept</b> to add the new IP address and Mask to the list. You will see the new server appear in the list pane which will now be enabled.
4	Click <b>OK</b> .

## Editing Corporate Web Filter servers

You can edit any of the corporate Web Filter servers that you have added to the Mobile Filter Administrator using the Corporate Web Filters dialog.

### Procedure 6 Editing an existing corporate Web Filter server

Step	Action
1	Select <b>Corporate Web Filters</b> from the <b>Configure</b> menu.
2	In the Corporate Web Filters dialog, select the Web Filter server from the list.
	<div data-bbox="317 625 900 995" data-label="Image"> </div> <div data-bbox="932 600 1351 659" data-label="Caption"> <p><b>Figure 6</b> Selecting the Web Filter server</p> </div> <div data-bbox="935 686 1393 823" data-label="List-Group"> <ul style="list-style-type: none"> <li>• <b>Add&gt;&gt;</b> - Add a new IP address.</li> <li>• <b>Edit&gt;&gt;</b> - Edit an existing IP address.</li> <li>• <b>Remove&gt;&gt;</b> - Remove an existing IP address.</li> </ul> </div>
3	Click <b>Edit</b> to expand the dialog.
	<div data-bbox="317 1096 863 1596" data-label="Image"> </div> <div data-bbox="932 1068 1406 1127" data-label="Caption"> <p><b>Figure 7</b> Editing the Web Filter server details</p> </div> <div data-bbox="932 1157 1406 1218" data-label="Text"> <p>See Step 2 Figure 5, for an explanation of fields in this dialog.</p> </div>
4	Make the required changes to the server settings and click <b>Accept</b> .
5	Click <b>OK</b> to apply the changes.

## CNDS

If your organization consists of more than one site, and you have a corporate Web Filter server in each one, then you can add each of these to the Mobile Administrator as a list. When a Mobile Filter client logs into the Mobile server, it informs the server of its IP address. This IP address is then tested against each Corporate Web Filter entry in the Corporate Web Filters dialog box to see if the Client's IP address exists within the range specified by each IP address and subnet mask.

The first entry found that matches the Client is then reported back for any additional checking against the CNDS, if installed. If it does not make a match with the first server it will try the next one in the list until it has tried them all. If no match is found, the client continues to filter, assuming it is not within its own corporate network.

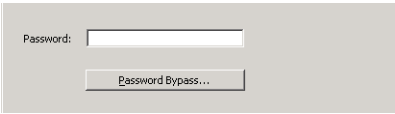
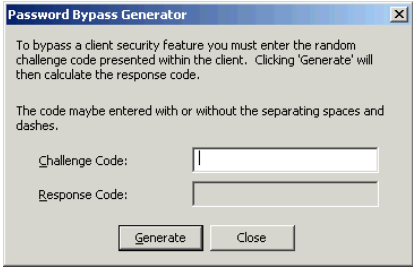
## TOOLS

The **Tools** menu enables you to set passwords and override them in the event of problems.

### Password Bypass Generator

To uninstall a client you need to supply the password that you entered during the client installation. If you forget this password you will have to use **Password Bypass** to override the original password and uninstall the client without it.

#### Procedure 7 Using Password Bypass Generator

Step	Action
1	If you find, when you are asked for your password that you cannot remember it, click the <b>Password Bypass</b> button in the Uninstall Password dialog on the client.
	 <p><b>Figure 8</b> Uninstall Password</p> <ul style="list-style-type: none"> <li>• <b>Password</b> - Enter the Client password.</li> <li>• <b>Password Bypass...</b> - Start to generate a bypass for this password if you can't remember it.</li> </ul>
2	You will see a Password Bypass dialog which carries a code in the Challenge Code edit field.
3	Go to the Mobile Filter Administrator select <b>Tools &gt; Bypass Generator</b> .
4	Copy the Challenge Code from the client into the 'Challenge Code:' edit field of this dialog.
	 <p><b>Figure 9</b> Password Bypass Generator</p> <ul style="list-style-type: none"> <li>• <b>Challenge Code:</b> - The code that you copy from the Client Password Bypass dialog.</li> <li>• <b>Response Code:</b> - The code that appears when you click <b>Generate</b>.</li> <li>• <b>Generate</b> - Generates the Response Code.</li> </ul>
5	Click <b>Generate</b> .

