



Version 5.5

# SurfControl Mobile Filter

*Administrator's Guide*



# NOTICES

---

Copyright © 2007 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.

SurfControl Web Filter contains the VeriSign International Domain Name (IDN) SDK

Copyright © 2003, VeriSign Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the VeriSign Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software is licensed under the BSD open source license. For more information visit [www.opensource.org](http://www.opensource.org).

SurfControl Web Filter contains the MD5.H - header file for MD5C.C: Copyright © 1991-2, ROSA Data Security, Inc. Created 1991. All rights reserved.

# TABLE OF CONTENTS

---

Notices.....	i
<b>Mobile Filter.....</b>	<b>1</b>
Finding your way around .....	2
The Client Administrator .....	2
Administrator Menus.....	4
File.....	4
Edit .....	4
View.....	5
Configure .....	6
Tools.....	10
Help .....	12
Client Details section .....	13
Client Description .....	13
Offline Action .....	14
Offline action issues .....	14
Dealing with unfiltered ports .....	15
Setting filtering sensitivity .....	15
Visibility Level.....	16
User Name .....	16
Host Name.....	17
Password.....	18
Other Configuration .....	19
Ports that can be filtered.....	19
Ports that can be monitored .....	19
Replacing the Mobile Filter database .....	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 .....	24
Connections between client and server using SP2 .....	26
Troubleshooting.....	27
Client not filtering .....	27
Client not picking up change to offline action .....	27
Repairing Internet filtering problems.....	27
<b>Appendix.....</b>	<b>29</b>
Comments on this Guide? .....	30
Technical Support.....	31
SurfControl Sales .....	32



## Mobile Filter

Finding your way around .....	page 2
Administrator Menus .....	page 4
Client Details section .....	page 13
Other Configuration .....	page 19
The Mobile Filter Client .....	page 21
Troubleshooting .....	page 27

## FINDING YOUR WAY AROUND

This guide describes how to configure SurfControl Mobile Filter. Mobile Filter provides the following functionality:

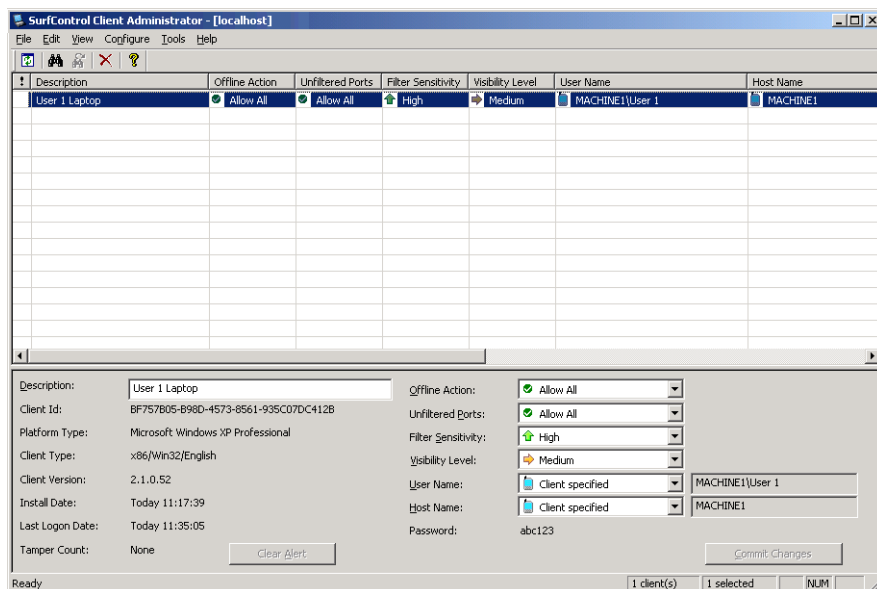
- Secure LDAP communication between Mobile Filter and the domain controller.
- The ability to configure the port between the client and Mobile Filter server.
- Network installation of clients via group policy.
- The ability to make the client invisible to the user.
- Secure communication between the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

The Client Administrator is where you manage your SurfControl Mobile Filter clients. It contains a configurable description of each remote device and it's settings. Select **Client Administrator** from the **Start > Programs > SurfControl Web Filter** menu to launch the Client Administrator, as shown below.

