



Version 5.5

SurfControl Web Filter for Citrix

Administrator's Guide



NOTICES

Copyright © 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.

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.

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

COMMENTS ON THIS GUIDE?

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

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

Version 5.5

September 2006

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.
- 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>

CONTENTS

Notices	i
Comments on this Guide?	ii
Technical Support	iii
SurfControl Sales	iii
Finding your way around	1
The SurfControl Client Administrator	1
Administrator Menus	3
File	3
Edit	3
Find	3
View	4
Configure	5
Tools	6
Help	9
Client Details section	10
Client Description	10
Offline Action	11
Dealing with unfiltered ports	12
Setting filter sensitivity	13
Visibility Level	14
Password	14
Other Configuration	15
Ports that can be filtered	15
Ports that can be monitored	15
Security and Web Filter for Citrix	15
The Web Filter for Citrix Client	16
Client Status Icons	16
Client properties	16
Client Security	19
Group Policy and client configuration	20
Connections between client and server using SP2	21
Troubleshooting	22
Client not filtering	22
Client not picking up change to offline action	22

FINDING YOUR WAY AROUND

This guide describes how to configure SurfControl Web Filter for Citrix. Web Filter for Citrix gives you the following functionality:

- Secure LDAP communication between Web Filter for Citrix and the domain controller.
- The ability to configure the port between the client and Web Filter for Citrix 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 Web Filter for Citrix clients see Chapter 8 - Rules Administrator of the Web Filter Administrators Guide. Web Filter for Citrix users and hosts can be selected from the Who objects tab.

THE SURFCONTROL CLIENT ADMINISTRATOR

The Client Administrator (see Figure 1) is where you manage your SurfControl Web Filter for Citrix clients. It contains a configurable description of each remote device with it's settings. Select **Client Administrator** from the **Start > Programs > SurfControl Web Filter for Citrix** menu.

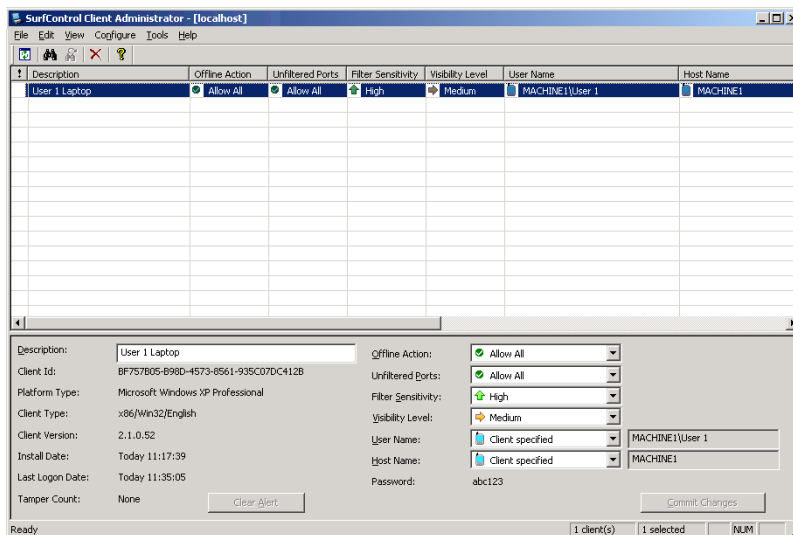


Figure 1 The SurfControl Client Administrator

Finding your way around

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, 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.

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.

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

Procedure 1 Changing client properties

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

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 Web Filter for Citrix clients to be administered by the Client Administrator. Only Web Filter for Citrix 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.

Procedure 2 Searching for clients

Step	Action
1	Choose Find from the Edit menu or click  on the toolbar.
2	The Find dialog box will appear.
	<div data-bbox="316 1375 890 1606" data-label="Image"> </div> <div data-bbox="925 1360 1249 1394" data-label="Caption"> <p>Figure 2 The Find dialog</p> </div> <div data-bbox="928 1417 1410 1575" data-label="List-Group"> <ul style="list-style-type: none"> • Find what:- enter the text you want to find. • Search Columns - select the check-boxes that correspond to the columns that you want to search. </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 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 Web Filter for Citrix 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 it communicates with the Web Filter for Citrix server.