Step	Action
6	A code will appear in the 'Response Code:' text box.
7	Go back to the client and copy this Response Code from the server into the 'Response Code:' text box of the Client Password Bypass dialog.
8	Click <b>OK</b> to proceed with uninstalling the client.

### Set Server Pass-phrase

During the installation of the Mobile Filter client on to a user's device, it registers with the Mobile Filter server and its details are written to the Mobile Filter database. During this registration process the server passes a pass-phrase (created during the installation of Service Pack 2) to the client. The following illustrates how this pass-phrase can be used:

#### PROBLEM

- The Mobile Filter database has been deleted/corrupted and cannot be restored. The server administrator creates a new database.
- The client attempts to log onto the server to ask for a categorization. The logon fails because the new database contains no details of this client (the client did not register with THIS database during installation).
- The client attempts to re-register. Re-registration requires that the client's details already exist in the database. As this is not the case, the client is not allowed to log on to the Mobile Filter server.

#### SOLUTION

The Set Server Pass-phrase deals with a situation like this in the following way:

- After the administrator has created the new Mobile Filter database, he assigns the same pass-phrase to this database as the one used for the old database that no longer exists (using the Set Server Pass-phrase dialog).
- The client tries to log on to the server for a categorization which fails (because there are no client details in the database). The client obtained the pass-phrase during the client upgrade process. It now passes this pass-phrase to the server.
- The server checks that the password matches the one assigned to the new database (which it does because the administrator has assigned the old pass-phrase to the new database), then writes the client's details to the new database. It then allows the client to log on.



**Note: Once you have configured the server to use a new database, you MUST restart IIS. This is to ensure that the scnmlSAPIExt.dll picks up the new settings.**

**Setting a new Pass-phrase.** If you have created a new database using the Database Creation Tool the new database will not have a pass-phrase assigned to it.

#### Procedure 8 Setting a new Pass-phrase

Step	Action
1	Opening the Mobile Administrator, will show a message telling you that no Server Pass-phrase has been set. Click <b>OK</b> .
2	In the dialog that follows, enter a pass-phrase for the new database. The 'Enter existing pass-phrase:' is grayed out because a pass-phrase has not yet been assigned to this new database.
3	Enter a new pass-phrase and confirm it: The new password must be between 8 - 16 characters long.
	<div data-bbox="284 688 695 940" data-label="Image"> </div> <div data-bbox="751 667 1142 699" data-label="Caption"> <p><b>Figure 10</b> Set Server Pass-Phrase</p> </div> <div data-bbox="751 726 1404 919" data-label="List-Group"> <ul style="list-style-type: none"> <li>• <b>Enter existing pass-phrase</b> - This will be grayed out if no pass-phrase has been set.</li> <li>• <b>Enter new pass-phrase</b> - The new pass-phrase that you want to add.</li> <li>• <b>Confirm new pass-phrase</b> - The same pass-phrase entered again for confirmation.</li> </ul> </div>
4	Click <b>OK</b> . The next time the client requests a URL category from the server it will be forced to re-logout. The pass-phrase will then be passed to it.

**Changing a Pass-phrase.** If you need to change your pass-phrase you can use the Set Server Pass-phrase to do this.

#### Procedure 9 Changing a Pass-phrase

Step	Action
1	Select <b>Set Server Pass-phrase</b> from the <b>Tools</b> menu.
2	Enter the old password into the 'Enter existing pass-phrase:' text box.
3	Enter the new pass-phrase and confirm it: The new password must be between 8 - 16 characters long
4	Click <b>OK</b> . The next time the client requests a URL category from the server it will be forced to re-logout. The new pass-phrase will then be passed to it.

## HELP

### About SurfControl Mobile Administrator

The About box contains 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.

## CLIENT DETAILS SECTION

---

### CLIENT DESCRIPTION

This reflects the description added during the client's installation. You can edit the initial description in the Description field in the bottom pane. Details relating to the client are shown in Table 1. These are specified by the client and cannot be edited in the Mobile Administrator.