Figure 1-1 The Client Administrator



Once you can see your clients within the Client Administrator you can edit their filter settings. When you select an individual client in the top pane of the Administrator, their 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.

---

## 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. To search for clients which meet specific criteria:


- 1 Select **Find** from the **Edit** menu.
- 2 Click the **Find First** button to find one client of a particular type.
- 3 Click the **Find All** button to find a group of clients of a particular type.

To change client properties:

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

## Client Administrator Columns

Every client that appears in the top pane of the Client Administrator, displays the current security settings that it has been configured with. Below is a description of the information shown in each column:

- **Information column (!)** - Signals whether the client has an unacknowledged tamper on it. The column shows the medic icon  if the tamper count has increased since the last tamper count was cleared.
- **Description** - Shows the current description of the client, entered at the time of the client installation. This can be edited in the **Description** text box in the bottom pane of the Client Administrator.
- **Offline Action** - The current offline action setting in use by the client.
- **Unfiltered Ports** - The current unfiltered ports setting in use by the client.
- **Filter Sensitivity** - The current filter sensitivity setting in use by the client.
- **Visibility Level** - The current visibility level setting in use by the client.
- **User Name** - Shows the user name that has been applied to, or returned by the client.
- **Host Name** - Shows the host name that has been applied to, or returned by the client.
- **Last Logon Date** - The last time the client made an internet request.
- **Client Id** - The unique identification number of the client.
- **Install Date** - The date the client installation took place.
- **Platform** - The platform installed on the selected client device.
- **Tamper Count** - Shows the amount of tampers on a particular client device.

## ADMINISTRATOR MENUS

---

The following menu options are available in the Client Administrator:

### FILE

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

### Open

The **Open** menu enables you to open a database of Mobile Filter clients to be administered by the Client Administrator. Only Mobile Filter compatible databases can be opened in the Administrator.

### Exit

Enables you to close the Client Administrator.

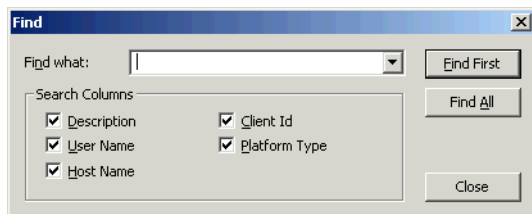
### EDIT

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. To search for Mobile Filter Clients:

- 1 Select **Find** from the **Edit** menu. The Find dialog box will appear.



- 2 Enter the text you want to search for in the **Find what** box.
- 3 Select the search columns that correspond to the columns you want to search on.
- 4 Click **Find First** to have the first client that fulfills this criteria highlighted or **Find All** 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 Client Administrator.

## Invert Selection

This reverses the selection status of the clients in the Client 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 Client Administrator. If you have not selected 'Reject new client installs' in the Server Settings dialog, the client will reappear the next time the Client Administrator opens.

## VIEW

The **View** menu enables you to specify how you want the Client 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 Client 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**

Select this to restore column widths to their default setting.

### Refresh

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

## CONFIGURE

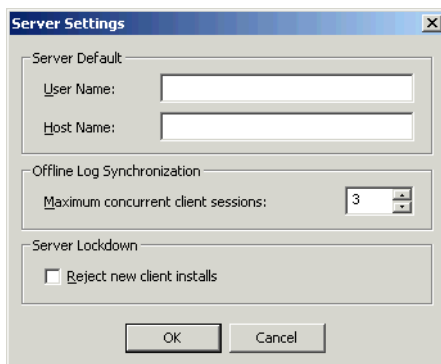
The **Configure** menu enables you to specify global attributes for clients as well as the location and scope of your corporate Web Filter installations.

### Server Settings

The Server Settings enables you to specify if 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 Client 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 Client 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. To configure Server settings:

- 1 Select Server Settings from the Configure menu to see the Server Settings dialog and enter the following information:
  - **User Name** - Enter or edit a system value which can be used for the 'Server default' user name. This must be in the format anydomain\firstname.lastname
  - **Host Name** - Enter or edit a system value which can be used for the 'Server default' host name. This must be in the format anydomain\firstname.lastname
  - **Offline Log Synchronization** - 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. Select 'Maximum concurrent client sessions' to limit the number of clients that can connect at one time.
  - **Server Lockdown** - Select the **Reject new client installs** check box called to specify whether new clients can or cannot be installed to the Mobile Filter server.

