



Version 5.5

SurfControl Mobile Filter

Starter Guide



NOTICES

©1996–2008, Websense Inc.

All rights reserved.

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published June 2008

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Websense Inc.

Every effort has been made to ensure the accuracy of this manual. However, Websense Inc., makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Websense Inc. shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Trademarks

SurfControl and Websense are registered trademarks of Websense, Inc. in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Microsoft, Windows, Windows NT, Windows Server, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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

Copyright (c) 2001-2004. The Apache Software Foundation. All rights reserved. Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at <http://www.apache.org/licenses/LICENSE-2.0>.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

This product contains software 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.

TABLE OF CONTENTS

Notices.....	i
Introduction.....	1
Why use Mobile Filter?	2
Pre-installation	3
Where to install.....	4
SurfControl Mobile Filter installed in a DMZ	4
SurfControl Mobile Filter installed in a main network location	4
System Requirements	5
Server	5
Client	6
Database Considerations	7
Database Platforms	7
SQL Server	8
Database Authentication	10
Installing the Server.....	11
Introduction.....	12
Installation Procedures	12
Changes to the Server.....	12
The Mobile Filter Server	14
Configuration Wizard	18
Installing Service Pack 3	31
Post Installation Tasks.....	35
Corporate Web Filter servers	35
Remote Administration and Mobile Filter.....	37
Uninstalling the Mobile Filter server	37
CNDS	38
Fine-tuning client filtering.....	38
Installing the Clients.....	43
The Mobile Filter Client.....	44
Manually Installing the Mobile Filter Client	45
Using Group Policy to Silently Install Clients	50
Before you start	50
Upgrading Clients	53
Upgrading your Mobile Filter clients	53
Uninstalling Clients	54
Tamper Protection	55
Appendix.....	57
Contact Technical Support	58
Sales and Feedback.....	60

Introduction

Why use Mobile Filter?page 2

WHY USE MOBILE FILTER?

SurfControl Mobile Filter enables you to extend your corporate Acceptable Use Policy beyond the walls of the office. With Mobile Filter you can manage the Internet use of mobile and remote employees. Mobile Filter uses a thin-client installed on a range of Internet enabled devices such as laptops and ties them into the corporate Internet usage policy to protect against the following problems:

- **Legal Liability**

Letting employees surf anywhere on the Internet can lead them to stray to clearly inappropriate sites; sexually explicit sites and those promoting violence, hate speech, and gambling. This kind of surfing can lead to lawsuits, harassment charges, and even criminal prosecution.

- **Productivity**

If an employee is accessing the Internet in company time with company property, you can ensure that it is for company use.

- **Network Security**

Protect against viruses and malicious content entering your work place via an employee using an external modem or Internet Service Provider (ISP).

Pre-installation

Where to install	page 4
System Requirements	page 5
Database Considerations	page 7

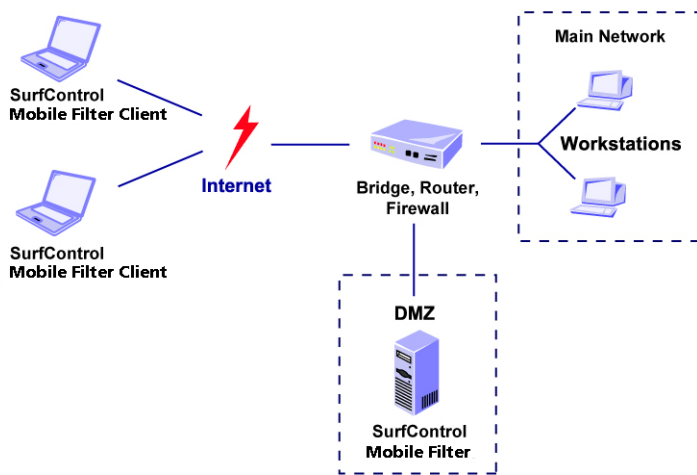
WHERE TO INSTALL

You must position the Mobile Filter server so that both internal and external clients can access it over TCP port 80.

SURFCONTROL MOBILE FILTER INSTALLED IN A DMZ

You can position the Mobile Filter server on a computer situated in the corporate network's demilitarized zone (DMZ) as in the figure below:

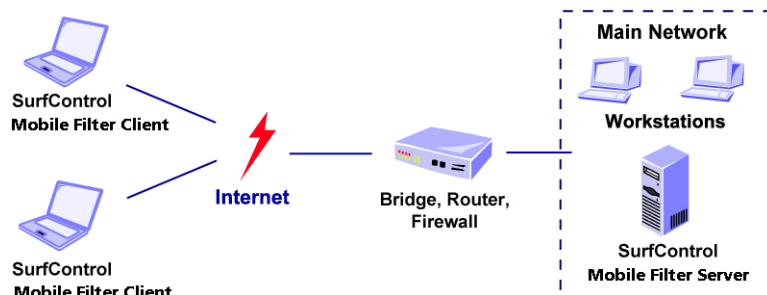
Figure 2-1 Mobile Filter within a DMZ



SURFCONTROL MOBILE FILTER INSTALLED IN A MAIN NETWORK LOCATION

In the figure illustrated below, the Mobile Filter server is installed within the main network. You need to configure your firewall to allow traffic on TCP port 80, providing this traffic is only going to this server:

Figure 2-2 Mobile Filter within the main network



SYSTEM REQUIREMENTS

You should check that the computers you will be using meet the system requirements, as outlined in the Server and Client sections below.

SERVER

Table 2-1 Mobile Filter server System Requirements

Component	Minimum	Recommended
Processor	Intel Pentium III	Intel Pentium IV
Memory	512 MB RAM	1 GB RAM
Supported Operating Systems (with latest Service Packs)	Windows 2000 Server Windows 2000 Advanced Server Windows Server 2003 Standard Edition Windows Server 2003 Enterprise Edition	
Disk Space	1 GB free	5 GB free
Supported database platforms (with latest Service Packs)	Microsoft SQL Server Express (Requires Windows Installer 3.1 if installing on a Windows 2000 computer) Microsoft SQL Server 2000 Microsoft SQL Server 2005 Note: SurfControl recommends that you have SQL Server Express or SQL Server installed before installing Mobile Filter.	
Applications	Microsoft Internet Information Services (IIS) 5 or higher. SurfControl Corporate Network Detection Service (CNDS). This is optional.	

Installing on Windows 2000 Server

Before you install the Mobile Filter server check that you have **Internet Services Manager** installed in the **Programs > Administrative Tools** menu. If this is not installed, perform the following steps to install it:

- 1 Open **Control Panel**.
- 2 Select **Add or Remove Programs**.
- 3 Select the **Add/Remove Windows Components** menu.
- 4 Select **Internet Information Services (IIS)**.
- 5 Click **Next** to begin the install process.

Installing on Windows Server 2003

The Windows Server 2003 default installation does not include IIS. Perform the following steps to install IIS:

- 1 Open **Control Panel**.
- 2 Select **Add or Remove Programs**.
- 3 Select the **Add/Remove Windows Components** menu.
- 4 Select **Application Server** and click **Details**.
- 5 Select **Internet Information Services (IIS)**.
- 6 Click **Next** to begin the install process.

You then need to configure IIS on a Windows Server 2003 computer by following the instructions below:

Configuring IIS on Windows Server 2003

- 1 From **Administrative Tools** in Control Panel, double-click **Internet Information Services (IIS) Manager**.
- 2 Expand the local computer tree and click **Web Service Extensions**.
- 3 Select **All Unknown ISAPI Extensions** and click **Allow**.
- 4 Install SurfControl Mobile Filter.

CLIENT

Table 2-2 Mobile Filter Client System Requirements

Component	Minimum	Recommended
Processor	Intel Pentium III	Intel Pentium IV
Memory	64 MB RAM	
Supported Operating Systems (with latest Service Packs)	Windows 2000 Windows XP Professional Windows Vista Business and Enterprise Editions	
Disk Space	10 MB free	
Applications	Microsoft Internet Explorer 5.5 or higher.	

DATABASE CONSIDERATIONS

Before you start to install Mobile Filter, you should decide:

- Which database platform you plan to use (SQL Server Express or SQL Server).
- How Mobile Filter will connect to the database (Windows or SQL authentication).

DATABASE PLATFORMS

Mobile Filter uses SQL Server Express, or a fully-licensed version of SQL Server 2000 or 2005. SurfControl recommends that you ensure your choice of database platform is installed and running before attempting to install Mobile Filter. Using SQL Server rather than SQL Server Express offers the following advantages:

- Allows greater scalability.
- The ability to fine-tune database performance.
- More suitable for environments with heavy Web traffic.
- SQL Server Express has a maximum size of **4GB**.

Mobile Filter connects to the database using a fully-qualified connection string. This string contains all the details required to connect to a database including database type, name of the server, user ID, password, and database name. Using a connection string does not require the creation of a Data Source Name (DSN). Therefore, any Mobile Filter server on the network can access the database without creating a link through the ODBC driver.

SQL Server Express

If you are not using SQL Server, you need to install SQL Server Express. SurfControl recommends you install your database platform before installing Mobile Filter. If you want to use SQL Server Express, be aware of the following:

- You must install **.NET Framework 2.0** before installing SQL Server Express.
- If installing on a **Windows 2000** computer, you must install **Windows Installer 3.1** before installing SQL Server Express.
- You must install SQL Server Express as a **Default Instance** when prompted during installation.
- You must install the **Database and Connectivity Components** when prompted during installation.
- You must perform the steps outlined in the Post SQL Server Express Installation Configuration detailed below before installing Web Filter.
- By default, SQL Server Express runs as a Network Service. When performing a database archive or restore, it needs to run with a local admin account to be able to access drive C.
- Microsoft specifies that the maximum size for a SQL Server Express database is **4GB**.

The following post SQL Server Express installation configuration is taken from the MSDN Blog entry: <http://blogs.msdn.com/sqlexpress/archive/2004/07/23/192044.aspx>, which explains the steps in more detail. The Post SQL Server Express Installation Configuration steps are as follows:

2

- 1 Make sure SQL Server Express is running correctly (assumes a default install).
- 2 Open a Command Prompt.
- 3 Type the following: `sqlcmd -S.\sqlexpress`
- 4 You should see a prompt like this: `1>`
- 5 Type: `Exit` to exit `sqlcmd`
- 6 Open the SQL Computer Manager.
- 7 Expand "Server Network Configuration".
- 8 Expand Protocols for "SQLEXPRESS".
- 9 Enable Np (for local and remote access).
- 10 Enable TCP (for local and remote access).
- 11 Restart SQL Server Express.

To access SQL Server Express database tables, you can use the Windows OSQL utility from the command prompt. For more details about the OSQL utility, visit www.microsoft.com.

For more information about SQL Server Express, visit: <http://www.microsoft.com/sql/editions/express/default.msp>

SQL SERVER

If you have SQL Server on your network, you should plan to create the database on that server (you can create and configure the database during the installation process).



Note: SurfControl recommends installing SQL Server on a dedicated server.

