



Version 5.5

SurfControl Web Filter

Starter Guide



NOTICES

©1996–2008, Websense Inc.
All rights reserved.
10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published February 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.

Notices

TABLE OF CONTENTS

Notices.....	i
Introduction.....	1
Standalone Windows Edition.....	2
Pass-by filtering technology.....	2
System Requirements.....	3
Installation Decisions.....	5
Introduction.....	6
Network Considerations.....	7
Hub versus switch.....	7
Network placement.....	9
Load balancing.....	13
Multiple NIC support.....	14
NIC Teaming.....	15
Firewall Port Configuration.....	16
User Name Resolution.....	17
EUM.....	17
Methods of Installing EUM.....	18
The EUM Agent on Domain Controllers.....	18
NetWareEUM.....	20
The EUM Login Agent.....	21
Database Considerations.....	25
Database Platforms.....	25
Database Location.....	27
Database Size.....	28
Database Connectivity.....	28
Database Authentication.....	28
Deployment Scenarios.....	30
Web Filter connected to a local database.....	30
Web Filter connected to a remote database.....	34
Other Considerations.....	38
Internet Threat Database.....	38
Categorization Options.....	38
E-mail Notifications.....	39
SurfControl Report Central.....	39
Virtual Control Agent.....	39
Mobile Filter.....	39
Remote Administration Client.....	40
Privacy Edition Considerations.....	41
Installing Web Filter.....	43
Introduction.....	44
Installing SQL Server Express (optional).....	45
Installing SurfControl Web Filter.....	46
Changes to the server.....	52
Configuring Web Filter.....	53

Installing Service Pack 3	66
Further Configuration.....	71
Post Installation Tasks.....	72
All Installations.....	72
Network Dependent.....	72
User Name Resolution	73
Installing the EUM Agent on Domain Controllers	73
Installing the EUM Login Agent on your Network	77
Installing NetWareEUM	77
Install SurfControl Report Central.....	79
Network Card Configuration	80
Installing the Remote Administration Client.....	83
Appendix.....	89
Contact Technical Support	90
Sales and Feedback.....	92

Introduction

Standalone Windows Edition page 2

System Requirements page 3

STANDALONE WINDOWS EDITION

SurfControl Web Filter for Windows:

- Uses pass-by technology (no latency).
- Provides flexible deployment.
- Does not rely on existing network architecture.
- Filters all TCP based protocols.
- Is transparent to the end user.

PASS-BY FILTERING TECHNOLOGY

Protocol analyzers and network sniffers are examples of pass-by technology. Using pass-by technology, the software monitors the three-way handshake established by the source and destination hosts. If the connection triggers a set of rules (like unacceptable destination or unauthorized IP source), the filtering software inserts a packet into the network with all the required characteristics of the destination host. In other words, a packet from the filtering software appears to be from the destination host.

At the same time, the filtering software sends a packet to the destination host, mimicking the source host. At this point, the source and destination hosts believe they are in conversation with each other, when they are really communicating with the filtering software.

SYSTEM REQUIREMENTS

Before you start, ensure that your client and server machines meet the minimum requirements for installing [SurfControl Web Filter Service Pack 3](#), as listed below. Specific hardware requirements relating to the size of your network are listed in further detail in "[Deployment Scenarios](#)" on page 30.

Figure 1-1 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)	<ul style="list-style-type: none"> Windows 2000 Server Windows 2000 Advanced Server Windows Server 2003 (Standard or Enterprise Edition) 	
Network	Up to three Network Interface Cards (NICs) in promiscuous mode.	
Supported database platforms (with latest Service Packs)	<ul style="list-style-type: none"> Microsoft SQL Server Express (Requires Windows Installer 3.1 if installing on a Windows 2000 computer) Microsoft SQL Server 2000 Microsoft SQL Server 2005 <p>Note: SurfControl recommends that you install SQL Server Express or SQL Server before installing Web Filter.</p>	
Disk Space	1 GB free	5 GB free
Optional NetWare user name support	If you plan to monitor users based on NetWare user names, then you must install the Novell NetWare Client (version 5.x) over IP on the Web Filter server prior to installing Web Filter. <ul style="list-style-type: none"> Active Directory (ADS) Microsoft NT 4 Domain Controllers 	
Optional Windows user name support	If you plan to monitor users based on Windows user names, then you must be using MS NT 4 or Active Directory domain controllers.	
Web browser	Microsoft Internet Explorer 5.0	Microsoft Internet Explorer 7.0
Applications	<ul style="list-style-type: none"> Adobe Acrobat Reader 6.0 for viewing reports and documentation in pdf format. 	



