



Web Filter

Version 5.0

SurfControl Web Filter for Citrix *Installation Guide for Service Pack 2*

Enterprise Threat Protection™



NOTICES

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

Copyright ©1998-2006 SurfControl plc. All rights reserved.

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

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

Version 5, printed December 2005.

CONTENTS

Notices	i
Introduction	1
Upgrading the Server.....	2
Installing Web Filter for Citrix Service Pack 2	2
The Web Filter for Citrix client	4
Upgrade each client individually	4
Using a Group Policy to silently upgrade or install clients	4
Installing new clients	7

INTRODUCTION

This guide describes how to install SurfControl Web Filter for Citrix Service Pack 2. It also explains how to install/upgrade clients to this service pack. Service Pack 2 enhances SurfControl Web Filter for Citrix to give you:

- 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.

UPGRADING THE SERVER

Before you start to install Web Filter for Citrix SP2 make sure that:

- SurfControl Web Filter for Citrix server version 5.0.1 is already installed on the server on which you intend to install Web Filter for Citrix SP2.
- All Web Filter for Citrix servers are disconnected from the Web Filter for Citrix database. This is to enable the database to be upgraded.

INSTALLING WEB FILTER FOR CITRIX SERVICE PACK 2

Procedure 1 Installing the service pack

Step	Action
1	Locate the Service Pack 2 executable file (setup.exe).
2	Double-click setup.exe to start the installation process.
Wizard Starts	
3	Navigate through the wizard clicking Next until you see the Server Pass Phrase Configuration screen.
Enter the Pass-phrase	
4	<p>In the Server Pass Phrase Configuration screen enter a Pass-Phrase and confirm it. You can change it at any time within the Web Filter for Citrix Administrator.</p> <p>In the event of a database failure and a new one having to be created, the pass-phrase enables the client to identify itself to the Web Filter for Citrix server. The server can then accept the client and write it's details to the new database without the client having to be reinstalled.</p> <p>For more information see 'Set Server Pass-phrase' in the Administrator Menu's section of the Web Filter for Citrix Administrator's Guide.</p>
	<div data-bbox="312 1289 922 1759" data-label="Image"> </div> <div data-bbox="979 1289 1423 1759" data-label="Caption"> <p>Figure 1 Server Pass-Phrase Configuration</p> <ul style="list-style-type: none"> • Enter Pass-Phrase - Enter a pass-phrase. • Confirm Pass-Phrase - Re-enter the pass-phrase. <p>Note: <i>The Pass-phrase MUST be between 8 - 16 characters long.</i></p> </div>
5	Click Next> to continue.

(Sheet 1 of 2)

Step	Action
Set security	
6	<p>This dialog enables you to use a secure SSL connection to your Active Directory server.</p> <p>To change this setting after upgrading, edit the <code>SecureConnection</code> registry setting. See 'Changing the security of Web Filter for Citrix' in the Miscellaneous Tasks section of the Administrator's Guide.</p>
7	<div data-bbox="316 533 922 982" data-label="Image"> </div> <div data-bbox="979 512 1406 810" data-label="Text"> <p>Figure 2 Secure Active Directory Connection Configuration</p> <ul style="list-style-type: none"> • Non - Secure Connection - To use a standard LDAP port to contact the Active Directory server. • Secure Connection - To use a secure SSL connection. This will be slower than an unsecure connection. </div>
8	Click Next> to Continue.
9	Click Next> in the Ready to install screen to start the install.
Finish	
10	In the InstallShield Wizard Complete screen, click Finish .
(Sheet 2 of 2)	

THE WEB FILTER FOR CITRIX CLIENT

When you have installed the Service Pack, SurfControl recommends that you upgrade all of your existing clients to enable them to make use of the new functionality that has been introduced. If you choose not to upgrade your clients, they will continue to function correctly, but the visibility setting will be disabled and the pass-phrase functionality will be unavailable. New clients will automatically pick up these benefits when they are installed. There are three ways to upgrade or install clients:

- Upgrade or install each client individually.
- Use a group policy to silently upgrade or install clients the next time the devices boot up.
- Upgrade or install clients via a network upgrade.

UPGRADE EACH CLIENT INDIVIDUALLY

If you do not have the mechanism for rolling out updates automatically you will need to upgrade each client individually. You can also inform users of available updates so that they can uninstall the client themselves. This installation can be started from a web page or by directing users to a directory containing the upgrade executable files. For direct installation, or for installing via a web page the upgrade interface is the same:

Procedure 2 Client upgrade

Step	Action
1	When the upgrade, starts the user will see the Welcome screen followed by the License Agreement.
2	Once they have accepted the license and clicked Next a Ready to install screen will show a status bar indicating how the upgrade is progressing. No dialogs that require any input from the user will be seen.
3	Once the Finish screen appears the user will need to reboot their device to finish the upgrade.