If you plan to use a SQL Server database, but have not installed Microsoft SQL Server, complete the following tasks before installing Web Filter:



Caution: Install SQL Server with the default setting of case insensitivity, including case insensitivity for Dictionary Order. Choosing case sensitivity may cause problems when installing Web Filter.

-
- 1 Install SQL Server on the designated server. This can be the same machine as the Web Filter server.
 - 2 Make sure your server has the minimum resources as listed in the table below:

Table 2-3 SQL Server minimum requirements on Web Filter server

# Users	Server Specification
<500	Intel Pentium IV, 2 GB RAM, 1.2 GHz processor, 10 GB hard drive.
500 - 1000	Intel Pentium IV, 3 GB RAM, 1.4 GHz processor, 20 GB hard drive.
1000 - 5000	Intel Pentium IV, 5 GB RAM, 1.4 GHz processor, 40 GB hard drive.
>5000	Intel Pentium IV, 7 GB RAM, 1.8 GHz processor, 60 GB hard drive.

- Configure SQL Server to limit memory and processors when running both Web Filter and SQL Server on the same computer.
 - There should only be one database owner (db_owner) per database.
 - If you need to have multiple user accounts with database access, the other users should only have db_datareader and db_datawriter permissions.

Reasons to Install SQL Server on a Dedicated Server

Use SQL Server 2000 or 2005 on a dedicated server if your organization:

- Needs to store large amounts of data (for example, you have a large number of users, high Internet activity, or need to retain data for an extended period).
- Requires more than one Web Filter server (collector) to consolidate data in a single database.
- Plans to store Web Filter and SurfControl E-mail Filter data on the same SQL Server installation.

Make sure your dedicated SQL Server has the minimum resources listed in the table below:

Table 2-4 SQL Server minimum requirements for large environments

# Users	Computer Specification
<500	Intel Pentium IV, 1 GB RAM, 1.2 GHz processor, 10 GB hard drive
500 - 1000	Intel Pentium IV, 2 GB RAM, 1.4 GHz processor, 20 GB hard drive
1000 - 5000	Intel Pentium IV, 4 GB RAM, 1.4 GHz processor, 40 GB hard drive
>5000	Intel Pentium IV, 6 GB RAM, 1.8 GHz processor, 60 GB hard drive

DATABASE AUTHENTICATION

Web Filter supports both Windows authentication and SQL authentication. SurfControl recommends SQL authentication for Mobile Filter.

Windows authentication

If you choose Windows authentication, make sure domain rights are correctly configured between the Web Filter server and the SQL Server. The Web Filter installer account requires SQL Server database creator rights.

SQL authentication

If you choose SQL authentication, you will need to create a SQL Server login specifically for Mobile Filter. This login is required for creating the database and should be used for all Mobile Filter database activities.

If you choose to connect to the SQL database using SQL authentication, make sure the SQL Server is configured to support SQL Server and Windows NT authentication.

Installing the Server

Introduction	page 12
The Mobile Filter Server	page 14
Configuration Wizard	page 18
Installing Service Pack 3	page 31
Post Installation Tasks	page 35
CNDS	page 38

INTRODUCTION

This chapter explains how to install SurfControl Mobile Filter. There are four stages to the installation process.

Table 3-1 Installation Workflow

Stage	Description
Database platform preparation	If you have chosen SQL Server Express for your database platform, download and install it from the Microsoft Web site. See Installing SQL Server Express (optional) on page 13.
Product installation and Configuration Wizard	Install Mobile Filter (complete installation).
Remote Administration	If you want to administrate the Mobile Filter server from a remote location, install the Remote Administration client on the remote computer. Install the VCA client if required.
Report Central	Download and install SurfControl Report Central from: http://www.surfcontrol.com

INSTALLATION PROCEDURES


This section contains the following procedures:

- 1 Installing SQL Server Express (optional) ([page 13](#)).
- 2 Installing Mobile Filter ([page 14](#)).


You can cancel the installation of Mobile Filter at any time by clicking **Cancel**. You will have to restart the installation process if you decide to install again at a later date.

CHANGES TO THE SERVER

Installing Mobile Filter makes the following changes to your server:

- Places a Web Filter icon  in the Notification Area at startup. From this icon, you can perform the following actions:
 - Stop or start the Web Filter and Scheduler services
 - Configure the Web Filter service settings.

- Serialize the product from the About dialog box.

If the Web Filter Service has stopped the Mobile Filter icon  becomes grayed out.



Note: On a Mobile Filter Remote Administration client, the grayed out icon is placed in the Notification Area to indicate that the service is not running locally.

- Adds necessary registry entries.
- Creates the SurfControl_WebFilter database.
- Adds the following services:
 - Web Filter service
 - Scheduler service
 - Remote Administration service
 - Audit Logger service
 - Virtual Control Agent service (can only be started with a licensed version of Mobile Filter)

Installing SQL Server Express (optional)

If you plan to use SQL Server Express for your database, you must install it in the following order before installing Web Filter:

- 1 Download and install .NET Framework 2.0 from <http://msdn.microsoft.com/netframework/>
- 2 If you are performing the installation on a Windows 2000 computer, download and install Windows Installer 3.1.
- 3 Download and install SQL Server Express from <http://www.microsoft.com/sql/editions/express/default.msp>



Note: You must install the Database and Connectivity Components when prompted during installation.

- 4 Perform Post SQL Server Express Installation Configuration as described in the section on [SQL Server Express](#).
- 5 You need to run SQL Server Express with a local admin account to be able to perform database management tasks such as Archive and Restore, as these tasks require access to drive C on your server. You will need to restart the server before installing SurfControl Mobile Filter.

You are now ready to begin installing the Mobile Filter server. Continue to [The Mobile Filter Server](#) installation instructions.

THE MOBILE FILTER SERVER

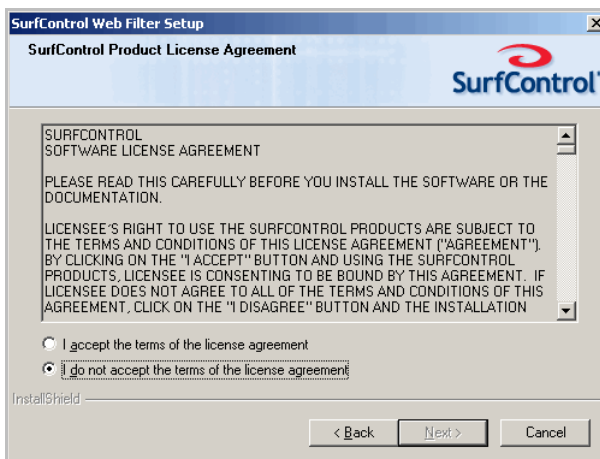
The following section outlines the instructions for installing SurfControl Mobile Filter on your server:

- 1 Locate the SurfControl Web Filter executable file (setup.exe).
- 2 Double-click setup.exe to start the installation process. The **Welcome** screen is displayed.



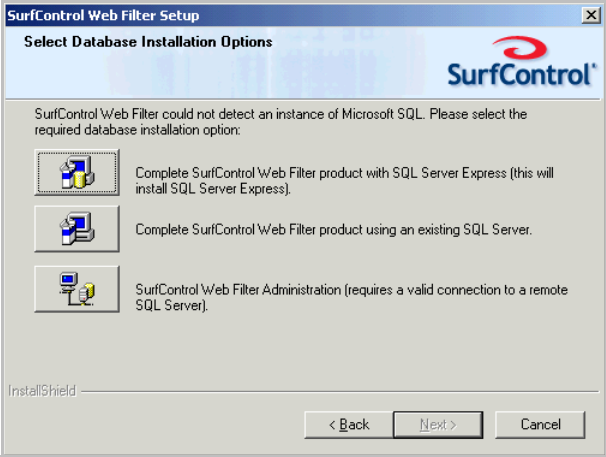
Click **Next**.

- 3 The **License Agreement** screen is displayed.



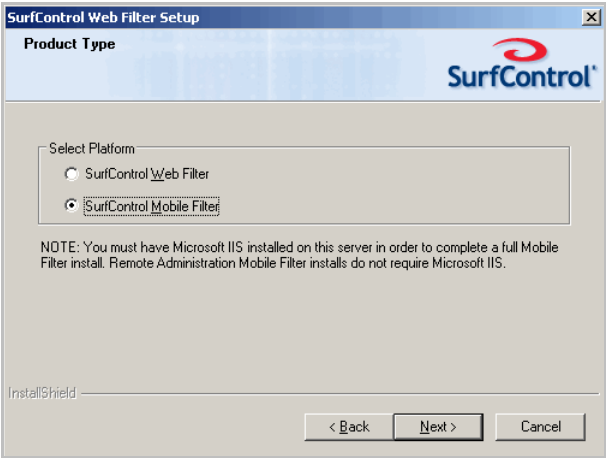
- i Select **I accept the terms of the license agreement**.
- ii Click **Next**.

- 4 If the setup program does not detect a suitable database, the **Select Database Installation Options** screen is displayed. (If you have already installed SQL Server Express or SQL Server) this screen will not be displayed.



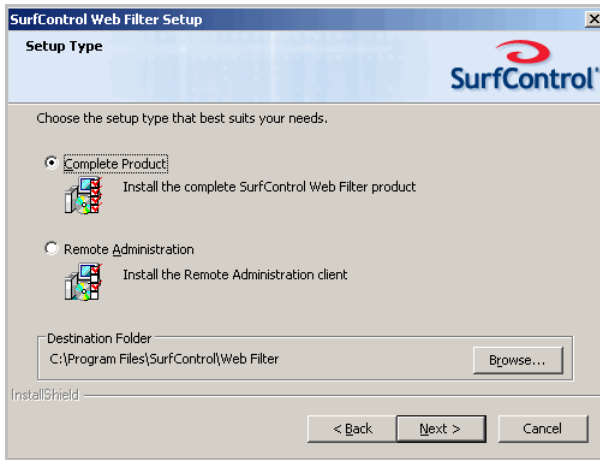
- i You can either:
 - Install the complete product which will also install SQL Server Express.
 - Install the complete product using an existing SQL Server database.
 - Install the Remote Administration version of Web Filter.
- ii Click **Next**.

- 5 The **Product Type** screen is displayed.



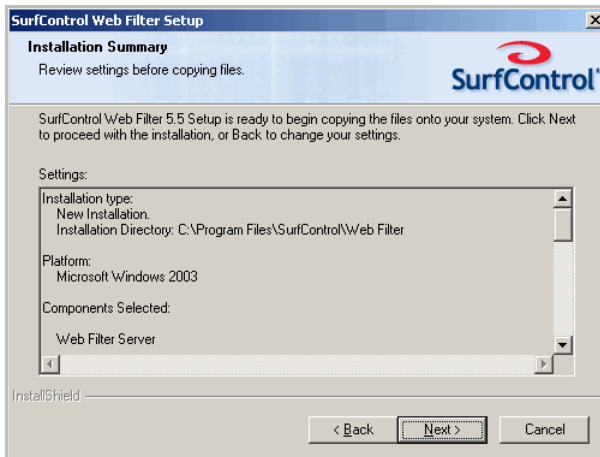
- i Select SurfControl Mobile Filter.
- ii Click **Next**.