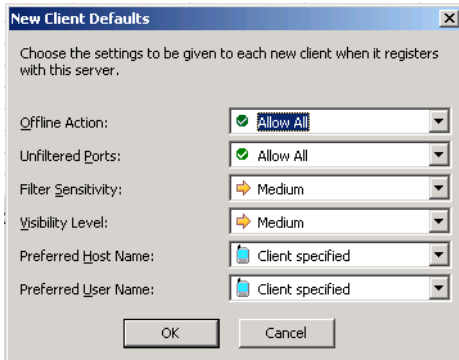


- 2 Click **OK**.

## New Client Defaults

Certain default settings are used when a client is connected to the Mobile Filter server. You can change these default values by setting up the **New Client Defaults**. Any clients that are installed after this point will contain these settings. To Configure New Client Defaults:

- 1 Select **New Client Defaults** from the **Configure** menu. The New Client Defaults dialog box appears:



- 2 In the New Client Defaults dialog box, enter the following information:
  - **Offline Action** - Set how the client will behave if the Mobile Filter server becomes unavailable. See [Client Details section on page 13](#) 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 15](#). The default is Allow All.
  - **Filter Sensitivity** - Set how much filtering is carried out. See [Setting filtering sensitivity on page 15](#) for more details. The default is Medium.
  - **Visibility Level** - Set how much of Mobile Filter the user sees. See [Visibility Level on page 16](#) for further details. The default is Medium.
  - **Preferred Host Name** - Set the name for the device that is being filtered. See [Host Name on page 17](#) for more details. The default is client specified.
  - **Preferred User Name** - Set the name for the user of the device that is being filtered. See [User Name on page 16](#) for more details. The default is client specified.
- 3 Click **OK** to save changes, or **Cancel** to exit without saving.

## 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 Starter Guide for more details.

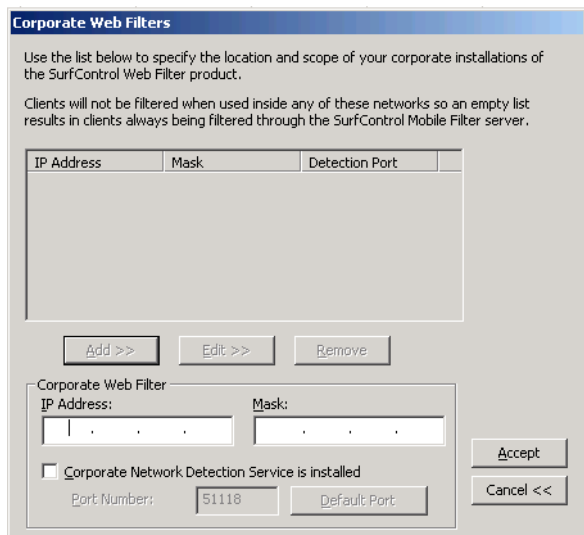
## Adding Corporate Web Filters

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. To add a corporate Web Filter server:

# 1 MOBILE FILTER

## Administrator Menus

- 1 Select **Corporate Web Filters** from the **Configure** menu. The Corporate Web Filters dialog box is shown:



- 2 Click **Add** to expand the dialog box.
- 3 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. You can then perform the following actions:
  - **Add** - Add a new IP address.
  - **Edit** - Edit an existing IP address.
  - **Remove** - Remove an existing IP address.

The **Corporate Network Detection Service is installed** option, indicates whether CNDS is installed. The **Port Number** is the connection to CNDS which Mobile Filter will use. The **Default Port** button resets the port number to 51118.

- 4 Once you have added all of the details that you need, click **Accept** 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.
- 5 Click **OK**.