**Table 1** Client Details

Field	Description
<b>Client ID</b>	Unique ID that helps locate a specific client installation. This ID is also visible in the client. See "Client properties" on page 22 for more details.
<b>Platform Type</b>	The client operating system. It is useful when locating and/or grouping installations.
<b>Client Type</b>	Identifies the Processor, Operating System Description and Language variant of a Mobile Filter client.
<b>Client Version</b>	Identifies the version number of the Mobile Filter client and indicates whether an upgrade is available.
<b>Install Date</b>	Date on which the Mobile Filter client software was installed on the selected device.
<b>Last Logon Date</b>	Date the client last made an Internet request that was logged by the Mobile Administrator.
<b>Tamper Count</b>	Tamper count - Should the client detect an unauthorized change to any of the offline log files or the gateway URL in the registry, it will notify the server that a tamper has occurred. Once the server has been notified that the client has been tampered with, it will increase the tamper count for that client.
<b>Password</b>	Password that was supplied during the client's installation process and is required if you uninstall the client.

## 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, Block All and Log & Allow.

### Procedure 10 Setting Offline Action

Step	Action
1	Select the client/s that you want to set the offline action for.
2	Click the arrow on the <b>Offline Action:</b> list to expand it:
	<div data-bbox="301 760 817 1008"> </div> <div data-bbox="858 743 1209 774"> <p><b>Figure 11</b> Offline Action List</p> </div> <div data-bbox="863 802 1407 1197"> <ul style="list-style-type: none"> <li>• <b>Allow All</b> - every Web request will be allowed (the default).</li> <li>• <b>Block All</b> - every Web request will be blocked.</li> <li>• <b>Log &amp; Allow</b> - 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.</li> </ul> </div>
3	Choose the type of Offline Action that you require, from the list.
4	Click <b>Commit Changes</b> 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 5 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, Block All and Filter.

### Procedure 11 Setting Unfiltered Ports

Step	Action
1	Select the client/s that you want to set the unfiltered ports behavior for.
2	Click the arrow on the <b>Unfiltered ports:</b> list to expand it:
	<div data-bbox="309 951 917 1222" data-label="Image"> </div> <div data-bbox="976 936 1337 966" data-label="Caption"> <p><b>Figure 12</b> Unfiltered ports list</p> </div> <div data-bbox="976 995 1244 1024" data-label="Text"> <p>Unfiltered ports actions:</p> </div> <div data-bbox="976 1035 1404 1430" data-label="List-Group"> <ul style="list-style-type: none"> <li>• <b>Allow All</b> - 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).</li> <li>• <b>Block All</b> - block access to any unfiltered ports without contacting the Mobile Filter server to see if there is a rule set up for the port.</li> <li>• <b>Filter</b> - contact the Mobile Filter Server to see if any rules are set to apply to all ports.</li> </ul> </div>
3	Choose the type of action that you require for unfiltered ports, from the list.
4	Click <b>Commit Changes</b> 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, Medium, Low and Automatic.

### Procedure 12 Setting up Filter Sensitivity

Step	Action
1	Select the client/s that you want to set the filtering sensitivity for.
2	Click the arrow on the <b>Filter Sensitivity:</b> list to expand it:
	<div data-bbox="316 661 845 934" data-label="Image"> </div> <div data-bbox="885 640 1252 672" data-label="Caption"> <p><b>Figure 13</b> Filter sensitivity list</p> </div> <div data-bbox="885 703 1181 735" data-label="Text"> <p>Filter Sensitivity strengths:</p> </div> <div data-bbox="885 745 1404 1323" data-label="List-Group"> <ul style="list-style-type: none"> <li>• <b>High</b> - 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.</li> <li>• <b>Medium</b> - all non-HTTP ports are categorized but only HTTP page requests are categorized while Images/sounds/style sheets, and XML requests are not categorized.</li> <li>• <b>Low</b> - 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.</li> <li>• <b>Automatic</b> - the client chooses High, Medium or Low based on the average Mobile Filter server response times and pre-configured thresholds.</li> </ul> </div>
3	Choose the level of filtering from the list.
4	Click <b>Commit Changes</b> to save the new Filter Sensitivity setting.