6 The **Setup Type** screen is displayed.



- i Select **Complete Product**. The setup program installs Web Filter to a default path of c:\program files\SurfControl\Web Filter. If you want to install Web Filter in a different location on the server, click **Browse** to choose a new path.
- ii Click **Next**.

7 The **Installation Summary** screen is displayed.



Review your settings before starting the installation. When you are ready, click **Next** to begin copying the Web Filter files.

8 You have successfully installed Web Filter.



Click **Finish**. The **Configuration Wizard** will start automatically. See [Using the Configuration Wizard on page 18](#) for more details.

CONFIGURATION WIZARD

The wizard will launch after you have finished the complete installation process on your Web Filter server. The following instructions guide you through the wizard.

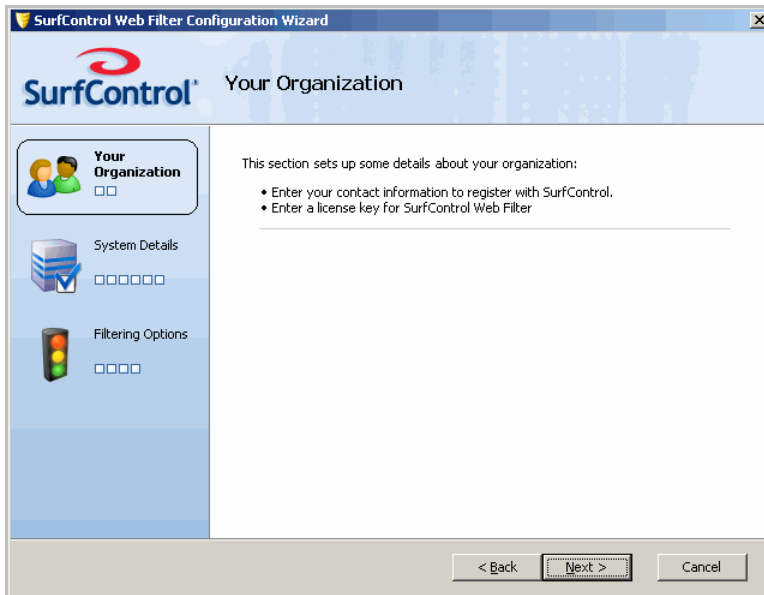
Using the Configuration Wizard

- 1 As soon as the setup program is complete, the Configuration Wizard will start.



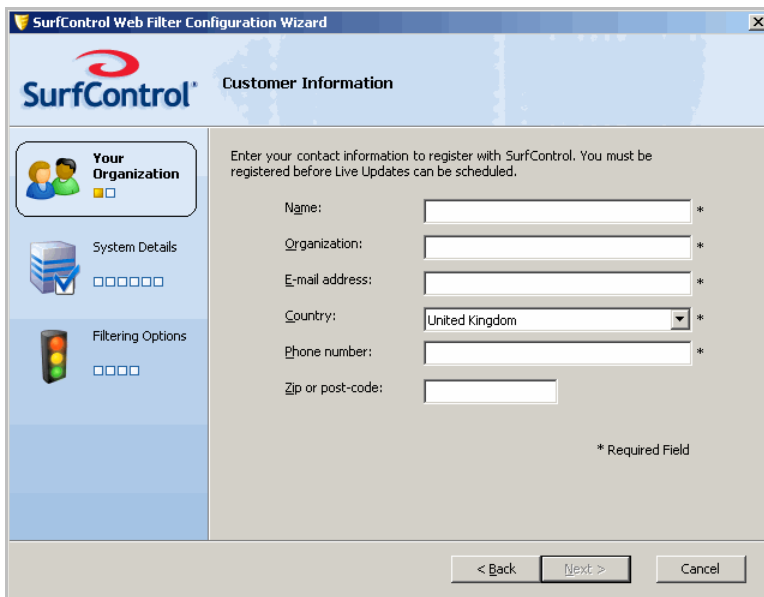
Click **Next**.

2 The **Your Organization** screen outlines the information you will enter in this section.



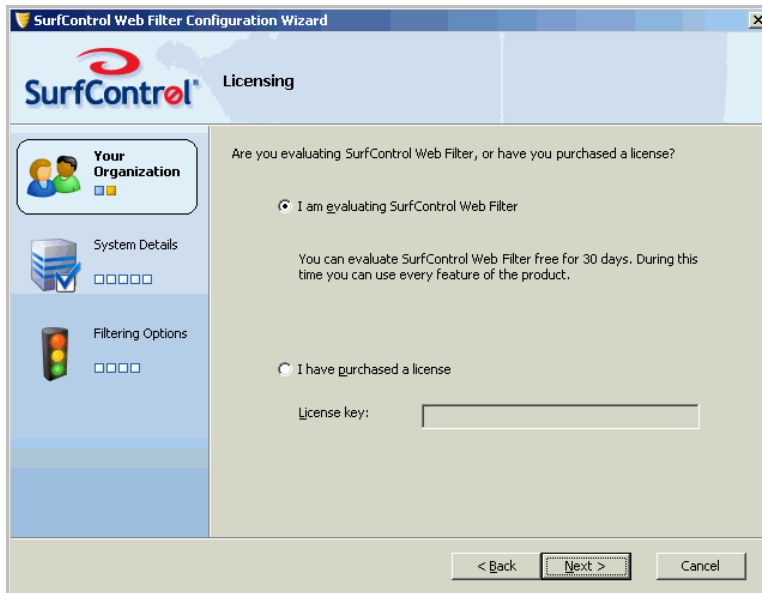
Click **Next**.

3 The **Customer Information** screen is displayed.



- i Fill in your details to register with SurfControl. Registered users can schedule live updates of the Internet Threat Database.
- ii Click **Next**.

- 4 The **Licensing** screen is displayed.



If you are an evaluating customer:

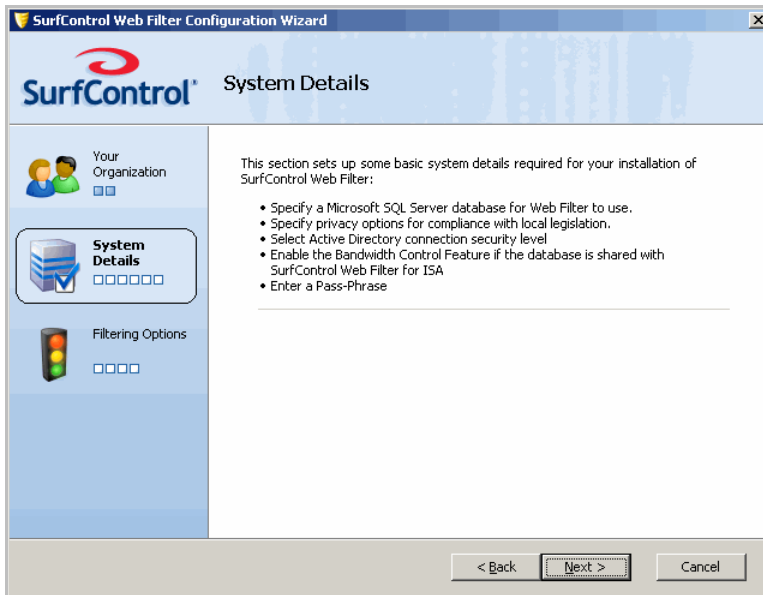
- i Select **I am evaluating SurfControl Web Filter**.
- ii Click **Next**.

If you have purchased a Web Filter license:

- i Select **I have purchased a license** and enter your license key.
- ii Click **Next**.

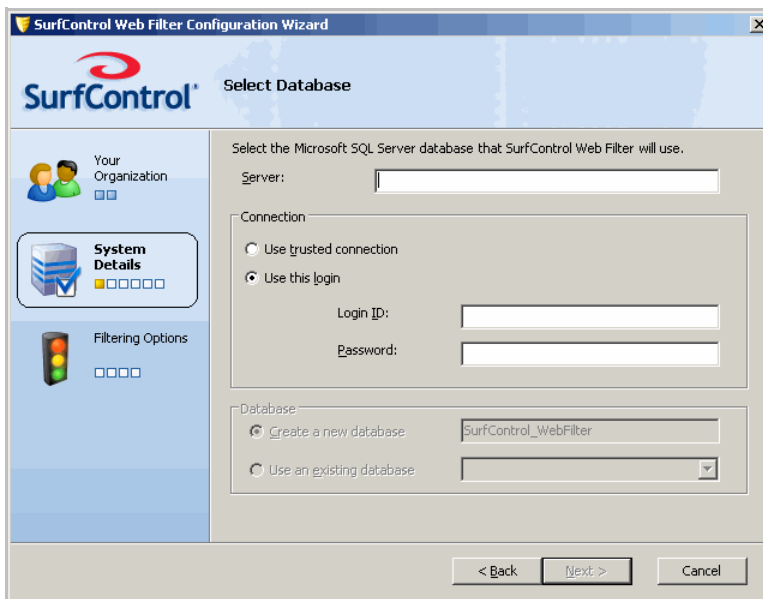
If you have purchased Web Filter but do not have a license key, contact SurfControl Sales.

5 The **System Details** screen outlines the information you will enter in this section.



Click **Next**.

6 The **Select Database** screen is displayed.



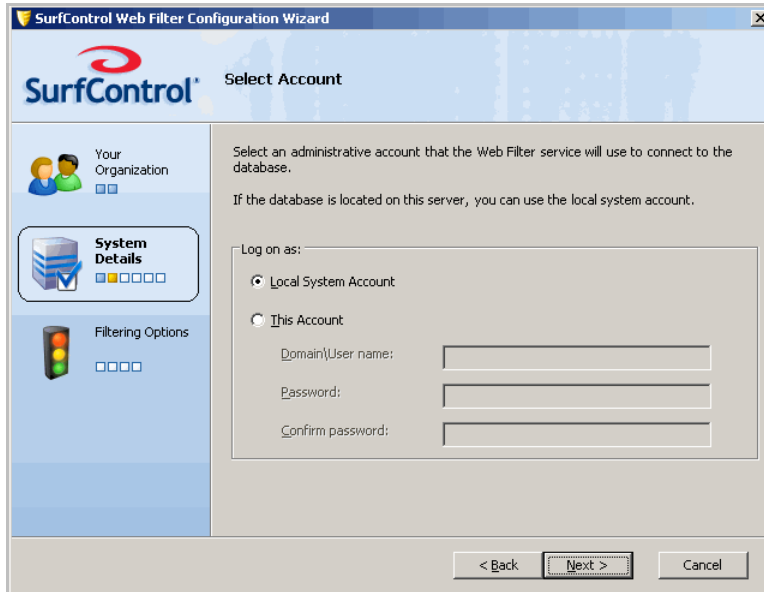
i Fill in the fields as follows:

- **Server:** enter the name or IP address of the server where your SQL Server Express or SQL Server database is located.
- **Connection:** specify how Web Filter connects to the database. Web filter uses either a SA username and password, or a trusted connection.
- **Database:** specify whether you want to use an existing Web Filter database, or create a new one.