## Connecting via a VPN

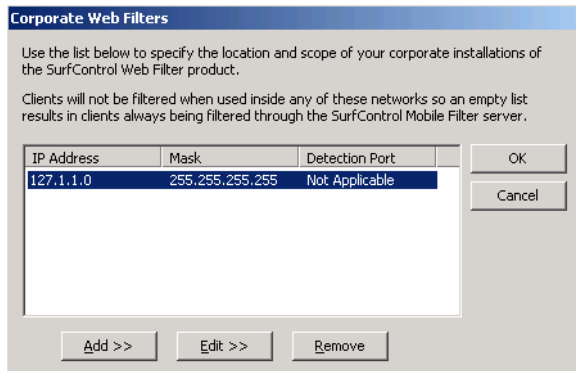
If your Mobile Filter clients connect to your corporate network through a Virtual Private Network connection (VPN), it is important that you add the subnet address of the VPN to the Corporate Web Filter list. This allows the Mobile Filter client to go to sleep and ensures that the Web Filter server takes over filtering when connected to the VPN server.

## Editing Corporate Web Filter servers

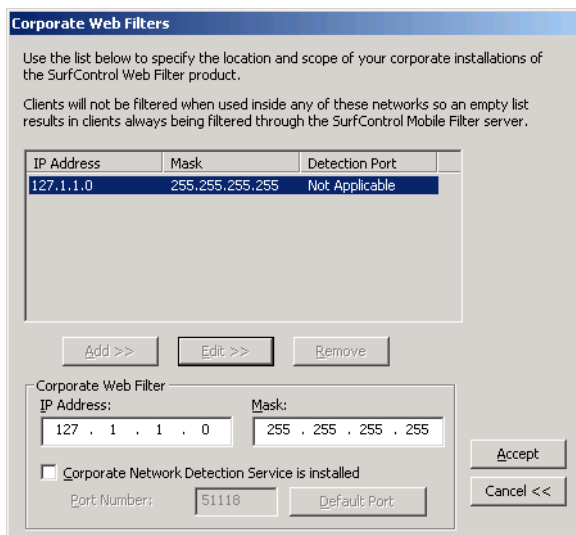
You can edit any of the corporate Web Filter servers that you have added to the Client Administrator using the Corporate Web Filters dialog. Perform the following steps to edit an existing corporate Web Filter server:

- 1 Select **Corporate Web Filters** from the **Configure** menu.

- In the Corporate Web Filters dialog, select the Web Filter server from the list. You can perform the following tasks:



- Click **Edit** to expand the dialog.



- Make the required changes to the server settings and click **Accept**.
- Click **OK** 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 Client 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. For details on configuring CNDS please consult the Web Filter *Administrator's Guide*.

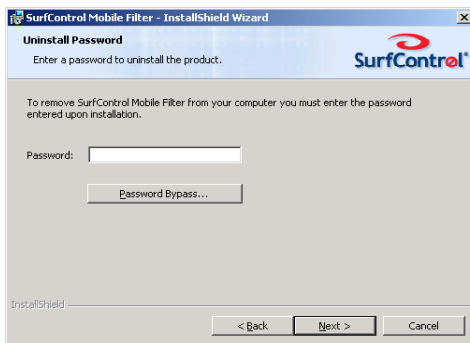
## TOOLS

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

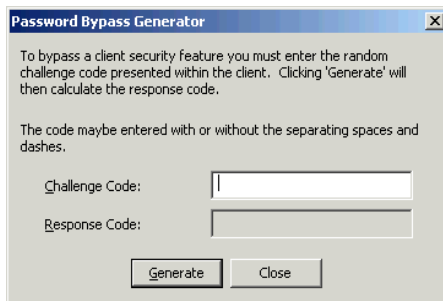
### Password Bypass Generator

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 the **Password Bypass Generator** to override the original password and uninstall the client without it. To generate a new password:

- 1 Click the **Password Bypass** button in the Uninstall Password dialog on the client. You will see a Password Bypass dialog box which carries a code in the **Challenge Code** text box.



- 2 In the Client Administrator click the **Tools** menu and select **Password Bypass Generator**.
- 3 Copy the Challenge Code from the client into the Challenge Code text box as shown below.



- 4 Click **Generate**. A code will appear in the Response Code text box.
- 5 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. Click **Next**.
- 6 Click **Remove** 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 to the client. The following illustrates how this pass-phrase can be used:

### PROBLEM

- 1 The Mobile Filter database has been deleted or corrupted and cannot be restored. The server administrator creates a new database.
- 2 The client attempts to log on to 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).
- 3 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:

- 1 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).
- 2 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.
- 3 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 `scnmISAPIExt.dll` picks up the new settings.