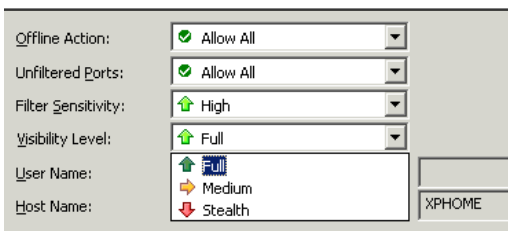
## VISIBILITY LEVEL

You can set up Mobile Filter to hide some or all of its features from the user. There are three levels of visibility: Full, Medium and Stealth.



**Note:** If the client tries to access a port that is blocked, they will see a warning pop-up, regardless of the visibility setting.

### Procedure 13 Setting up Visibility Level

Step	Action
1	Select the client/s that you want to set the visibility level for.
2	Click the arrow on the <b>Visibility Level:</b> list to expand it:
	<div style="display: flex; align-items: flex-start;"> <div style="flex: 1;">  </div> <div style="flex: 1; padding-left: 20px;"> <p><b>Figure 14</b> Visibility Level list</p> <p>Visibility levels:</p> <ul style="list-style-type: none"> <li>• <b>Full</b> - Full visibility. All features and pop-ups will be visible.</li> <li>• <b>Medium</b> - The user interface will be visible to the user but pop-ups will be disabled though critical messages will be shown. This is the default setting for a new client.</li> <li>• <b>Stealth</b> - No features will be visible to the user. Only pop-ups containing critical messages will be shown.</li> </ul> <p><b>Note:</b> <i>The client interface will be displayed when an upgrade is available, even if the client is set to Stealth mode.</i></p> </div> </div>
3	Choose the level of visibility from the list.
4	Click <b>Commit Changes</b> to save the new Visibility 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, Server override and Server default.

### Procedure 14 Setting Client User names

Step	Action
1	Select the client(s) that you want to set the user name for.
2	Click the arrow on the <b>User Name:</b> list to expand it:
	<div data-bbox="319 682 877 934"> </div> <div data-bbox="917 672 1404 1554"> <p><b>Figure 15</b> Client User Name list</p> <p>Client user name list:</p> <ul style="list-style-type: none"> <li>• <b>Client specified</b> - 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. <b>'Client specified'</b> sends this user name to the server and this is used in subsequent filtering.</li> <li>• <b>Server override</b> - 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, although 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 are.</li> <li>• <b>Server default</b> - 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.</li> </ul> </div>
3	Choose the type of User Name that you require from the list.
4	Click <b>Commit Changes</b> 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.

## PASSWORD

This is the password that is needed to uninstall the Mobile Filter Client.

## OTHER CONFIGURATION

---

Once you can see your clients within the Mobile Administrator you can select any of these and use the bottom half of the Administrator interface to change their filter settings. These clients can then be added to SurfControl Web Filter rules so that you can apply your company filtering policy to them.

### 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 within 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.'

## SECURITY AND MOBILE FILTER

SurfControl Mobile Filter now offers support for secure connection:

- Between the Mobile Filter server and your LDAP server
- Between the Mobile Filter server and client.

### Mobile Filter server and LDAP server

A secure connection can now be made between the Mobile Filter server and your LDAP server. During installation you were asked to specify whether you required a secure or non-secure connection. You can change this setting by editing the `SecureConnection` registry setting.

#### Procedure 15 Changing the registry setting

Step	Action
1	Open the registry using regedit and navigate to:  HKEY_LOCAL_MACHINE\SOFTWARE\JSB\SurfControl Scout
2	Set the SecureConnection DWORD value: <ul style="list-style-type: none"><li>• 1 - gives a secure connection though there will be an impact on connection speed.</li><li>• 0 - connection is faster but unsecure.</li></ul>

## THE MOBILE FILTER CLIENT

If a client is not set to Stealth it 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 if the visibility level on the client is set to 'Full'. These will also be recorded in a Message history window with the most recent messages at the top, as in Figure 16. These messages are not permanently stored.