3

ii Click **Next**.

7 The **Select Account** screen is displayed if you chose a trusted connection in step 6.

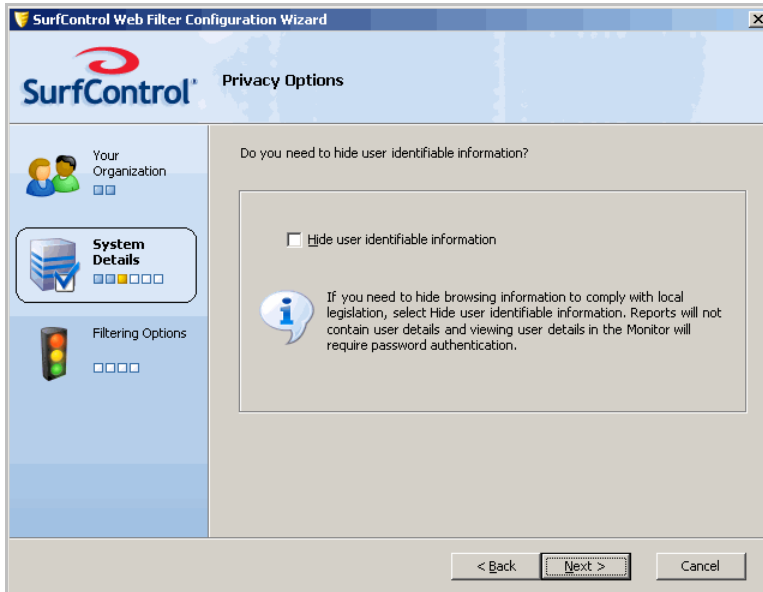


i You need to choose how Web Filter will connect to your database.

- If your database is located on the same server as Mobile Filter, you can select **Use Local System Account**.
- If your database is hosted remotely on another server, you need to select **This Account**. You need to enter the **Domain and User name**, with the corresponding **Password** for that user.

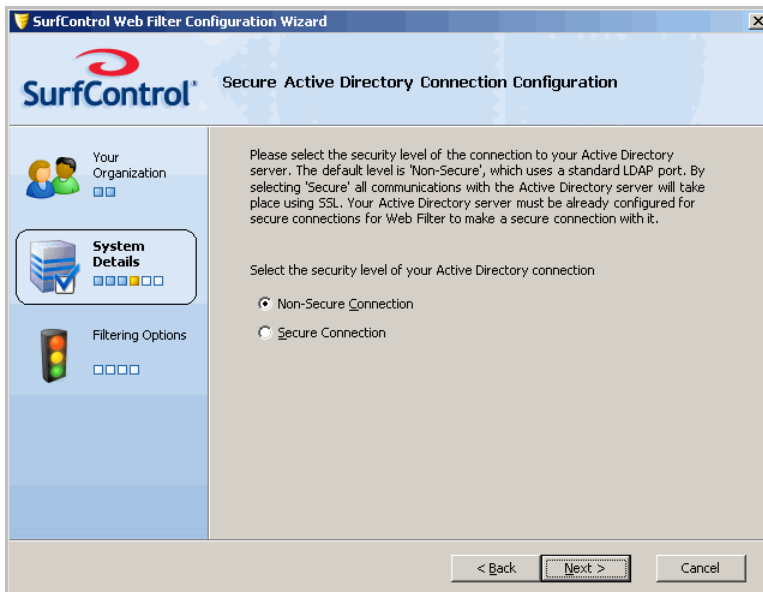
ii Click **Next**.

- 8 The **Privacy Options** screen is displayed. (This screen will not appear if you selected an existing database in Step 6).



- i If you need to hide user information to comply with regional legislation, select **Hide user identifiable information**.
- ii Click **Next**.

- 9 The **Secure Active Directory Connection Configuration** screen is displayed.



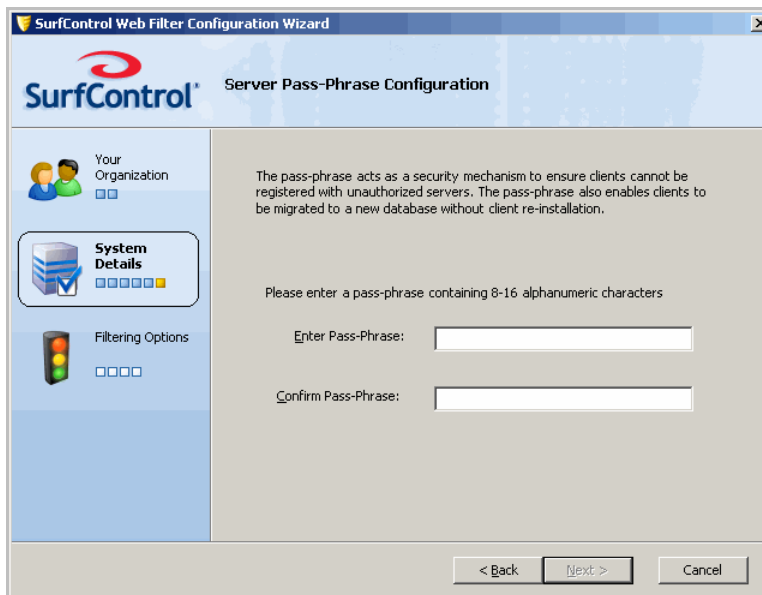
- i By default a non-secure connection is made to your Active Directory server. To change this to a secure SSL connection, select **Secure Connection**.
- ii Click **Next**. Web Filter will attempt a secure connection.

10 The **Enable the Bandwidth Control Feature** screen is displayed.



If you are installing Mobile Filter on an ISA Server platform, you can enable this feature. This allows you to prioritize traffic by applying a bandwidth control to a rule. Click **Next**.

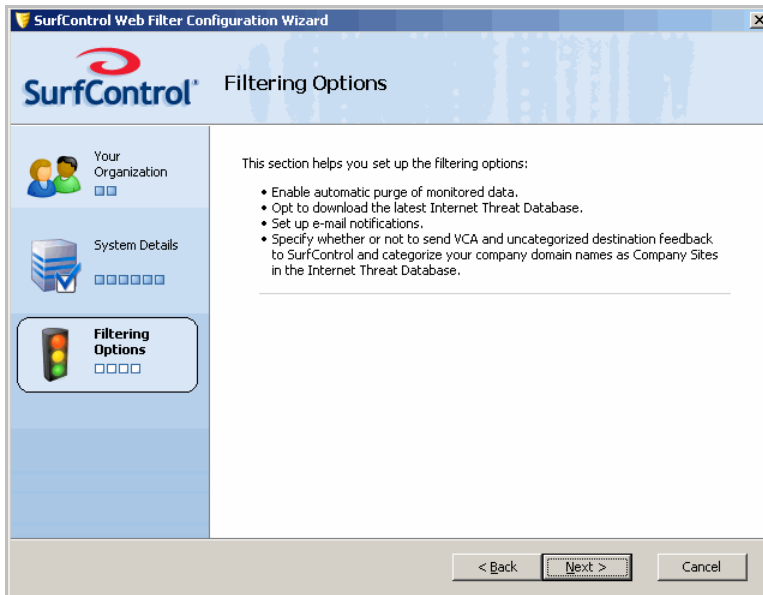
11 The **Server Pass-Phrase Configuration** screen is displayed.



The pass-phrase ensures that Mobile Filter clients only connect to the specified server. It is also used when performing a client upgrade.

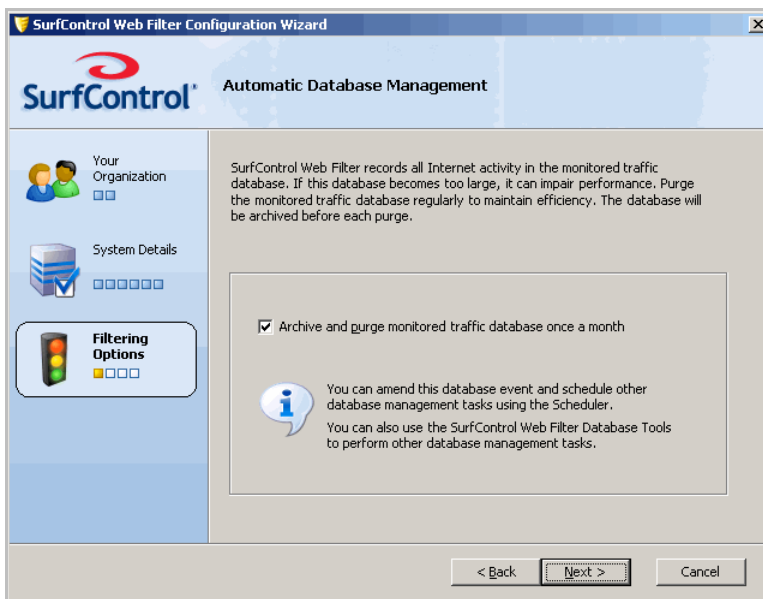
- i Enter an alphanumeric password of between 8 to 16 characters.
- ii Click **Next**.

12 The **Filtering Options** screen outlines the information you will enter in this section.



Click **Next**.

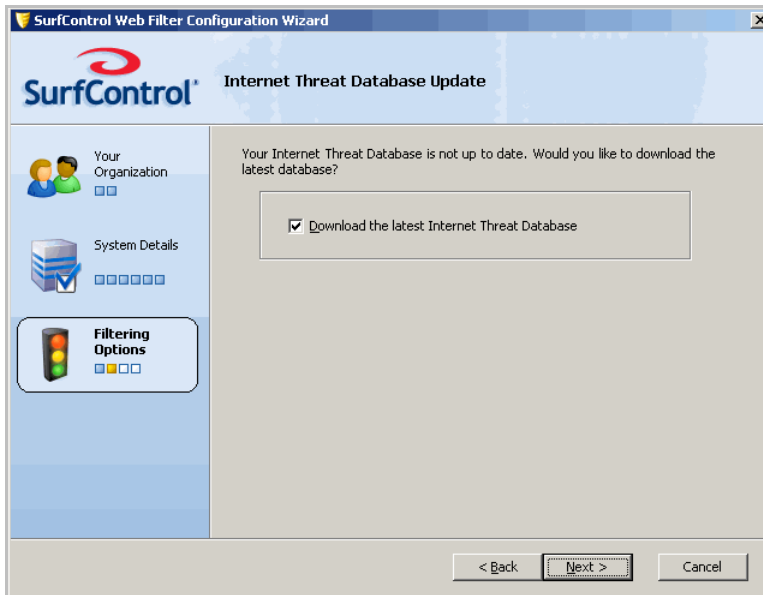
13 The **Automatic Database Management** screen is displayed.



To purge the Web Filter database automatically once a month:

- i Select **Archive and purge monitored traffic database once a month**.
- ii Click **Next**.