---

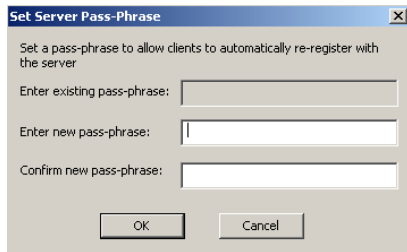
## Setting a new Pass-phrase

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

- 1 On opening the Client Administrator, a message is displayed stating that a Server Pass-phrase has not been set. Click **OK**.
- 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.

# 1 MOBILE FILTER Administrator Menus

- 3 Enter a new pass-phrase and confirm it: The new password must be between 8 and 16 characters long.



- 4 Click **OK**. The next time the client requests a URL category from the server it will be forced to re-logon. 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** utility. Perform the following steps to change the pass-phrase:

- 1 Select **Set Server Pass-phrase** from the **Tools** 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 and 16 characters long.
- 4 Click **OK**. The next time the client requests a URL category from the server it will be forced to re-logon. The new pass-phrase will then be passed to it.

## HELP

The Help menu contains the **About** sub-menu which launches the About box. This 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

---

The lower pane of the Client Administrator displays configuration information for whichever client is selected in the main pane.

### 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 the table below. These are specified by the client and cannot be edited in the Client Administrator.

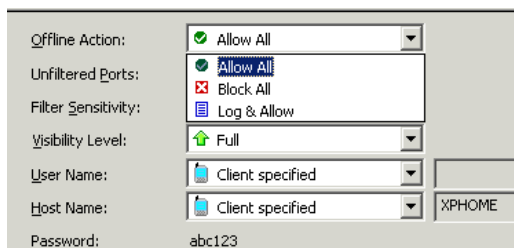
**Table 1-1** Client Details

Field	Description
Client ID	Unique ID that helps locate a specific client installation. This ID is also visible in the client. See <a href="#">Client properties on page 22</a> 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.
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 Client Administrator.
Tamper Count	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.
Password	Password that was supplied during the client 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), 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, and 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. To configure offline action settings:

- 1 Select the client(s) that you want to set the offline action for.
- 2 Click the arrow on the **Offline Action** list to expand it, as shown below:



The screenshot shows a configuration window with the following fields and values:

Offline Action:	Allow All
Unfiltered Ports:	Allow All, Block All, Log & Allow
Filter Sensitivity:	Log & Allow
Visibility Level:	Full
User Name:	Client specified
Host Name:	Client specified XPHOME
Password:	abc123

- 3 Choose the type of Offline Action that you require, from the list:
  - **Allow All** - All Web requests on the client are allowed whilst the Mobile Filter Server is offline.
  - **Block All** - All Web requests are blocked on the client whilst the Mobile Filter Server is offline.
  - **Log & Allow** - All Web requests are allowed and written to a local log file on the client whilst the Mobile Filter Server is offline. Once the Mobile Filter Server has restored network connectivity, the client will upload the log file to the Mobile Filter Server's Monitor database.
- 4 Click **Commit Changes** to add the new Offline Action setting to the client in the Mobile Filter client Administrator.

## OFFLINE ACTION ISSUES

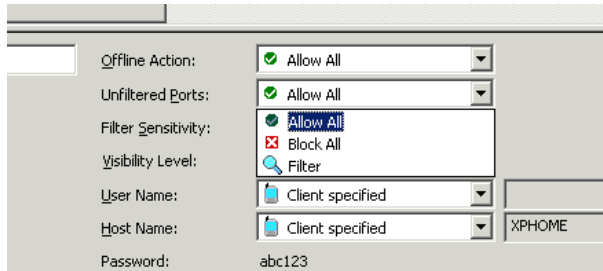
When a server is offline the client repeatedly polls the server until it can re-connect to it. As soon as the client establishes a successful connection, any offline logs are sent to the Mobile Filter server.