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** - Selecting Reset Widths restores the 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

Server Settings - specify the global default user name and host name, the maximum amount of concurrent client sessions after a period of offline activity and whether the Web Filter for Citrix server is accepting new clients.

New Client Defaults

Certain default settings are used when a client is connected to the Web Filter for Citrix 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.

Procedure 3 Configuring New Client Defaults.

Step	Action
1	Select New Client Defaults from the Configure menu.
2	<p>In the New Client Defaults dialog box, enter the following information:</p> <ul style="list-style-type: none"> • Offline Action: - set how the client will behave if the Web Filter for Citrix server becomes unavailable. See "Client Details section" on page 10 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 12. The default is Allow All. • Filter Sensitivity: - set how much filtering is carried out. See "Setting filter sensitivity" on page 13 for more details. The default is Medium. • Visibility Level - set how much of Web Filter for Citrix the user sees. The default is Medium. <ul style="list-style-type: none"> - Full - all features and pop-ups will be visible to the user. - Medium - the Client UI will be available but pop-ups will be disabled. - Stealth - no features will be available to the user. Only pop-ups containing a critical message will be shown. • Preferred Host Name: - set the name for the device that is being filtered. See "Host Name" on page 14 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 14 for more details. The default is client specified.

Step	Action
	<div data-bbox="306 346 742 682" data-label="Image"> </div> <div data-bbox="790 331 1157 363" data-label="Caption"> <p>Figure 3 New Client Defaults</p> </div> <ul style="list-style-type: none"> • Offline Action: - How clients behave if the server goes offline. • Unfiltered Ports: - How Web Filter for Citrix treats ports that are not included for filtering. • Filter Sensitivity: - The strength of filtering. • Visibility Level: - How much of the client interface the user sees. The default is medium. • Preferred Host Name: - The name of the device being filtered. • Preferred User Name: - The name of the user of the device being filtered.
3	Click OK .

Client Upgrade Details

Client Upgrade Details specify whether there is an upgrade available for Web Filter for Citrix clients. See **Upgrading Clients** in **Chapter 3** of the *Installation Guide* for more details.

Adding Corporate Web Filters

Not applicable for Web Filter for Citrix.

TOOLS

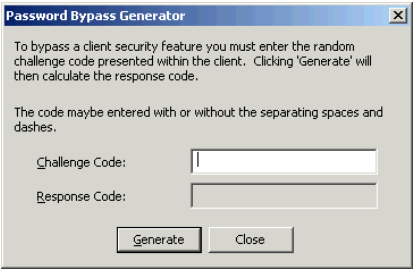
The **Tools** menu enables you to set passwords and override them in the event of problems.

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.

Procedure 4 Using Password Bypass Generator

Step	Action
1	If you cannot remember the uninstall password when asked for it, click Password Bypass in the Uninstall Password dialog box on the client.
	<div data-bbox="306 1644 710 1759" data-label="Image"> </div> <ul style="list-style-type: none"> • Password - Enter the Client password. • Password Bypass - Start to generate a bypass for this password if you can't remember it.
2	A Password Bypass dialog displays with a code in the Challenge Code: field.

Step	Action
3	Go to the SurfControl Client Administrator select Tools > Password Bypass Generator .
4	Copy the Challenge Code from the client into the Challenge Code: field.
	 <ul style="list-style-type: none"> • Challenge Code: - The code that you copy from the Client Password Bypass dialog. • Response Code: - The code that displays when you click Generate. • Generate - Generates the Response Code.
5	Click Generate .
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 OK to proceed with uninstalling the client.

Set Server Pass-phrase

During the installation of the Web Filter for Citrix client on to a user's device, it registers with the Web Filter for Citrix server and its details are written to the Web Filter for Citrix 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

- The Web Filter for Citrix 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 Web Filter for Citrix server.

SOLUTION

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

- After the administrator has created the new Web Filter for Citrix 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 `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.

Procedure 5 Setting a new Pass-phrase

Step	Action
1	Opening the Web Filter for Citrix Administrator, will show a message telling you that no Server Pass-phrase has 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.
3	Enter a new pass-phrase and confirm it: The new password must be between 8 - 16 characters long.
	<div data-bbox="290 1018 699 1272" data-label="Image"> </div> <ul style="list-style-type: none"> • Enter existing pass-phrase - This will be grayed out if no pass-phrase has been set. • Enter new pass-phrase - The new pass-phrase that you want to add. • Confirm new pass-phrase - The same pass-phrase entered again for confirmation.
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 to do this.