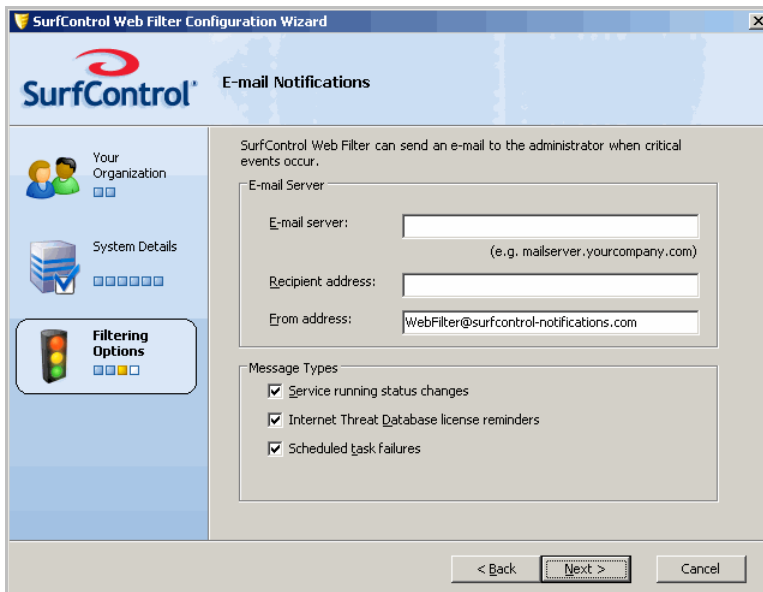
14 The **Internet Threat Database Update** screen is displayed.



For maximum protection you need the latest threat information.

- i Select **Download the latest Internet Threat Database**.
- ii Click **Next**.

15 The **E-mail Notifications** screen is displayed.

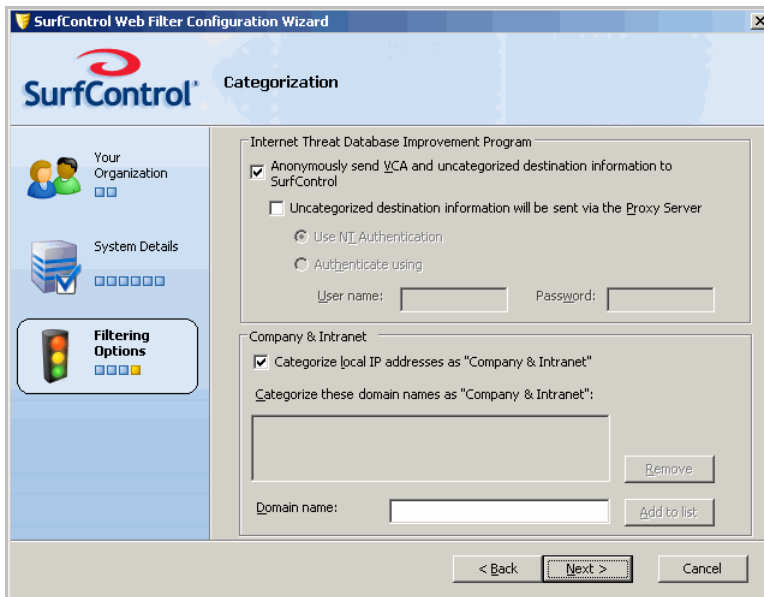


Web Filter can notify the systems administrator when system events occur.

- i **E-mail Server:** enter the name or IP address of the e-mail server for your domain. Web Filter will use this e-mail server to send notifications.
- ii **Recipient address:** enter the e-mail address of the systems administrator.

- iii **From address:** enter the address that the notification e-mails will be sent from.
- iv Now specify which **Message Types** you want to be notified of. Choose any or all of the following:
 - Service running status changes
 - Internet Threat Database license reminders
 - Scheduled task failures
- v When you have made your choices, click **Next**.

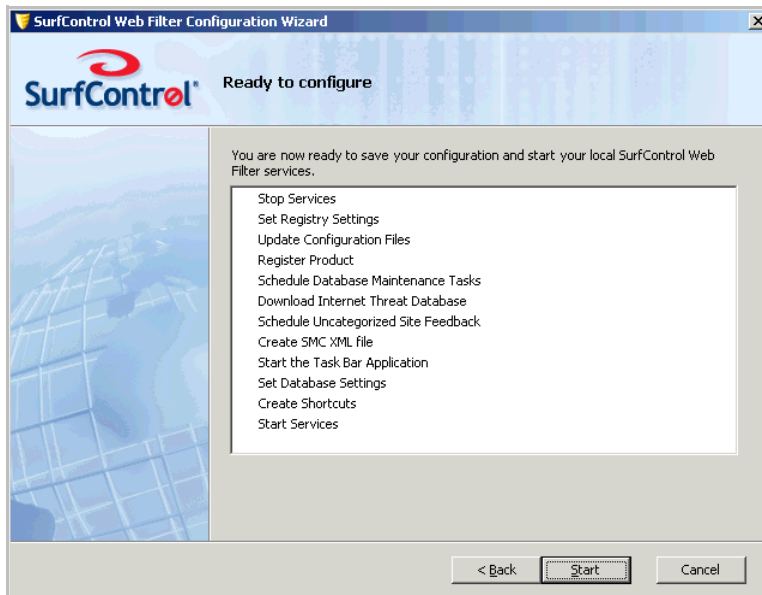
16 The **Categorization** screen is displayed.



When Web Filter encounters an uncategorized Web destination, it can send the details anonymously to SurfControl. This helps to improve the effectiveness of the Internet Threat Database for future updates.

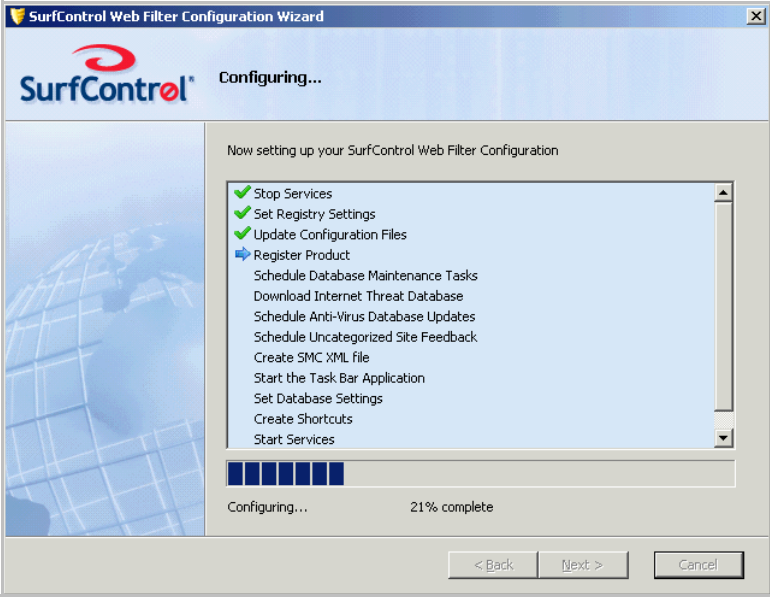
- i Clear the **Anonymously send VCA and uncategorized destination information to SurfControl** check box to opt out of sending this information.
 If you access the Internet via a proxy server, you can set the authentication for sending information via this method.
 You can also categorize your organization's domains as belonging to the Company and Intranets category. This means that when users visit your organization's Web site or intranet, their visit will be logged under this category.
- ii Click **Add** to add your domain (without entering the http://www prefix).
- iii Click **Next**.

- 17 The **Ready to Configure** screen shows a list of tasks that the Configuration Wizard will perform to configure Mobile Filter.



Click **Start**.

18 The **Configuring** screen is displayed.



A blue arrow shows the task currently in progress. As each task is completed, you will see a green check.

If there is a problem with a task, you will see a warning icon ⚠ next to it. You can either go **Back** to change your settings, or **Skip** the task and move on to the next one.

If there is a serious problem with a task, you will see a failure icon ❌ next to it. If this happens, the **Skip** button will be disabled and you must go back to correct your settings.



Note: If you skip a task, Mobile Filter may not filter traffic effectively.

19 The **Configuration Complete** screen is displayed.



You will need to install **SurfControl Report Central** to run reports on the internet traffic monitored by Web Filter. This is available from a product DVD or as a download from: <http://www.surfcontrol.com>.

Click **Finish**.

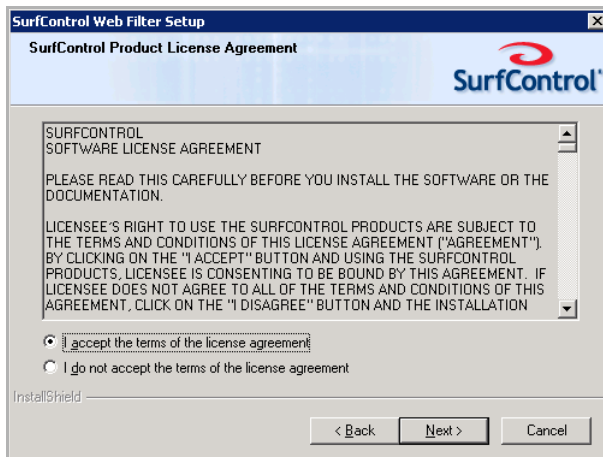
INSTALLING SERVICE PACK 3

This section contains information on Installing Web Filter Service Pack 3. You can cancel the installation at any time by clicking **Cancel**. You will have to restart the installation process if you decide to install it again at a later date.

- 1 Download the service pack from the SurfControl Web site to a suitable location.
- 2 Double-click **setup.exe** to start the installation process. A Welcome screen appears:

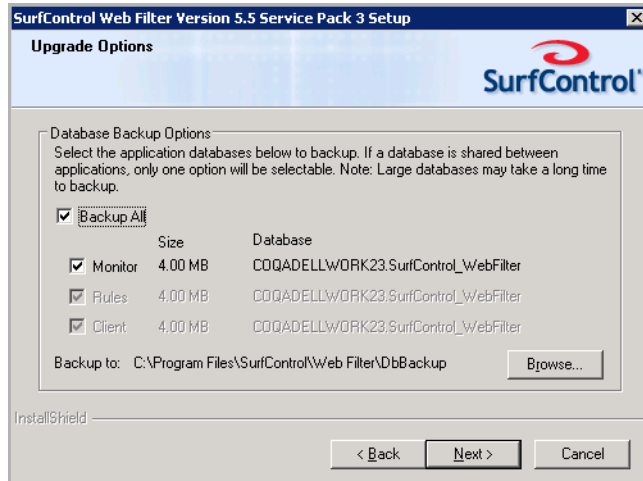


- 3 Click **Next**.
- 4 When you see the **License Agreement** screen, select **I accept the terms of the license agreement**:



- 5 Click **Next**.