**Note:** No client properties can be seen if the client visibility is set to Stealth.

## CLIENT STATUS ICONS

Once the Mobile Filter client is installed on the mobile device your users will see an icon in the status area, as long as the client visibility is not set to Stealth. The available icons are described in Table 1:

**Table 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 17). 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:

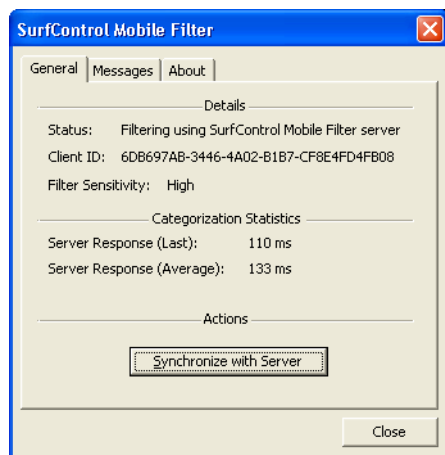


Figure 16 Mobile Filter General tab

- **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 15 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’.

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.

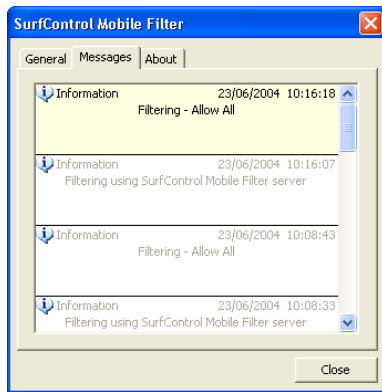


**Note: Clicking Synchronize with Server will not update the last response time.**

---

## 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 18). These messages are stored in the Messages pane with the most recent at the top:



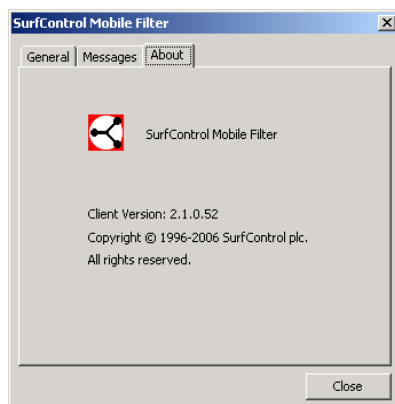
**Figure 17** Mobile Filter Messages tab



**Note:** If the client visibility is set to Medium, only messages concerned with blocked ports, tampers and upgrades will be displayed.

## About

The About tab (see Figure 19) tells you the version number of the product and can be used as a reference for upgrading etc:



**Figure 18** Mobile Filter About tab

## CLIENT SECURITY

During installation, the Mobile Filter server's contact information is stored in the registry of the client machine as the Gateway URL. Some users may try to change this URL to avoid being filtered. The client can detect unauthorised changes and automatically repair invalid entries. It does this in the following way:

- If the gateway URL in the registry is not formed correctly, it will instantly be replaced with the last gateway URL that was used by the client to successfully contact the server. A tamper will be logged.
- If the gateway URL contained in the registry is valid but cannot be contacted, the client will enter it's default offline action state. It will then check the gateway URL periodically for a specified period of time (24hrs by default).
- If the server cannot be contacted after the specified time period, the gateway URL in the registry, and the last successfully connected gateway URL will be compared.
  - If the two are different, the gateway URL in the registry will be changed to match the last successful gateway URL. A tamper will be raised and the client will attempt to connect to the server using the updated gateway URL in the registry.
  - If the two gateway URL's are the same, the client remains in it's offline state and will periodically poll the server.

## GROUP POLICY AND CLIENT CONFIGURATION

It is now possible to use Group Policy to configure the Mobile Filter server (and port) to be used by clients. Procedure 16 details the steps that must be followed in order to add the new SurfControl template to the Administrative Templates within a Group Policy Object, as well as how to configure the new server information.

The following instructions assume that you are familiar with Active Directory and using the Microsoft Group Policy Manager to apply policies to machines or groups of machines.