Note: Web Filter is supported when installed on VMWare Server or ESX server.

You will need additional client access licenses (CALs) for the following scenarios, if you have purchased SQL Server under a Server plus Device CALs, or a Server plus User CALs license model:

- A single Web Filter remote administration client is installed.
- SRC installed on a different server to Web Filter.



Note: For each additional remote administration client, an additional CAL is required.

For more information about SQL Server CAL requirements, go to the following Microsoft pages:

<http://www.microsoft.com/sql/howtobuy/default.mspx>

http://www.microsoft.com/resources/sam/lic_cal.mspx#perprocessor

Installation Decisions

Introduction	page 6
Network Considerations	page 7
Load balancing	page 13
Multiple NIC support	page 14
Firewall Port Configuration	page 16
User Name Resolution	page 17
Database Considerations	page 25
Deployment Scenarios	page 30
Other Considerations	page 38

INTRODUCTION

There are certain decisions you must make before you start to install SurfControl Web Filter, based on the design of your network.

During the Configuration Wizard part of the installation, specific information is required which relates to your network topology, database location and how network user names should be resolved. Therefore it is important to consider how you will deploy Web Filter, to enable the most effective monitoring and filtering solution for your environment. The following sections describe the different areas that should be considered before you start.

Network Considerations ([page 7](#))

- How will you attach Web Filter to the network (hub or switch)?
- Where will you place the Web Filter server within the network?
- How many NICs does your installation require (1, 2 or 3)?

User Name Resolution ([page 17](#))

- How do you want Web Filter to handle user name resolution?
- How do you want to monitor users (IP address, workstation name, EUM, NetwareEUM)?

Database Considerations ([page 25](#))

- Which database platform do you plan to use (SQL Server Express or SQL Server)?
- How do you want Web Filter to connect to the database (Windows authentication or SQL authentication)?

Deployment Scenarios ([page 30](#))

- How many users do you need to monitor?
- What are the recommended hardware requirements for the size of your network?

Other Considerations ([page 38](#))

- Content information.
- Which e-mail notifications should Web Filter send?
- Do you need to install the Remote Administration Client?

NETWORK CONSIDERATIONS

SurfControl Web Filter is modular in design, which allows maximum flexibility in network configuration. The optimum location for the Web Filter server depends on your network's configuration. Web Filter uses a sniffer engine to monitor Internet traffic. Because of this, the location of the Web Filter server is critical, as Web Filter can only monitor and block the Internet traffic it can see. Routers, switches, and gateways are all devices which may prevent Web Filter from seeing certain parts of your network, so it is important to understand your network architecture before installing Web Filter.