- 6 You can now make a backup of your existing application databases using the Upgrade Options screen:



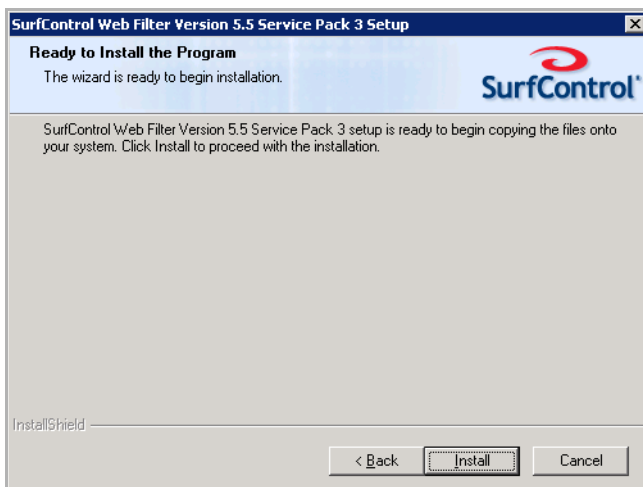
This enables you to 'roll back' to your previous database, should this be necessary:

- Select **Backup All** to backup all of the available databases
OR
- Select the database you want to back up from the list.

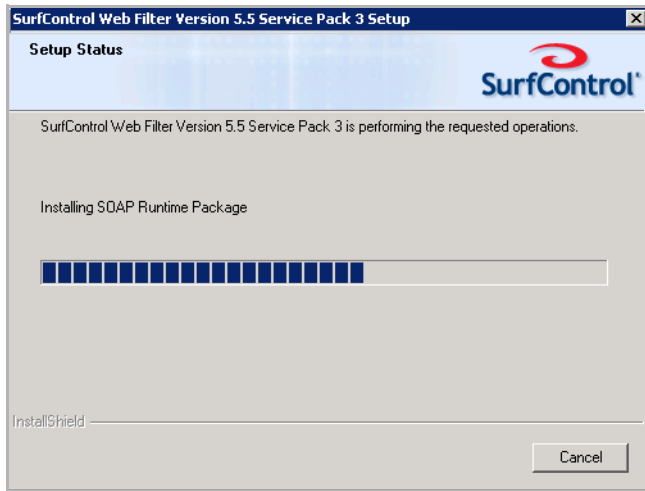


Note: If a database is shared with more than one application, you will only be able to select one of the applications that uses it.

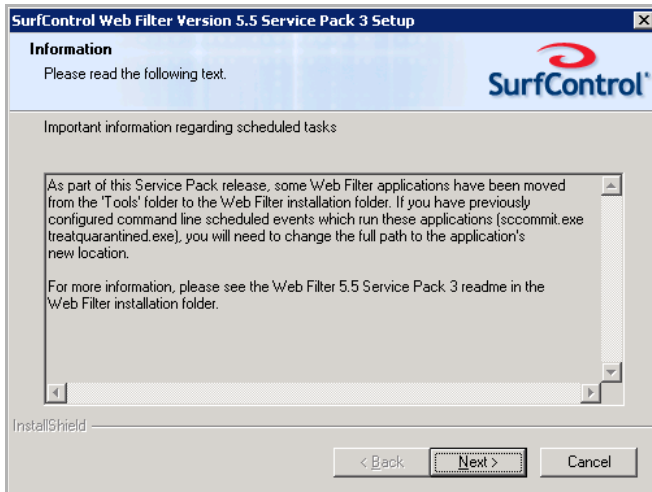
- 7 Click **Next**.
- 8 A screen informs you that the wizard is ready to install the service pack:



- 9 Click **Install** to start the installation. A progress bar indicates how the installation is progressing:



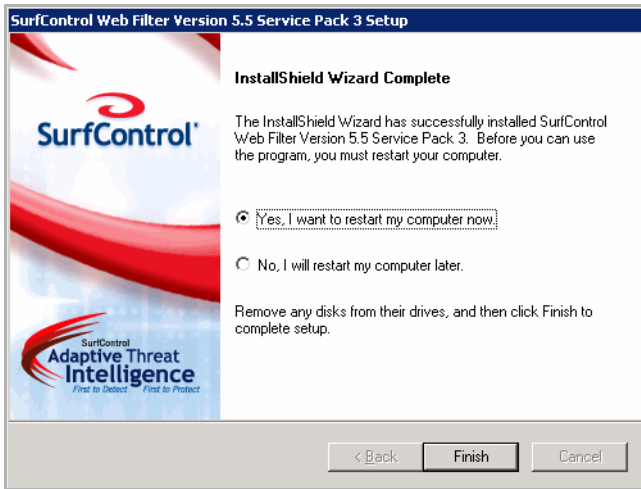
- 10 The next screen contains important information relating to changes that have been made to the product and how these changes may affect command line scheduled events:



Read this information carefully as it could impact on the automatic updating of your Internet Threat Database, or database maintenance tasks.

- 11 Click **Next**.

12 You should now see the Install Wizard Complete screen:



Choose when to restart the computer: now or later. You must restart the server before you can begin remote filtering.

13 Click **Finish** to finish the installation.

POST INSTALLATION TASKS

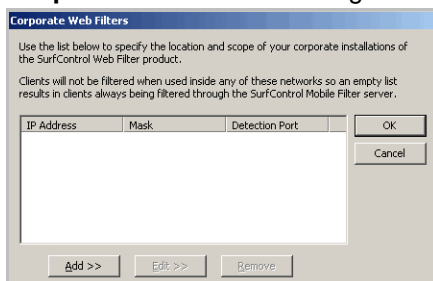
Follow the instructions outlined in this section if you need to add or remove corporate Web Filter server settings to Mobile Filter, install the Corporate Network Detection Service (CNDS), or uninstall Mobile Filter.

CORPORATE WEB FILTER SERVERS

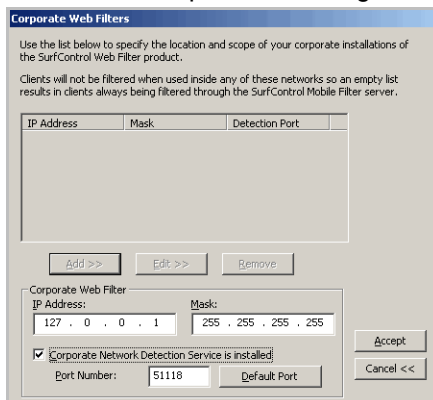
Mobile Filter has the ability to recognize when it is in the vicinity of an installation of the corporate Web Filter product, which will then take over filtering of the client.

Adding your Web Filter servers

- 1 Open the **Client Administrator** and select **Corporate Web Filters** from the **Configure** menu. The **Corporate Web Filters** dialog box is displayed.



- 2 Click **Add** to expand the dialog box.



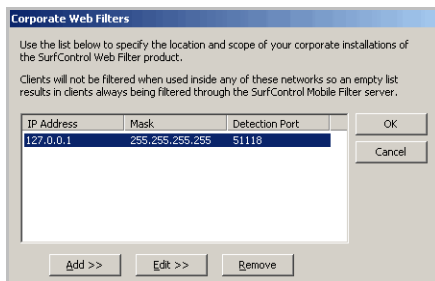
- i Enter the IP address of the Web Filter server, along with a subnet mask to show the range of IP addresses that Mobile Filter has to look for.
- ii Click **Accept** to add the new IP address and Mask to the list. You will see the new server appear in the list pane which will now be enabled.
- iii 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.

Making changes to server details

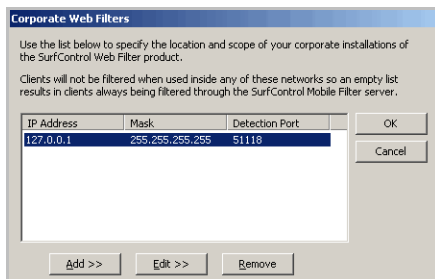
- 1 Select the Web Filter server from the list and click **Edit** to expand the dialog box.



- 2 Make the required changes to the server settings.
- 3 Click **OK**.

Removing a server

- 1 Select the Web Filter server from the list.



- 2 Click **Remove**.
- 3 Click **OK** to apply the changes.

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. See [CNDS on page 38](#) for more details. 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.

REMOTE ADMINISTRATION AND MOBILE FILTER

When you install Mobile Filter, you can choose to install the complete product, or a Remote Administration client from which you can administer components on your Web Filter server. If you choose to install the Remote Administration client, you will also have access to the Client Administrator.



Note: Before you install the Remote Administration client, you must have a complete installation of Mobile Filter installed on a computer that the Remote Administrator can be connected to.

For full details on how to install the Remote Administration Client, see the Starter Guide supplied with Web Filter.

UNINSTALLING THE MOBILE FILTER SERVER

To uninstall the Mobile Filter server, select **Add or Remove programs** from **Control Panel**.

CNDS

While your users are working away from the office, Mobile Filter will apply its filtering to the devices that they are using. However, you may already have SurfControl Web Filter operating within your office as a standalone product. This will be used to filter all users on your corporate network and will filter mobile users once they reconnect to your network.

For this reason, a Mobile Filter client can switch off when it detects that the device is connected to a corporate network, and recognizes that it is now in the same IP range as a listed Web Filter server. This saves on bandwidth and prevents duplication. Adding this information within the Client Administrator enables the Mobile Filter client to recognize when it is within the network of this server. As soon as the user connects to the company network Mobile Filter recognizes that its IP address is within the scope of the Web Filter server and stops filtering. Once the client is removed from the network and taken outside the range of the Web Filter server, Mobile Filter switches on once again and starts to filter the clients traffic using the Mobile Filter server.

FINE-TUNING CLIENT FILTERING

A Network Address Translation (NAT) device (firewall, router or computer) enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. This can conflict with SurfControl Mobile Filter, in that if you use a NAT device within your network then occasionally the client will see the IP addresses within the vicinity of another NAT device as those within the network of its own corporate Web Filter server. It will then switch off in the belief that the corporate Web Filter will carry on filtering, not realizing that it is not actually within its own network environment.

To stop this from happening you can install SurfControl's **Corporate Network Detection Service (CNDS)** on your corporate network's Web Filter server, which the Mobile Filter client can query as soon as it believes that it is within range of that server. If this service is present then the client will suspend filtering. If it is not, it will carry on filtering, assuming that an alternative form of filtering is not present.



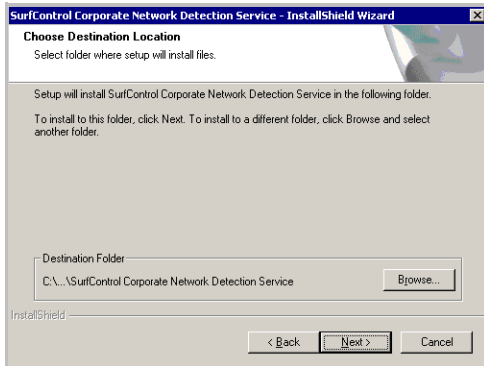
Note: If you are evaluating SurfControl Mobile Filter, and already have SurfControl Web Filter, you will need to install CNDS separately on the Web Filter server.

Installing CNDS

The CNDS must be installed on your corporate Web Filter computer.