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 6](#) 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. To set the sensitivity for unfiltered ports:

- 1 Select the client(s) that you want to set the unfiltered ports behavior for.
- 2 Click the arrow on the **Unfiltered ports** list to expand it:

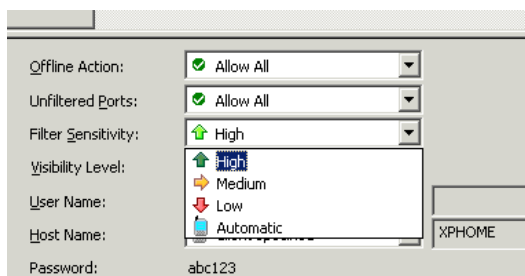


- 3 Choose the type of action that you require for unfiltered ports, from the list.
  - **Allow All** - Allow access to all unfiltered ports without contacting the Mobile Filter server to see if there is a rule set up for the port (this is the default).
  - **Block All** - Block access to any unfiltered 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.
- 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, Medium, Low and Automatic. To configure Filter Sensitivity:

- 1 Select the client(s) that you want to set the filtering sensitivity for.
- 2 Click the arrow on the **Filter Sensitivity** list to expand it:

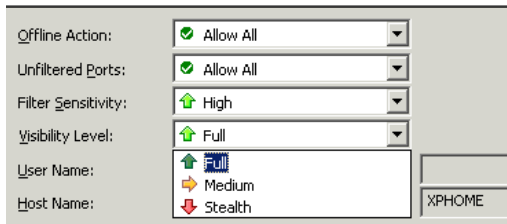


- 3 Choose the level of filtering from the list.
- 4 Click **Commit Changes** to save the new Filter Sensitivity setting.

## 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. Perform the following steps to configure Visibility Level:

- 1 Select the client(s) that you want to set the visibility level for.
- 2 Click the arrow on the **Visibility Level** list to expand it:



The screenshot shows a configuration window with several settings. The 'Visibility Level' dropdown menu is expanded, showing three options: 'Full' (with a green up arrow), 'Medium' (with an orange right arrow), and 'Stealth' (with a red down arrow). Other settings include 'Offline Action' (Allow All), 'Unfiltered Ports' (Allow All), and 'Filter Sensitivity' (High). The 'User Name' field is empty, and the 'Host Name' field contains 'XPHOME'.

- 3 Choose the level of visibility from the list.
  - **Full** - Full visibility. All features and pop-ups will be visible to the user.
  - **Medium** - The user interface and critical messages will be visible to the user but pop-ups will be disabled. This is the default setting for a new client.
  - **Stealth** - Features will not be visible to the user. Only pop-ups containing critical messages will be shown.



**Note:** The client interface will be displayed when an upgrade is available, even if the client is set to Stealth mode

- 4 Click **Commit Changes** to save the new Visibility setting.



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

- 1 Select the client(s) that you want to set the user name for.

- 2 Click the arrow on the **User Name** list to expand it, as shown below:



The screenshot shows a configuration window with several settings. The 'User Name' dropdown menu is expanded, showing three options: 'Client specified' (selected), 'Server override', and 'Server default'. Other settings include 'Offline Action', 'Unfiltered Ports', 'Filter Sensitivity', and 'Visibility Level', all set to 'Allow All', 'High', and 'Full' respectively. The 'Host Name' field contains 'XPHOME' and the 'Password' field is empty.

You have the following options to choose from:

- **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. This must be in the format **anydomain\firstname.lastname**. 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 domain\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.
  - **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. This must be in the format **anydomain\firstname.lastname**.
- 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. This must be in the format anydomain\firstname.lastname. It is particularly useful for devices that cannot supply a host name. You could enter a host name such as domain\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. This must be in the format anydomain\firstname.lastname.



## **PASSWORD**

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

## OTHER CONFIGURATION

---

Once you can see your clients within the Client 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 'What' object must be applied to rules. Those rules that do not contain a protocol/port 'What' 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.'

### REPLACING THE MOBILE FILTER DATABASE

In the event that you may need to create a new Mobile Filter database, (either because it has been deleted or corrupted, and therefore cannot be restored), you will need to restart the Internet Information Services (IIS) service on the Mobile Filter server. This is because the Mobile Filter clients communicate with the Mobile Filter server through an ISAPI extension (scnmISAPIExt.dll), which is registered automatically with IIS during the Mobile Filter server installation.

Restarting the IIS service on the server will enable the Mobile Filter clients to re-register with the Mobile Filter server, acquire the new database settings and resume database connectivity. For further details about setting the server pass-phrase in order to re-register with the Mobile Filter server, see [Set Server Pass-phrase on page 11](#).