Procedure 6 Changing a Pass-phrase

Step	Action
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 - 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

About

The About box contains information such as the version number of the Web Filter for Citrix 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 Web Filter Client Administrator.

Table 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 "Client properties" on page 16 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 Web Filter for Citrix client.
Client Version	Identifies the version number of the Web Filter for Citrix client.
Install Date	Date on which the Web Filter for Citrix client software was installed on the selected device.
Last Logon Date	Date the client last made an Internet request that was logged by the Web Filter for Citrix Administrator.
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's installation process and is required if you uninstall the client.

OFFLINE ACTION

There may be times when the Web Filter for Citrix 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 one of the following: Allow All or Block All.

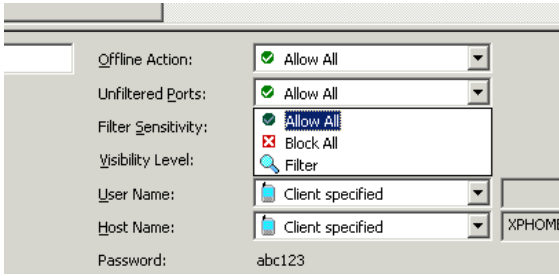
Procedure 7 Setting Offline Action

Step	Action
1	Select the client(s) that you want to set the offline action for.
2	Click the arrow on the Offline Action: list to expand it:
	<div data-bbox="300 751 820 1003" data-label="Form"> <p>Offline Action: <input checked="" type="checkbox"/> Allow All</p> <p>Unfiltered Ports: <input type="checkbox"/> Allow All</p> <p>Filter Sensitivity: <input type="checkbox"/> Block All</p> <p>Filter Sensitivity: <input type="checkbox"/> Automatic</p> <p>Visibility Level: <input type="checkbox"/> Medium</p> <p>User Name: <input type="checkbox"/> Client specified</p> <p>Host Name: <input type="checkbox"/> Client specified</p> <p>Password: abc123</p> </div> <ul style="list-style-type: none"> • Allow All - every Web request will be allowed (the default). • Block All - every Web request will be blocked.
3	Choose the type of Offline Action that you require, from the list.
4	Click Commit Changes to add the new Offline Action setting to the client in the Web Filter Client Administrator.

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 8 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 Unfiltered ports: 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>Unfiltered ports actions:</p> <ul style="list-style-type: none"> • Allow All - allow access to all unfiltered ports without contacting the Web Filter for Citrix 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 Web Filter for Citrix server to see if there is a rule set up for the port. • Filter - contact the Web Filter for Citrix Server to see if any rules are set to apply to all ports. </div> </div>
3	Choose the type of action that you require for unfiltered ports, from the list.
4	Click Commit Changes to save the new Unfiltered Ports: setting.

SETTING FILTER SENSITIVITY

Filter sensitivity enables you to set how much filtering is carried out by Web Filter for Citrix 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.

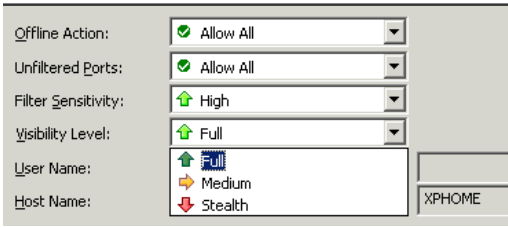
Procedure 9 Setting up Filter Sensitivity