USING A GROUP POLICY TO SILENTLY UPGRADE OR INSTALL CLIENTS

You can now upgrade or install the clients of SurfControl Web Filter for Citrix remotely without the user's interaction via Active Directory and Group Policy. After the administrator deploys the software, it is available for installation the next time the client computer reboots. To configure group policies you must have a domain running Active Directory. Any computers that you intend to manage must be members of this domain, and be seen within Active Directory Users and Computers. To use Remote Install you need to:

- Create an MST file.
- Create a group policy.

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.

Step 1 - Create an MST file

Before you can configure a group policy software installation, it is necessary to create an .mst file that contains the configuration options relevant to your environment. The minimum amount of information required within the .mst file for a client installation are the name (or IP address) of the Web Filter for Citrix server and the un-installation password. If required, the following items can also be entered:

- **Client description** - this will be the same for each client installed using the group policy
- **Port** - The port over which communication between the client and the server can be specified. IIS must be configured to support communication over the selected port
- **Secure communications** - You can choose to have secure (https) communication between the client and the server. IIS must have a certificate installed to allow SSL and the clients must all trust the issuing certificate authority.

Procedure 3 Creating an MST file

Step	Action
1	Place the Web Filter for Citrix Client install files in a directory that is shared with all computers in Active Directory. This folder must allow read access for all domain computers.
2	Navigate to the Tools directory of your Web Filter for Citrix server and locate the <code>scgenmst.vbs</code> file.
3	<p>Copy and run this script from the Active Directory server where you are hosting the Web Filter for Citrix.msi (this is the Web Filter for Citrix.msi that you copied as the source file):</p> <ul style="list-style-type: none"> • source - the source msi file: enter the name "SWF Citrix.msi". • destination - the destination mst file: enter a name for this file. • /server:<name> - the Web Filter for Citrix server name (or IP address). • /passwd:<password> - the client password. <p>You can also enter the following values if required:</p> <ul style="list-style-type: none"> • /descr:<description> - enter a description of the client. This description will be seen in the Web Filter for Citrix Administrator. • /port:<port> - enter a port number if you do not intend to use port 80, which is the default. • /secure - use a secure connection. • /dump - show the settings on screen that will be added to the MST file.

Example command line

The following is an example of a command line with the necessary values entered:

```
cscript scgenmst.vbs "SWF Citrix.msi" customer.mst /server:mfserver /passwd:abc123
```

The transform file can also be used along with the MSI to set a machine group policy to install the client. See the Windows group policy documentation for more details.

Step 2 - Create a group policy

To use the following procedure you need to download and install the Group Policy Management console from the Microsoft website at: <http://www.microsoft.com/downloads>

Procedure 4 Creating a group policy

Step	Action
1	Select Administrative Tools > Active Directory Users and Computers from the Start menu.
Create an Organizational Unit	
2	If you wish to add devices to an existing organizational unit go straight to step 7. If you need to create a new one then follow steps 3-6.
3	In the Active Directory Users and Computers window, right-click your Active Directory.
4	Select New > Organizational Unit .
5	Enter a name into the New Object - Organizational Unit dialog and click OK .
6	The new object will appear in the domain tree. Select the Computers node to see all available computers (devices) in the right-hand pane.
7	Drag the devices that you want to install the Web Filter for Citrix client on to into the new organizational unit that you have just created.
Create Group Policy Object	
8	Right-click on the new organizational unit and select Properties .
9	Select the Group Policy tab, then click Open . This opens your organizational structure within the Group Policy Management console. <i>Note: If you did not download and install this software you will not see the option to open this program. You will need to close the Active Directory Users and Computers window and reopen it after you have installed the program, if you do it now.</i>
10	In the Group Policy Management window right-click the organizational unit that you have just created and select Create and link a GPO from here .
11	In the dialog that follows enter a name for the Group Policy Object. This name is then shown beneath both the organizational unit and the group policy object.
12	Right-click the new group policy object and select Edit...
13	The policy for Web Filter for Citrix must always be applied to computers, not users. Expand Computer Configuration then expand Software Settings .
14	Right-click Software Installation and select New > Package .
15	In the Explorer dialog, enter a UNC path to the .MSI installer file that you created in Procedure 4. Click Open . <i>Note: If you want to browse to the file rather than enter a UNC path, you must navigate via My Network Neighbourhood, otherwise the computers in your domain will not be able to access the .MSI installer file.</i>

Step	Action
16	In the Deploy Software dialog box select the Advanced option, then click OK .
17	You will now see the SurfControl Web Filter for Citrix Properties dialog. Select the Modifications tab, then click Add .
18	Navigate to the transform file (MST) using a UNC path then click Open .
19	Click OK .
20	The software package is listed under Software Installations ready for deployment. You can double-click the package to edit it at any time.