### Procedure 16 Applying Group Policy to the Gateway URL

Step	Action
1	Open Group Policy Manager on the Mobile Filter server.
2	Right-click the Default Domain Policy object and select <b>Edit</b> .
3	In the Group Policy Object Editor select Computer <b>Configuration</b> > <b>Administrative Templates</b> .
4	Right-click and select <b>Add/Remove Templates..</b>
5	In the Add/Remove Template dialog that follows click <b>Add</b> .
6	Navigate to the Scmfcli.adm file. By default this will be stored in: C:\Program Files\SurfControl\Web Filter\Tools
7	Select the file Scmfcli.adm and click <b>Open</b> .
8	Click <b>Close</b> in the Add/Remove Templates dialog.
9	Expand the Administrative Templates folder in the Group Policy Manager and you will now see a list of directories beneath it.
10	Select SurfControl Mobile Filter Client then select Server URL in the right-hand pane.
11	Click the <b>Properties</b> hyper-link.
12	In the dialog that follows select the <b>Enabled</b> option. This will enable the URL text box underneath.
13	Enter the following URL: <code>&lt;protocol&gt;://&lt;server.domain:port&gt;/scnmgw/scnmisapiext.dll</code> where <code>&lt;protocol&gt;</code> is either <code>http</code> or <code>https</code> and <code>&lt;server.domain:port&gt;</code> is the name of your server and domain. The optional port specification, <code>:port</code> , enables you to use a different port to the defaults of 80 for <code>http</code> and 443 for <code>https</code> . <b>Note:</b> <i>Do not alter the name, or the path to, the dll.</i>

Step	Action
	<div data-bbox="304 348 699 779" data-label="Image"> </div> <div data-bbox="751 331 1406 621" data-label="List-Group"> <p><b>Figure 19</b> The Server URL Properties dialog</p> <ul style="list-style-type: none"> <li>• <b>Not Configured</b> - no Group Policy URL has been added.</li> <li>• <b>Enabled</b> - the Group Policy URL will override the default Gateway URL setting in the registry.</li> <li>• <b>Disabled</b> - the Group Policy URL has been added but it has been disabled. The default Gateway URL will be used.</li> <li>• <b>URL:</b> - the URL to the Mobile Filter server.</li> </ul> </div>
14	Click <b>OK</b> .

## CONNECTIONS BETWEEN CLIENT AND SERVER USING SP2

If you are using IIS v5.0, once a connection to an ISP is established it is maintained and remains open indefinitely until the client logs off. This may be a problem if you have to pay for your network use on a 'pay for time used' basis. This is not an issue with IIS v6.0 so upgrading to this IIS version should fix the problem.

## TROUBLESHOOTING

---

If you are encountering difficulties with a client, we recommend that you perform the following procedures in the order listed. It is advisable to retest the client between each step:

- Try closing and restarting the problematic application.
- Open the Mobile Filter client UI, and click the **Synchronize with Server** button.
- Restart the computer.
- Check the Mobile Filter Web site for an up to date list of known problems.
- Re-run the Mobile Filter client setup and try the Repair option.
- Uninstall the Mobile Filter client software, reboot and then re-install the software.

### CLIENT NOT FILTERING

Mobile Filter has the intelligence to know when it is in the company environment so that it will switch off and leave the filtering to the company web filter. It does this by recognizing the range of IP addresses that it is exposed to and recognizing that it is within its own network. However, companies can use ranges of IP addresses which can be duplicated across different companies. If the Mobile Filter client should go into an environment that consists of IP addresses within the same range of those of the company from which it originates then it will think that it is now within its own company and will switch off.



**Note:** You can install CNDS to make sure that the client only switches off when it is within its own network and not someone else's. See 'CNDS' in the Mobile Filter Installation Guide for details on how to install this service.

---

### CLIENT NOT PICKING UP CHANGE TO OFFLINE ACTION

When a Mobile Filter client cannot communicate with the Mobile Filter Server, perhaps because the server is offline, the Mobile Filter client applies filtering to the device depending on the Offline Action that was present within the Mobile Administrator at the last successful connection to the Mobile Filter Server. This means that, although you may change the Offline Action for a particular client on the Mobile Administrator, this change will only come into effect once the client has been able to successfully logon to the Mobile Filter server and pick up this new configuration setting.

## *Troubleshooting*