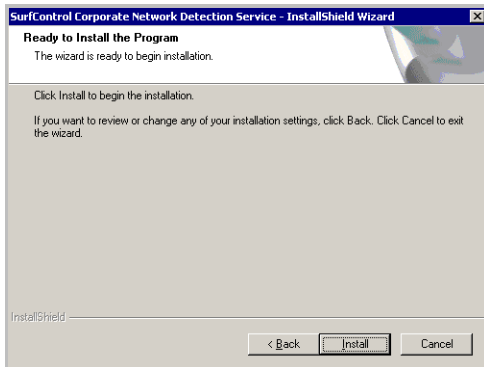
- 1 Download the Corporate Network Detection Service from the SurfControl website or navigate to the Corporate Network Detection Service setup.exe file on your SurfControl DVD.
- 2 Double click **setup.exe** to start the installation.
- 3 On the Welcome screen, click **Next**.

4 The **Choose Destination Location** screen is displayed.



- i Click **Browse** to specify a location other than the default.
- ii Click **Next** to continue.

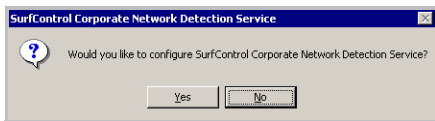
5 The **Ready To Install the Program** screen is displayed.



Click **Back** to change the Destination Location or click **Install** to start the installation. CNDS will be installed to the location specified.

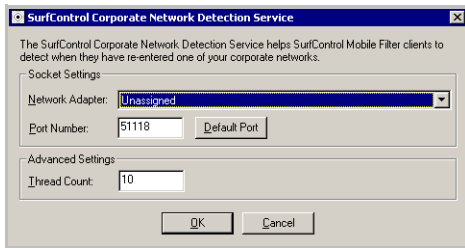
6 The **InstallShield Wizard Complete** screen is displayed. Click **Finish** to complete the installation.

7 A CNDS configuration screen is displayed.



- If you want CNDS to use its default settings click **No**.
- If you want to examine your settings click **Yes**.

8 If you chose **Yes** in the previous step, the **CNDS Configuration** screen is shown.



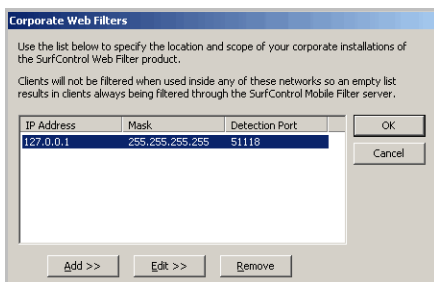
You can change the following settings:

- **Network Adapter** - Choose your network adapter from the drop-down list. 'unassigned' means that the service will listen on the default available network adapters.
- **Port Number** - Specify the port number on which the Server will await a connection from the client. This must be in the range of 1 – 65535. Click Default Port to return to the default setting of 51118.
- **Thread Count** - Set the maximum number of threads created to handle incoming requests.

Once you are happy with the settings click **OK** to apply them to the service.

Configuring the Corporate Web Filters for CNDS

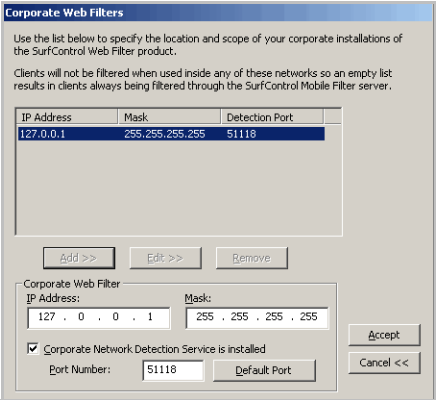
1 From the Client Administrator select **Corporate Web Filters** from the **Configure** menu.



You will see the Corporate Web Filters dialog box with the IP Address of your corporate Web Filter machine. If you have not entered the IP address of your corporate Web Filter to SurfControl Mobile Filter see [Adding your Web Filter servers on page 35](#).

Click **Edit**.

2 You will see the IP Address and Mask of the Corporate Web Filter machine in the text boxes within the Corporate Web Filter section where they can be changed if necessary:



- i In the **Corporate Network Detection Service** section, select **Corporate Network Detection Service is installed**.
- ii Check that the port for CNDS to listen on is the same as specified in Step 8.
- iii Click **Accept**.

You can change the settings for the CNDS at any time by going to the corporate Web Filter machine and selecting **Corporate Network Detection Service** from the **Start > All Programs > SurfControl Web Filter** menu. You will now see the SurfControl Corporate Network Detection Service Setup dialog box where you can configure these settings.

Installing the Clients

The Mobile Filter Client	page 44
Manually Installing the Mobile Filter Client	page 45
Using Group Policy to Silently Install Clients	page 50
Upgrading Clients	page 53
Uninstalling Clients	page 54
Tamper Protection	page 55

THE MOBILE FILTER CLIENT

You can install the Mobile Filter client software in one of the following ways:

- Install each client manually by either copying the setup files to a shared network drive that your remote devices will be able to access, or create a CD of the client software and then manually install it on to each device.
- Use Group Policy to perform a silent install.

Once you have installed your Mobile Filter server you can install the Mobile Filter client on any supported devices that you want to filter. Before you start to install the client make sure that you are in possession of the following:

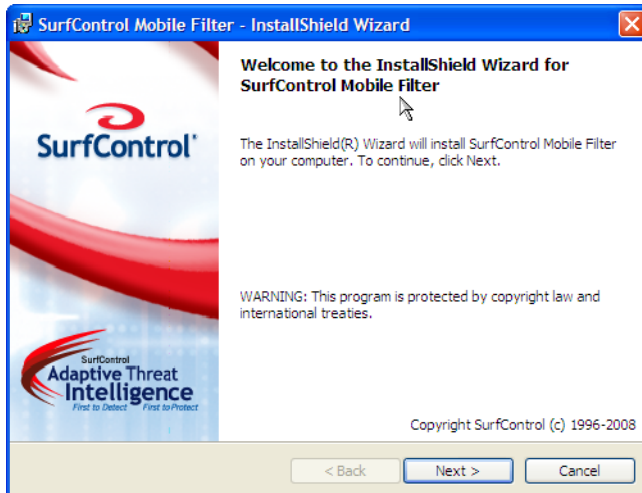
- The Fully Qualified Domain Name or IP address of your Mobile Filter server.
- A password that can be entered during installation to prevent a user from uninstalling the client.
- A description that will enable you to identify this client easily in the Client Administrator.
- Make sure that the device that you are about to install on meets the client system requirements listed in the [Pre-installation](#) section.



Note: To manually install the Mobile Filter client on computers running Windows Vista, use the **setup.exe**. To use the **Mobile Filter.msi** file, you must log onto Vista as Administrator or disable the User Account Control (UAC). You can use the msi file to deploy the client via GPO on this operating system regardless.

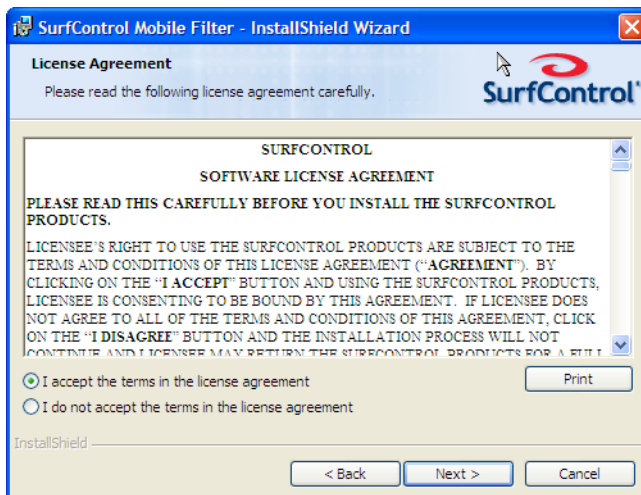
MANUALLY INSTALLING THE MOBILE FILTER CLIENT

- 1 Double-click the Mobile Filter.msi or setup.exe file to begin the client installation. The **Welcome** screen is displayed.



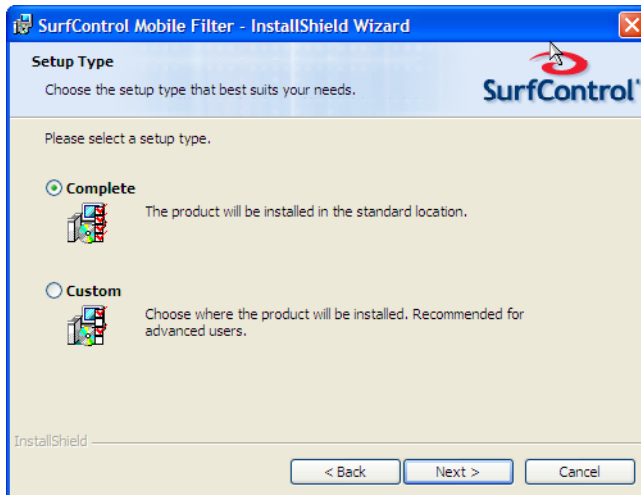
Click **Next**.

- 2 The **License Agreement** screen is displayed.



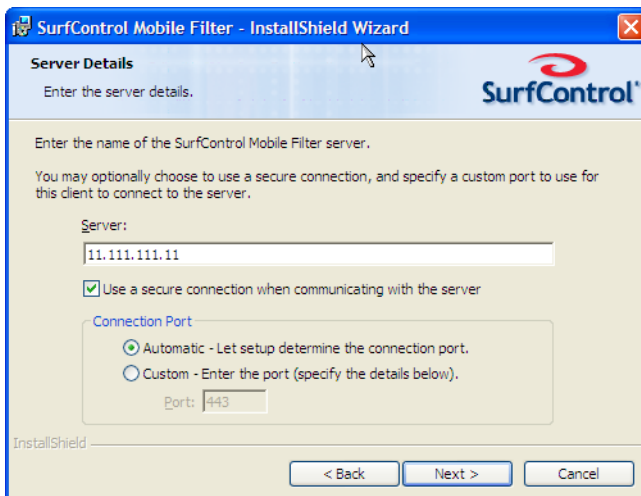
- i Select **I accept the terms in the license agreement**.
- ii Click **Next**.

- 3 The **Setup Type** screen is displayed.



- i SurfControl recommends that users select the **Complete** option.
- ii Click **Next** to continue.

4 The **Server Details** screen is displayed.



Enter the Fully Qualified Domain Name (FQDN) or IP address of the Mobile Filter server. This FQDN or IP address must be resolvable and contactable by the device when it is both internal AND external to your network. All client Internet requests will be monitored via this server.

- 5 Click **Next**. The installation tries to communicate with the specified server. If the server does not respond, an error message is displayed. This could be because you have entered the server name incorrectly or the server is not running. Other possible causes include incorrect firewall configuration.
- 6 The **Security Information** screen is displayed.