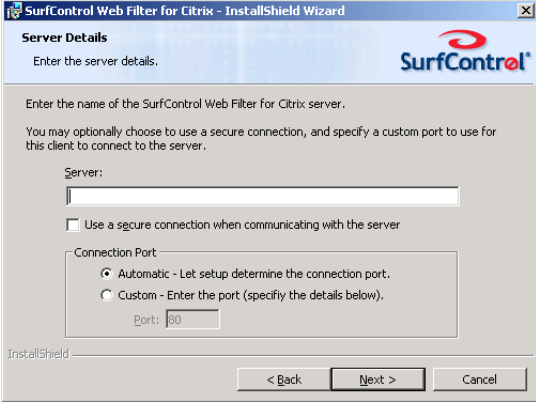
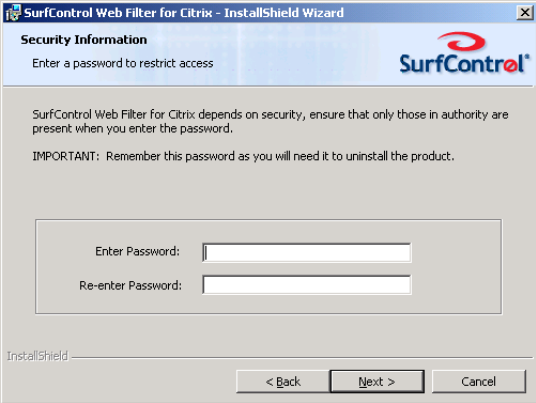
Note: It is not possible to uninstall clients via Group Policy. This must always be done on an individual basis.

INSTALLING NEW CLIENTS

Procedure 6 describes the client installation process. This is what you will see if you manually install a new client onto a device:

Procedure 5 Install process for the client

Step	Action
1	Start the Web Filter for Citrix client installation from your chosen location.
2	When you see the Welcome screen click Next to continue with the install.
3	If you select 'I Accept the terms in the license agreement' and click Next then you will see the Setup type dialog. Select a Setup Type: <ul style="list-style-type: none"> • Complete - a default installation and the recommended way to install the client. • Custom - enables you to specify the location to install to.
4	Click Next to see the Server Details dialog.
5	The Server Details dialog tells the client which Web Filter for Citrix server to connect to for categorization requests, and whether to make this a secure connection or not. The various options available in this dialog include: <ul style="list-style-type: none"> • Leave the 'Use a secure connection...' check-box deselected and the Connection Port at Automatic - this will make an unsecure connection over the default port 80. • Leave the 'Use a secure connection...' check-box deselected and select Custom in the Connection Port section - this will make a unsecure connection over the port that you enter into the Port field. • Select the 'Use a secure connection...' check-box and select Automatic in the Connection Port section - this will make a secure connection over port 443. • Select the 'Use a secure connection...' check-box and select Custom in the Connection Port section - this will make a secure connection over the port that you enter into the Port field. <p>Note: For a secure connection the Fully Qualified Domain Name needs to be entered.</p>

Step	Action	
		<p>Figure 3 The Server Details dialog</p> <ul style="list-style-type: none"> • Server: - the name of the Mobile Server. • Use a secure connection when communicating with the server - select to use a secure connection. • Automatic - port 80 will be used for an insecure connection, port 443 for a secure connection. • Custom - specify your own port.
6	Click Next .	
7	The next dialog you will see is the Security Information dialog where you can enter a password for this client. The password will be required when you try to uninstall the client, and will be visible within the Web Filter for Citrix Administrator.	
		<p>Figure 4 The Security Information dialog</p> <ul style="list-style-type: none"> • Enter Password - enter a password for this client. • Re-enter Password - confirm the password.
8	Click Next> .	
9	The next dialog is the Client Description dialog. The client description appears within the Web Filter for Citrix Administrator and enables the administrator to identify the client. Click Next> and progress through the installation to the Finish .	