## 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.

- 1 Open the registry using regedit and navigate to:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\JSB\SurfControl Scout
- 2 Set the `SecureConnection` DWORD value:
  - 1 - gives a secure connection though there will be an impact on connection speed.
  - 0 - connection is faster but unsecure.

# 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. These messages are not permanently stored.









**Note:** Client properties cannot 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 notification area (as long as the client visibility is not set to Stealth). The available icons are described in the table below:

**Table 1-2** Client Status 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

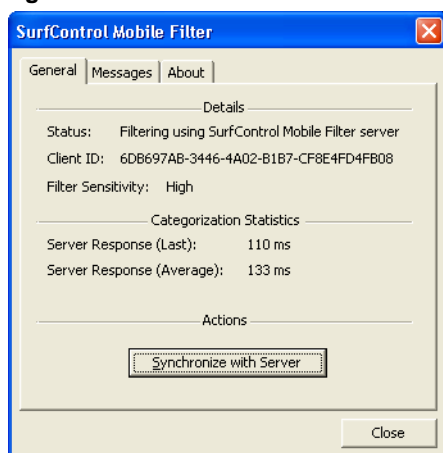
Mobile Filter client properties can be seen by double-clicking the Mobile Filter notification area icon (see Figure 1-2). You can also right-click the icon and select **Open** from the pop-up menu. This will launch the Mobile Filter dialog box which contains the following tabs:

- General
- Messages
- About

### General

The General tab contains three sections:

Figure 1-2 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 Client 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.

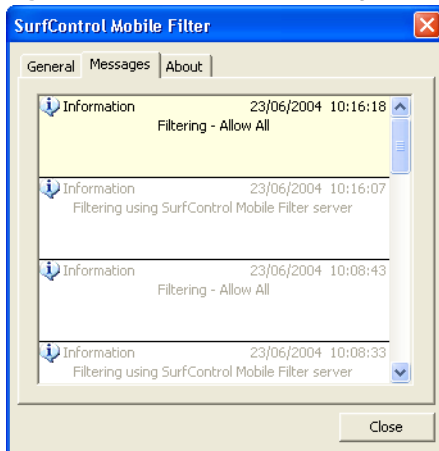


**Note:** Clicking Synchronize with Server will not update the last response time.

## 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, as shown in the figure below. These messages are stored in the Messages pane with the most recent at the top:

**Figure 1-3** Mobile Filter Messages tab

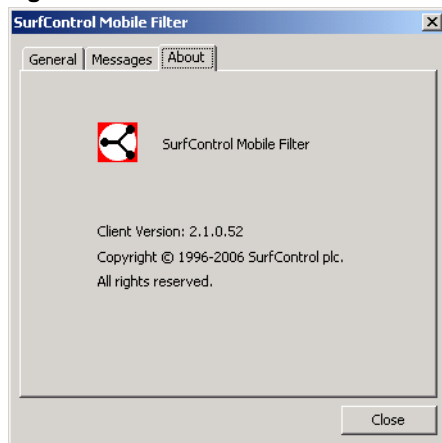


**Note:** If the client visibility is set to Medium, only messages concerned with blocked ports, tamper and upgrades will be displayed.

## About

The About tab informs you of the version number of the product, which can be used as a reference for upgrading.

Figure 1-4 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 unauthorized 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 its 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 its 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. The steps below details how 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.

- 1 Open Group Policy Manager on the Mobile Filter server.
- 2 Right-click the Default Domain Policy object and select Edit.
- 3 In the Group Policy Object Editor select Computer Configuration > Administrative Templates.

- 4 Right-click and select Add/Remove Templates.
- 5 In the Add/Remove Template dialog that displays click Add.
- 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 Open.
- 8 Click Close 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 Right click the Server URL and select Properties.
- 12 Select the Enabled option. This will enable the URL text box underneath.