Step	Action
1	Select the client(s) that you want to set the filtering sensitivity for.
2	Click the arrow on the Filter Sensitivity: list to expand it:
	<div data-bbox="316 655 842 928" data-label="Image"> <p>The screenshot shows a configuration window with several fields: Offline Action (Allow All), Unfiltered Ports (Allow All), Filter Sensitivity (High), Visibility Level (High), User Name, Host Name (XPHOME), and Password (abc123). The Filter Sensitivity dropdown menu is open, showing four options: High (with a green up arrow), Medium (with an orange right arrow), Low (with a red down arrow), and Automatic (with a blue down arrow).</p> </div> <div data-bbox="890 646 1404 1270" data-label="List-Group"> <p>Filter Sensitivity strengths:</p> <ul style="list-style-type: none"> • High - all non-HTTP ports and all HTTP requests are categorized. There may be a performance impact if the client is making a lot of requests on a slow internet connection. • Medium - all non-HTTP ports are categorized but only HTTP page requests are categorized while Images/sounds/style sheets, and XML requests are not categorized. • Low - all non-HTTP ports are categorized. For HTTP requests, the URL will be categorized and, if allowed the domain level part of the URL is cached for 3 minutes. • Automatic - the client chooses High, Medium or Low based on the average Web Filter for Citrix server response times and pre-configured thresholds. </div>
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 Web Filter for Citrix to hide some or all of its features from the user. There are three levels of visibility: Full, Medium and Stealth. If the client tries to access a port that is blocked, the user will see a warning pop-up, regardless of the visibility setting.

Procedure 10 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 Visibility Level: list to expand it:
	<div style="display: flex; align-items: flex-start;"> <div style="flex: 1;">  <p>The screenshot shows a configuration window with several settings. The 'Visibility Level' dropdown is expanded, showing three options: 'Full' (with a green up arrow icon), 'Medium' (with an orange right arrow icon), and 'Stealth' (with a red down arrow icon). 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'.</p> </div> <div style="flex: 1; padding-left: 20px;"> <p>Visibility levels:</p> <ul style="list-style-type: none"> • Full - Full visibility. All features and pop-ups will be visible. • Medium - 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. • Stealth - No features will be visible to the user. Only pop-ups containing critical messages will be shown. <p><i>Note: 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 Commit Changes to save the new Visibility setting.

User Name

The **User Name** is the name that the Web Filter for Citrix server uses when checking Internet requests against the rule set. It must be set to **Client specified**, otherwise the Web Filter for Citrix server will not be able to check the user name against rules.

Host Name

The **Host Name** specifies which Citrix server is handling an Internet request, so you can create rules to control what requests a specific Citrix server is allowed to make. It must be set to **Client Specified** otherwise the Web Filter for Citrix server will not be able to check the host name against enabled rules.

PASSWORD

This is the password that is needed to uninstall the Web Filter for Citrix Client.

OTHER CONFIGURATION

Once you can see your clients within the SurfControl Client Administrator you can select and edit any of them. These clients can then be added to SurfControl Web Filter for Citrix rules so that you can apply your company filtering policy to them.

PORTS THAT CAN BE FILTERED

To reduce the amount of communication between Web Filter for Citrix 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 Web Filter for Citrix client only filters ports that appear in active rules.

PORTS THAT CAN BE MONITORED

You can set the protocols to be monitored or unmonitored. The SurfControl Web Filter for Citrix client both filters and intercepts activity on those ports chosen to be monitored within the SurfControl Web Filter Manager, and informs the Web Filter for Citrix server.

Monitoring issues with Web Filter for Citrix

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 Web Filter for Citrix client and server communicate.

SECURITY AND WEB FILTER FOR CITRIX

SurfControl Web Filter for Citrix now offers support for secure connection:

- Between the Web Filter for Citrix server and your LDAP server
- Between the Web Filter for Citrix server and client.

Web Filter for Citrix server and LDAP server

A secure connection can now be made between the Web Filter for Citrix server and your LDAP server. You can change the security setting specified during installation, by editing the `SecureConnection` registry setting.

Procedure 11 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"> • 1 - gives a secure connection though there will be an impact on connection speed. • 0 - connection is faster but unsecure.

THE WEB FILTER FOR CITRIX 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 Web Filter for Citrix client is installed on the Citrix server 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 2:

Table 2 Client Icons

Icon	Description
	The Web Filter for Citrix Server is offline, and offline action is set to Allow All.
	Server is offline, and offline action is set to Block All.
	The product Icon. This is used while the client is using the Web Filter for Citrix Server for filtering.
	The client is waiting for the user to access the Internet before trying to log on to the Web Filter for Citrix server.