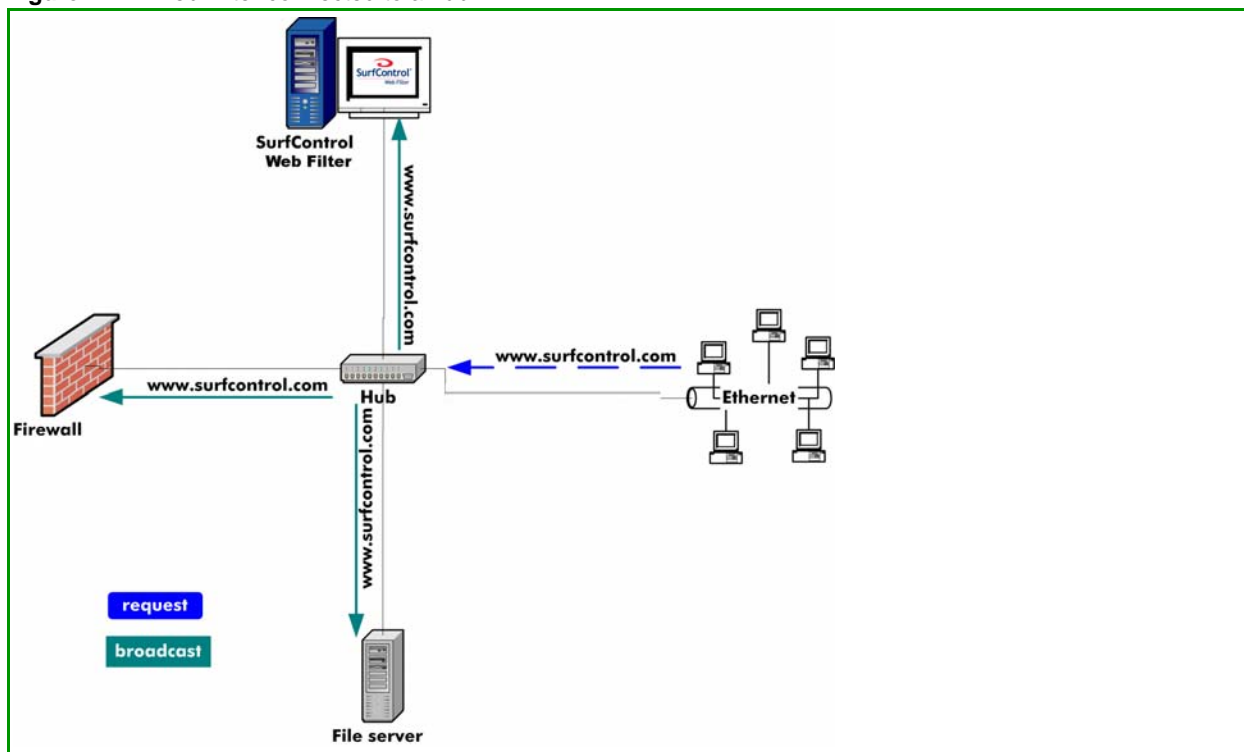
HUB VERSUS SWITCH

Since Web Filter is based on pass-by filtering technology, you must place it in a location where it can “sniff” the protocols you want to filter. You must decide which method is best for your network configuration.

Hub

Since hubs broadcast data to all ports, Web Filter is able to intercept the request and filter accordingly, as illustrated below:

Figure 2-1 Web Filter connected to a hub



Switch

In order for Web Filter to see a request through a switch, you must setup a mirrored or spanned port between the port which connects the network to the Internet gateway, and the port which the Web Filter server is connected to. This is illustrated in the following examples:

2 INSTALLATION DECISIONS

Network Considerations

Figure 2-2 Web Filter connected to a switch

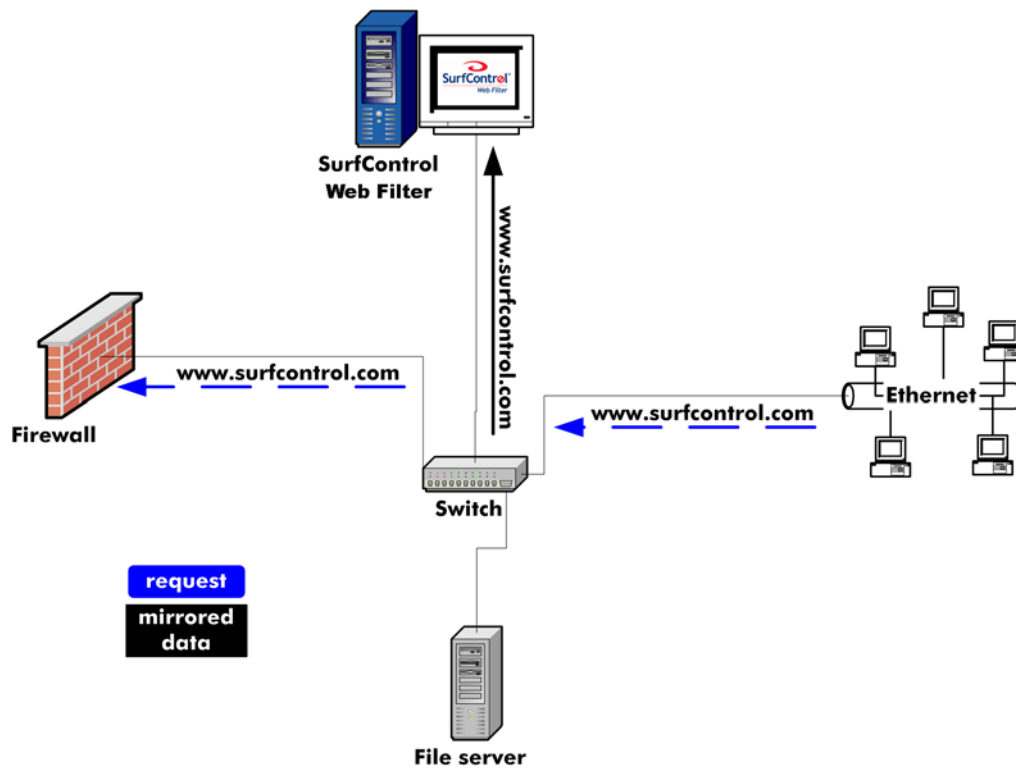
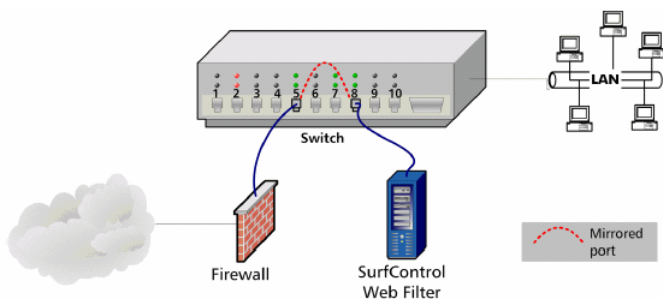


Figure 2-3 Web Filter mirrored port connection



If your switch is uni-directional and does not allow broadcasting and monitoring on the mirrored or spanned port, a second NIC is required. This is explained further in "[Multiple NIC support](#)" on page 14.

For further information on configuring spanned ports, link to the following Knowledge Base articles at

<http://kb.surfcontrol.com>:

- 1194 - About Installing SurfControl Web Filter on a switch.
- 1201 - SurfControl Web Filter is installed on the destination port and cannot block traffic.

You should also consult the documentation from the manufacturer of your switch for information on setting up spanned ports.

NETWORK PLACEMENT

SurfControl recommends installing Web Filter on a dedicated server. You should always place Web Filter in a location where it can see the traffic you want to monitor. In general, this is usually on the same switch or hub as the internal interface of your firewall.



Caution: In order to accurately monitor users, Web Filter should always be placed downstream from any proxy servers or caching devices.

Figure 2-4 Web Filter in a single-segment network

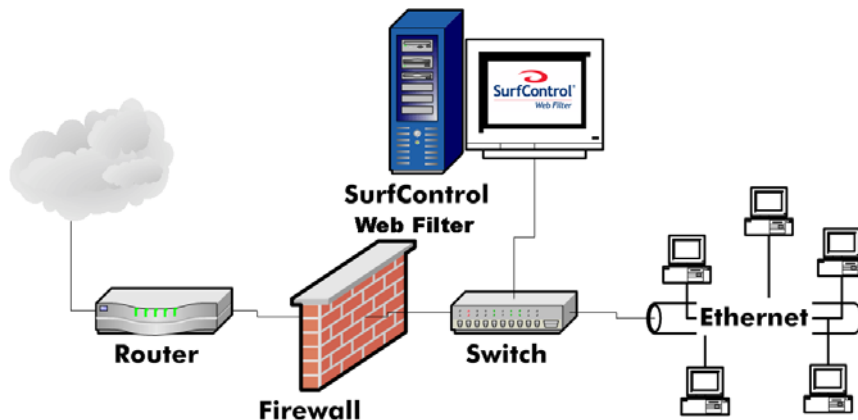
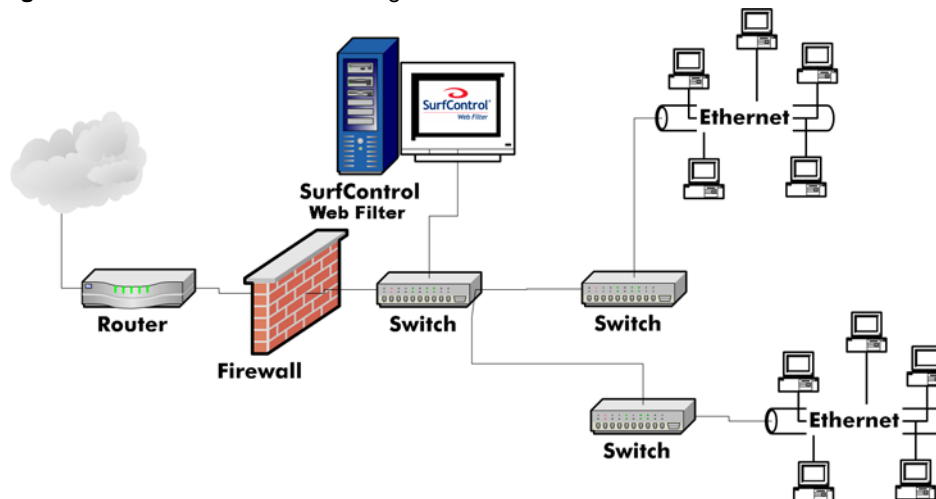