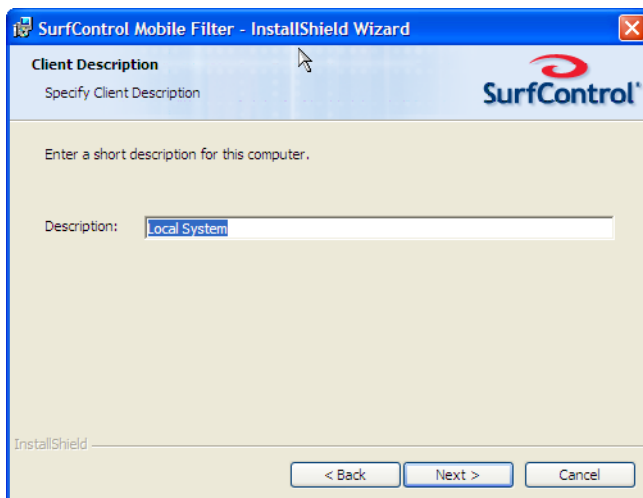


- i Enter and re-enter a password.

This is to ensure that anyone using this device cannot uninstall the Mobile Filter client via the bypass filtering mechanism. This password is available to the administrator in the Client Administrator interface. The password should be a maximum of 13 characters.

- ii Click **Next**.

7 The **Client Description** screen is shown.



- i Enter a description for this Mobile Filter client.

This identifies the client within the Client Administrator. When distributing the client installation executable, you may want to include a list of client descriptions for each device. Users can then enter the description allocated to their device.

- ii Click **Next** to continue. The client is ready to be installed.

8 The **Ready to Install the Program** screen is displayed. Click **Install** to continue.



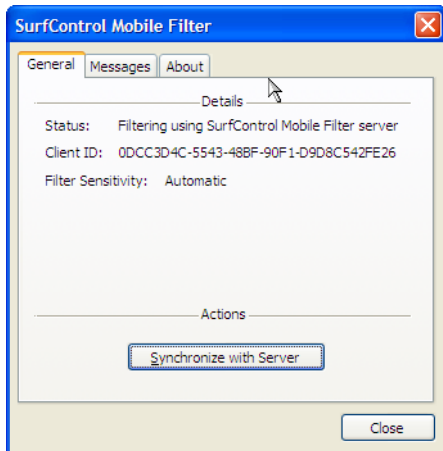
- 9 The **InstallShield Wizard Completed** screen is displayed.



Click **Finish** to complete the client installation. A SurfControl Mobile Filter icon appears in the toolbar.



Double-click it to view Mobile Filter client status. The status should report “Filtering using SurfControl Mobile Filter server.”



If it does not, click **Synchronize with Server**. If the status still does not report active filtering, check the following:

- You have a live Internet connection.
- You have restarted all browsers on the client.
- You have entered the server name correctly in the client installation wizard.
- The SurfControl Web Filter server is running.
- Your firewall is properly configured.

USING GROUP POLICY TO SILENTLY INSTALL CLIENTS

You can install the clients of SurfControl Mobile Filter remotely, through Active Directory and Group Policy. This gives you the ability to perform the installation without interaction from the user.

After you have deployed the software, it is available for installation the next time the client computer restarts. 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.

BEFORE YOU START

To install clients on to a Windows XP machine, you need to apply a policy setting that turns off fast network startup, otherwise each client will need to restart twice before software installation policy changes will be applied to it. To turn off Fast Logon Optimization, you can enable the following policy setting:

Computer Configuration\Administrative Templates\System\Logon\ Always wait for the network at computer startup and logon.

Refer to the Microsoft KB article: <http://support.microsoft.com/kb/q305293/> for more information on the issues of Fast Logon Optimization.

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 Mobile filter server and the uninstallation 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.

To create the .MST file:

- 1 Place the **Mobile Filter.msi** and the **Data1.cab** install files into a shared folder that can be accessed by all computers in the Active Directory. This folder must allow read access for all domain computers.
- 2 Navigate to the Web Filter directory of your Mobile Filter server and locate the **scgenmst.vbs** file.

3 Copy and run this script from the Active Directory server where you are hosting the mobile filter.msi (this is the mobile filter.msi that you copied as the source file):

- **source** - The source msi file: enter the name "mobile filter.msi".
- **destination** - The destination mst file: enter a name for this file.
- **/server:<name>** - The Mobile Filter server name (or IP address).
- **/passwd:<password>** - The client password.

You can also enter the following values if required:

- **/descr:<description>** - Enter a description of the client. This description will be seen in the Mobile Filter Administrator.
- **/port:<port>** - Enter a port number if you do not intend to use the default port 80.
- **/secure** - Use a secure connection.
- **/dump** - Show the settings on screen that will be added to the MST file.

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

```
cscript scgenmst.vbs "mobile filter.msi" customer.mst /server:mfserver /passwd:abc123
```



Note: 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 create a Group Policy, you need to download and install the Group Policy Management console from the Microsoft website at: <http://www.microsoft.com/downloads>

In order to create a Group Policy, you have to perform the following two activities:

- Create an Organizational Unit.
- Create a Group Policy Object (GPO).

To create the Organizational Unit:

- 1 Select **Administrative Tools > Active Directory Users and Computers** from the **Start** menu.



Note: If you wish to add devices to an existing organizational unit go straight to step 6. If you need to create a new one then follow steps 2-5

- 2 In the Active Directory Users and Computers window, right-click your Active Directory.
- 3 Select **New > Organizational Unit**.
- 4 Enter a name into the **New Object - Organizational Unit** dialog and click **OK**.

- 5 The new object will appear in the domain tree. Select the Computers node to see all available computers (devices) in the right-hand pane.
- 6 Drag the devices that you want to install the Mobile Filter client on into the new organizational unit that you have just created.

To create a Group Policy Object:

- 1 Right-click on the new organizational unit and select **Properties**.
- 2 Select the **Group Policy** tab, then click **Open**. This opens your organizational structure within the Group Policy Management console.



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 re-open it after you have installed the program.

- 3 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**.
- 4 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.
- 5 Right-click the new group policy object and select **Edit**.
- 6 The policy for Mobile Filter must always be applied to computers, not users. Expand **Computer Configuration** then expand **Software Settings**.
- 7 Right-click **Software Installation** and select **New > Package**.
- 8 In the Explorer dialog, enter a UNC path to the .MSI installer file that you created.
- 9 Click **Open**.



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.

- 10 In the **Deploy Software** dialog box, select the **Advanced** option, then click **OK**.
- 11 You will now see the SurfControl Mobile Filter Properties dialog. Select the **Modifications** tab, then click **Add**.
- 12 Navigate to the transform file (MST), using a UNC path then click **Open**.
- 13 Click **OK**.
- 14 The software package is listed under **Software Installations ready for deployment**. You can double-click the package to edit it at any time.



Note: To uninstall clients via Group Policy, you can use a start-up script; otherwise, you must uninstall clients individually.

UPGRADING CLIENTS

If you have already installed Mobile Filter Clients on your network, to upgrade them to the latest version of the Mobile Filter Client software, you must uninstall the clients then reinstall them from scratch.

UPGRADING YOUR MOBILE FILTER CLIENTS

On each Mobile Filter Client in your network, do the following:

- 1 Uninstall the Mobile Filter Client as described in [Uninstalling Clients on page 54](#).
- 2 When prompted, supply the password that you set during the installation of the Mobile Filter Client. This password can be found in the Client Administrator.
- 3 Download the new Mobile Filter Client software.
- 4 Install the Mobile Filter Client software as described in [Manually Installing the Mobile Filter Client on page 45](#).

(You can also use Group Policy to install groups of clients. See [Using Group Policy to Silently Install Clients on page 50](#).)

UNINSTALLING CLIENTS

Use **Add or Remove Programs** from **Control Panel** to uninstall the Mobile Filter client. You will need to supply the password that you set during the installation of the Mobile Filter client to uninstall it. This password can be found in the Client Administrator. Restart the device after uninstalling.

You can use **Password Bypass** to override the password and gain access to the Mobile Filter client uninstall process. For information on how to do this, see the Administrator Menu section of the *Mobile Filter Administrator's Guide*.

On Windows 2000, make sure you have the latest Microsoft service pack; otherwise, stop the Mobile Filter Client service before uninstalling it.

On Vista, you must log on as Administrator or disable the UAC (User Account Control) before uninstalling clients. To disable the UAC:

- 1 Select **MSCONFIG** from the Run menu.
- 2 Click the **Tools** tab.
- 3 Choose **Disable UAC** and click **Launch**.
- 4 Close MSCONFIG.
- 5 Reboot the client.

TAMPER PROTECTION

The Mobile Filter client protects against end user tampering in a number of ways.

First, end users cannot uninstall the product unless they have the password you established during installation.

If a user attempts to manually delete offline logs, the client notifies the server that a tamper has occurred.

In addition, unless you intentionally disable tamper protection, the registry entry cannot be modified; the installation files cannot be removed; and the filtering service cannot be stopped. If end users try to do these things to avoid being filtered, they receive an error message.



Appendix

Contact Technical Support	page 58
Sales and Feedback	page 60



CONTACT TECHNICAL SUPPORT

Websense provides technical information about SurfControl products online 24 hours a day, including:

- latest release information
- searchable Knowledge Base
- show-me tutorials
- product documents
- tips
- in-depth technical papers

Access support on the Web site at:

www.websense.com/SupportPortal/

If you need additional help, please fill out the online support form at:

www.websense.com/SupportPortal/Contact.aspx

Note your case number. If you need to send Support files to help us diagnose your problem, do the following:

- 1 Select **Start > SurfControl Web Filter > Support Tools > Create Web Filter Support Files**. This creates an e-mail message containing a copy of your configuration files that will help Support to discover the reason for any problems you are having. These include:
 - Event Logs (System and Application)
 - A list of file Versions
 - Registry Keys
 - System Information
 - Trace Logs
- 2 Add your case number to the subject line of the email message.
- 3 Navigate to C:\Program Files\SurfControl\Web Filter\Support. In this directory you will find the following files:
 - Application.evt
 - System.evt
 - FileVersion.txt
 - registry.txt
 - systeminfo.txt
- 4 Zip or rar these files and attach them to the email.
- 5 Press Send.



If your issue is urgent, please call one of the offices listed below.

Location	Contact information
North America	+1 858-458-2940
France	Contact your Websense Reseller. If you cannot locate your Reseller: +33 1573 232 27
Germany	Contact your Websense Reseller. If you cannot locate your Reseller: +49 6951 709 347
UK	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 2030 244 401
Rest of Europe	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 2030 244 401
Middle East	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 2030 244 401
Africa	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 2030 244 401
Australia/NZ	Contact your Websense Reseller. If you cannot locate your Reseller: 1-800-881-011, Access Code 800-542-8609
Asia	Contact your Websense Reseller. If you cannot locate your Reseller: +86 (10) 5884-4200
Latin America and Caribbean	Contact your Websense Reseller.

You will be routed to the first available technician, who will gladly assist you.

For the latest support information on SurfControl products, visit www.websense.com/SupportPortal/.



SALES AND FEEDBACK

For product and pricing information, or to place an order, contact Websense. To find your nearest Websense office, please visit our web site: www.websense.com