Enter the following URL:

```
<protocol>://<server.domain:port>/scnmgw/scnmisapiext.dll
```

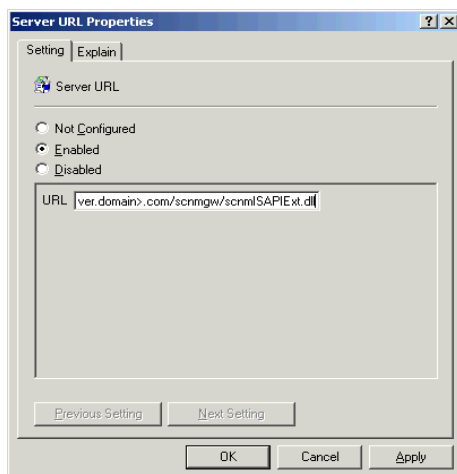
where <protocol> is either http or https and <server.domain:port> is the name of your server and domain. The optional port specification, :port, enables you to use a different port to the defaults of 80 for http and 443 for https.



**Caution:** Do not alter the name, or the path to the dll.

The following options are available to select:

- **Not Configured** - A Group Policy URL has not been added.
- **Enabled** - The Group Policy URL will override the default Gateway URL setting in the registry.
- **Disabled** - The Group Policy URL has been added but it has been disabled. The default Gateway URL will be used.



- 13 Click **OK**.

## **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, restart the computer and then reinstall 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 it's 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 it's own network and not someone else's. See 'CNDS' in the Mobile Filter Starter 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 Client 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 Client 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.

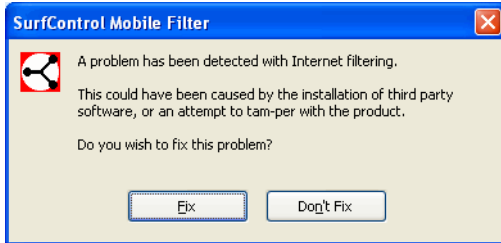
## REPAIRING INTERNET FILTERING PROBLEMS

If the Mobile Filter client detects a problem with its layered service provider (LSP), it will automatically attempt to repair it. This type of problem can be caused by tampering with the LSP, or the installation of filtering software from a third party manufacturer. The repair process is a privileged operation, so it relies on the logged in user having local administrative rights to be able to succeed. The following sections describe how to perform the repair on specific operating systems.

## Windows 2000 and XP

If your Mobile Filter client is installed on Windows 2000 or XP, and a problem is detected with internet filtering, perform the following:

- 1 From the repair prompt , click **Fix** to start the repair process.



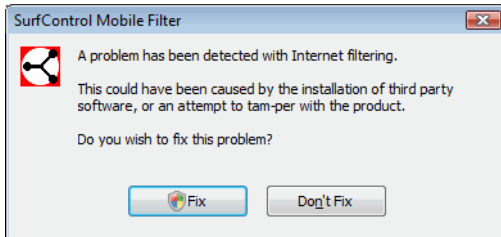
- 2 Once the repair has completed, click **OK**. The computer will restart. If the repair is unsuccessful, click **OK**, and contact your System Administrator to resolve the problem.

## Windows Vista

Windows Vista provides user security in the form of User Account Control (UAC). UAC enables System Administrators to run most applications with limited privileges, but gives the option to elevate certain programs which need Administrator authentication to run. Standard users follow the same process, but will have to supply an Admin password to perform program elevation.

If your Mobile Filter client is installed on Windows Vista, and UAC is enabled, it will need the permission of an elevated user to run the repair. This means that you will have to log in as Administrator, or as a standard user who knows the Administrator password. To start the repair, perform the following:

- 1 From the Mobile Filter repair prompt, click **Fix** to start the repair process.



- 2 You will need to elevate Mobile Filter in one of the following ways:
  - If you are logged in as Administrator, click **Continue**.
  - If you are logged in as a standard user, supply the Administrator password and click **Continue**.
- 3 Once the repair has completed, click **OK**, and restart the computer. If the problem could not be repaired, click **OK** and contact your System Administrator to rectify the problem.

## Appendix

[Comments on this Guide? .....](#) .page 30

[Technical Support .....](#) .page 31

[SurfControl Sales .....](#) .page 32

## COMMENTS ON THIS GUIDE?

---

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

Was this guide helpful? E-mail us at [documentation@surfcontrol.com](mailto:documentation@surfcontrol.com) to suggest changes or make a correction.

Version 5.5

May 2007

## TECHNICAL SUPPORT

---

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

- **Search our Knowledge Base** - Our new, constantly updated Knowledge Base contains articles, FAQs and glossary items to answer your questions about all SurfControl products.
- **Online Support Request** - 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 Web site <http://www.surfcontrol.com>