Figure 2-5 Web Filter in a multi-segment network



MULTIPLE COLLECTORS

You will need to deploy multiple Web Filter servers (called collectors) if your network:

- Has more than one Internet gateway (you need a collector at each gateway).
- Is geographically disperse (you have multiple locations around the world).

2 INSTALLATION DECISIONS

Network Considerations

- Has more than 10,000 users accessing the Internet through a single Internet gateway (each collector can filter approximately 10,000 users).

In addition, if your company has locations around the globe, you may want to deploy regional collectors and SQL Servers for three reasons:

- Cultural and legal differences may require different rule sets.
- Language barriers may bar global rule creation.
- Local administration of international servers may be required.

Larger networks may require multiple Web Filter servers to monitor and block Internet traffic. In these networks, you may choose to install two Web Filter servers at the firewall or to install separate Web Filter servers for separate segments of the network as shown in the figures below:

Figure 2-6 Multiple collectors at the firewall

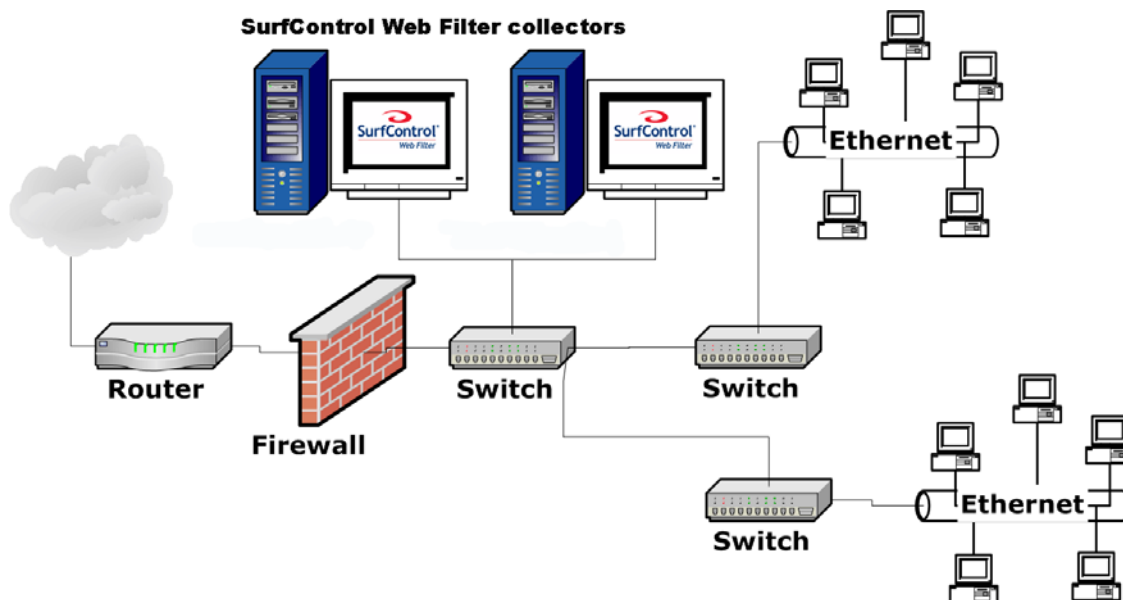
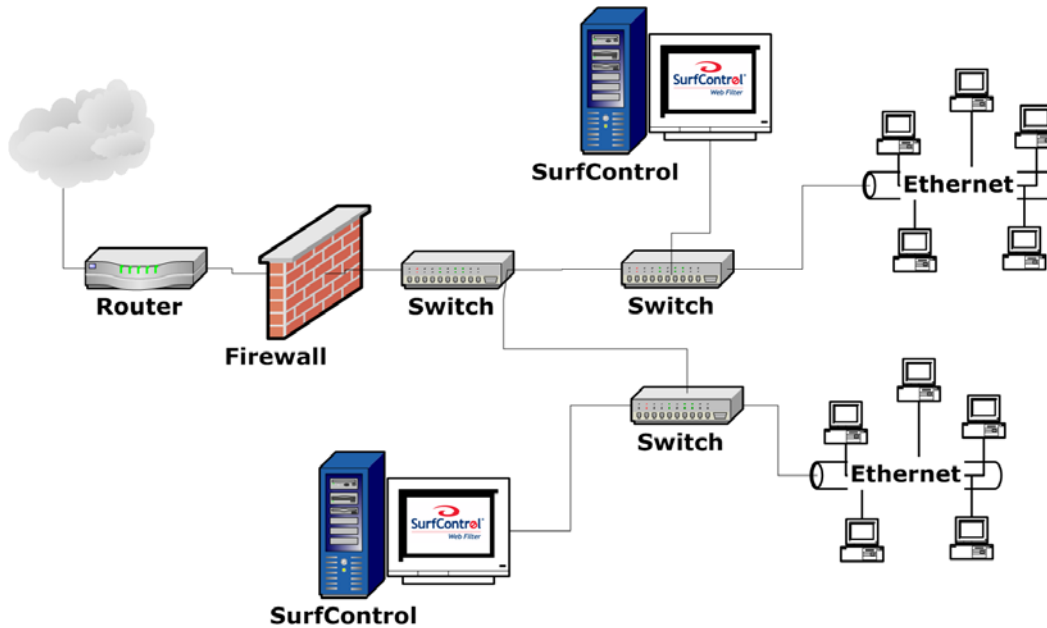


Figure 2-7 Multiple collectors for separate segments



If your network has multiple Internet gateways, you will need to deploy at least one Web Filter server at each gateway. In general, a single Web Filter server can monitor and block at least 10,000 users in an environment where you are monitoring HTTP, HTTPS, and FTP.



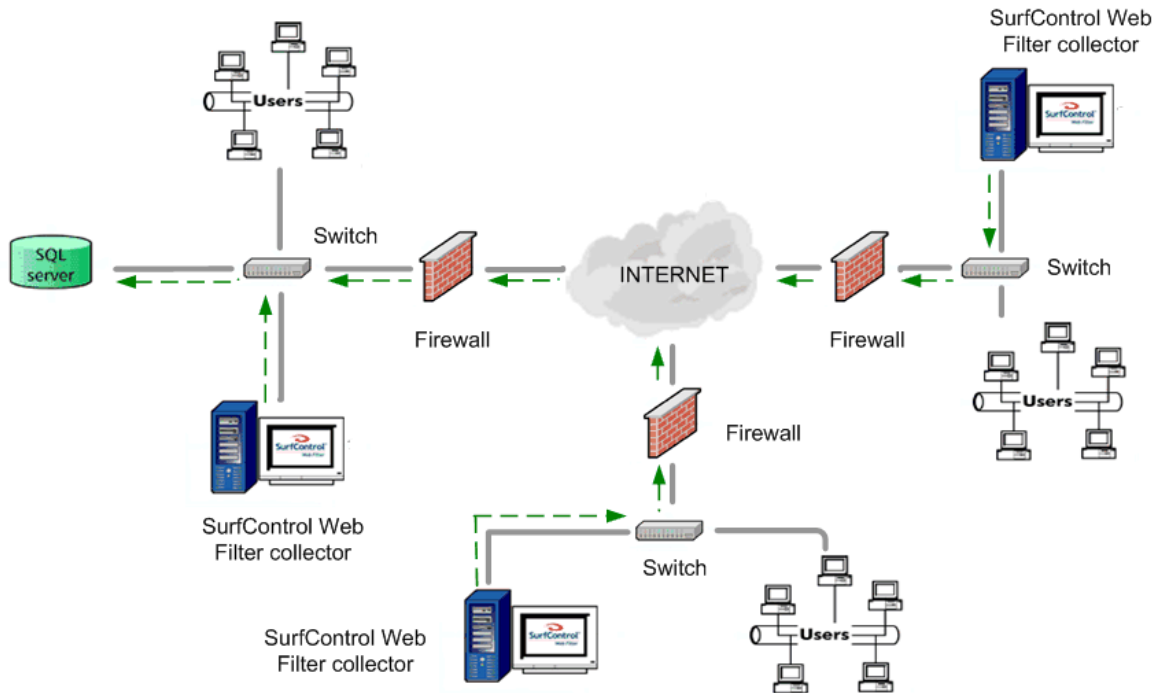
Note: The number of users that a single Web Filter server can monitor is dependent on the number of protocols you decide to monitor and the amount of traffic the users generate.