CLIENT PROPERTIES

Web Filter for Citrix client properties can be seen by double-clicking the Web Filter for Citrix Notification Area icon (see Figure 4). You can also right-click the icon and select **Open** from the pop-up menu. This will launch the Web Filter for Citrix dialog box which contains the following tabs:

- General
- Messages
- About

General

The General tab contains three sections:

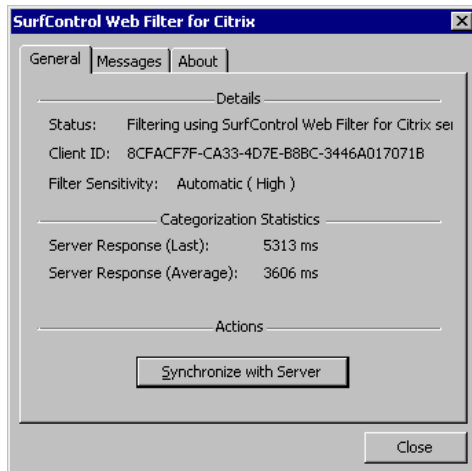


Figure 4 Web Filter for Citrix General tab

- **Details** - this shows a summary of the Web Filter for Citrix 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 Web Filter for Citrix Administrator) and the level of filtering sensitivity. See “Setting filter sensitivity” on page 13 for more information on this setting.
- **Categorization Statistics** - every time an Internet request is made, the Web Filter for Citrix client contacts the Web Filter for Citrix 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 Web Filter for Citrix server.



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

Messages

Every time there is a change in the way the Web Filter for Citrix client is filtering, it will display a message relating to what has occurred (see Figure 5). These messages are stored in the Messages pane with the most recent at the top:

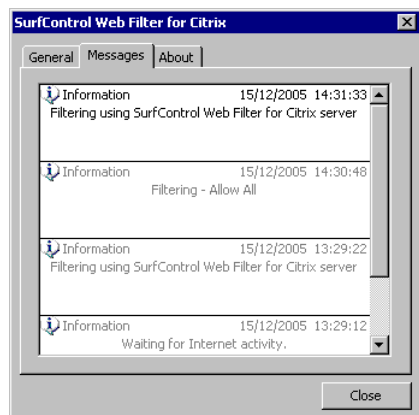


Figure 5 Web Filter for Citrix Messages tab



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 displays the version number of the product and can be useful as a reference for upgrading.

CLIENT SECURITY

During installation, the Web Filter for Citrix 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 Web Filter for Citrix server (and port) to be used by clients. Procedure 12 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 12 Applying Group Policy to the Gateway URL

Step	Action
1	Open Group Policy Manager on the Web Filter for Citrix 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 follows 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 Web Filter for Citrix Client then select Server URL in the right-hand pane.
11	Click the Properties hyper-link.
12	In the dialog that follows select the Enabled option. This will enable the URL text box underneath.
13	Enter the following URL: <code><protocol>://<server.domain:port>/scnmgw/scnmisapiext.dll</code> where <code><protocol></code> is either <code>http</code> or <code>https</code> and <code><server.domain:port></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> . Note: <i>Do not alter the name, or the path to, the dll.</i>

Step	Action
	<div data-bbox="304 348 699 772" style="border: 1px solid gray; padding: 5px;"> </div> <ul style="list-style-type: none"> • Not Configured - no Group Policy URL has 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. • URL: - the URL to the Web Filter for Citrix server.
14	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 Web Filter for Citrix client UI, and click **Synchronize with Server**.
- Restart the computer.
- Check the Web Filter for Citrix Web site for an up to date list of known problems.
- Re-run the Web Filter for Citrix client setup and try the Repair option.
- Uninstall the Web Filter for Citrix client software, restart the computer and then reinstall the software.

CLIENT NOT FILTERING

Web Filter for Citrix 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 Web Filter for Citrix 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.

CLIENT NOT PICKING UP CHANGE TO OFFLINE ACTION

When a Web Filter for Citrix client cannot communicate with the Web Filter for Citrix Server, perhaps because the server is offline, the Web Filter for Citrix 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 Web Filter for Citrix Server. This means that, although you may change the Offline Action for a particular client in the Client Administrator, this change will only come into effect once the client has been able to successfully logon to the Web Filter for Citrix server and pick up this new configuration setting.