2 INSTALLATION DECISIONS

Network Considerations

The example below illustrates how Web Filter can be deployed in an enterprise network with multiple Internet gateways.

Figure 2-8 Web Filter in an enterprise environment



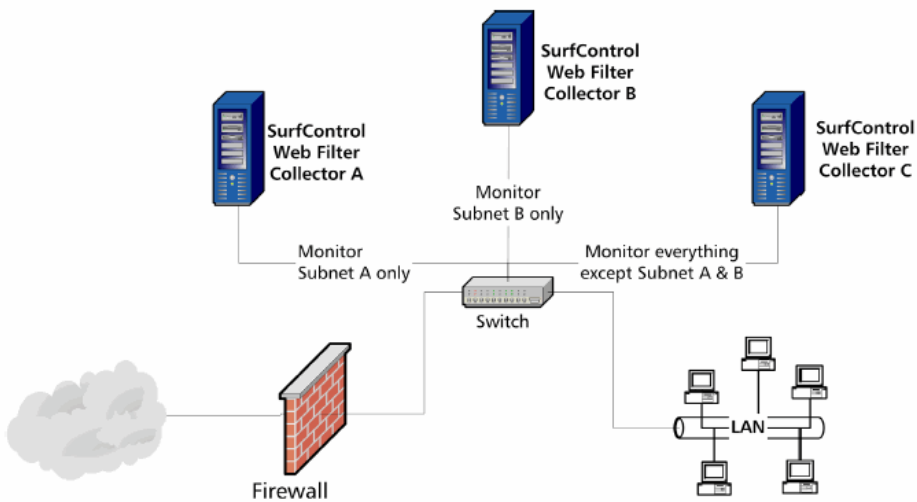
LOAD BALANCING

Web Filter works as a network sniffer by default, which means that all relevant TCP traffic is monitored, regardless of the source or destination IP address.

The Subnet feature is a simple way of partitioning traffic and sharing the load of monitoring and blocking across multiple collectors. This solution is effective, as Web Filter sees all traffic, but only processes the relevant packets. You can configure which subnets should be monitored by Web Filter during the configuration wizard part of the installation, which is explained in the ["Configuring Web Filter" on page 53](#).

The figure below illustrates how Web Filter performs load balancing by subnets.

Figure 2-9 Subnet monitoring



MULTIPLE NIC SUPPORT

SurfControl Web Filter monitors Internet traffic by analyzing the data delivered from the spanned or mirrored port. Web Filter blocks traffic by inserting packets into the stream. Switches support two methods of spanning: uni-directional and bi-directional. A switch that supports bi-directional spans allows the recipient server to receive and send data through the switch.

However, a switch that only supports uni-directional spans only allows the recipient server to receive data. Therefore, with a uni-directional span, Web Filter is unable to block Internet access. Since some switches don't support bi-directional spans, Web Filter supports multiple NICs (Network Interface Cards). In most cases, only two NICs are necessary: one to monitor, the other to block. Implementing Web Filter with multiple NICs resolves prior issues with switches that only supported one way mirroring of a port.

You can configure your Web Filter network interface cards in one of the following ways:

- **Single NIC (NIC1) configuration:**
 - NIC1 monitors, blocks, and performs all TCP/IP related activity (for example, database queries, database communication, DNS queries).
 - Configure this NIC to have an IP address.
 - During installation, bind Web Filter to this NIC.
 - This configuration requires a bi-directional span on the switch.
- **Dual NIC (NIC1 and NIC2) configuration (option 1):**
 - NIC1 monitors and blocks Internet traffic.
 - Do not configure this NIC to have an IP address.
 - During installation, bind Web Filter to this NIC.
 - NIC2 performs all other TCP/IP related activity (for example, database queries, database communication, DNS queries).
 - Configure this NIC to have an IP address.
 - This configuration requires a bi-directional span on the switch.
- **Dual NIC (NIC1 and NIC2) configuration (option 2):**
 - NIC1 monitors Internet traffic.
 - Do not configure this NIC to have an IP address.
 - During installation, bind Web Filter to this NIC.
 - NIC2 blocks Internet traffic and performs all other TCP/IP related activity (for example, database queries, database communication, DNS queries).
 - Configure this NIC to have an IP address.
 - This configuration requires a uni-directional span on the switch.
- **Triple NIC (NIC1, NIC2, and NIC3) configuration:**
 - NIC1 monitors Internet traffic.

- Do not configure this NIC to have an IP address.
- During installation, bind Web Filter to this NIC.
- NIC2 blocks Internet traffic.
- Do not configure this NIC to have an IP address.
- NIC3 performs all other TCP/IP related activity (for example, database queries, database communication, DNS queries).
- Configure this NIC to have an IP address.
- This configuration requires a uni-directional span on the switch.

NIC TEAMING

Web Filter supports NIC teaming, which is the process of grouping together two or more physical network cards into one virtual network card. This improves fault tolerance in the instance where one network card may fail, another network card in the team will continue to transmit packets without any loss of network service. By adopting this method, you can also help to balance the load of network traffic on the Web Filter server by distributing network traffic through each network card in the team.

If you have a uni-directional switch, and therefore have to configure each network card to perform separate tasks of monitoring or blocking, you can only team the monitoring network cards together or the blocking cards together.

For further instruction on how to setup NIC teaming on your Web Filter server, consult the documentation from the manufacturer of your network cards.

FIREWALL PORT CONFIGURATION

If you are using Microsoft ISA Server as a firewall, you will need to edit your system policy to allow Web Filter to communicate across certain network ports. Opening up these ports at the firewall will enable you to use all of the available Web Filter services. Refer to the *ISA Starter Guide* for instructions on setting up ISA policy rules for Web Filter services. The table below describes which ports need to be configured at the firewall for each Web Filter service you want to use:

Table 2-1 Web Filter communication ports

Web Filter Service	Port
Corporate Network Detection Service	51118
SMTP E-mail Notifications	25
EUM Login Agent	61695
EUM Login Agent for Netware	61696
Group enumeration in Active Directory (LDAPS)	636
Group enumeration in Active Directory and Netware (LDAP)	389
Live Updates	Allow outbound access to *.surfcontrol.com
Real-Time Monitor	5000
Remote Administration Client (UDP)	1024 - 65535
SurfControl Report Central	Allow inbound access to 8888 and/or 8443
SQL Server (Remote installations only)	Allow inbound and outbound access to 1433 -1434
User Name Resolution (NetBIOS)	139
Workstation name resolution	53
Workstation name resolution (WINS)	42

USER NAME RESOLUTION

By default, SurfControl Web Filter does not monitor user names. The **Configuration Wizard** enables you to monitor your users by name, in the following ways:

- By issuing a NetBIOS query based on the MAC address.
- By installing the supplied **Enterprise User Monitoring (EUM)** utility, which you can install either on your domain controllers, Novell NDS tree servers or via a logon program stored on your network.



Note: Web Filter supports three monitoring methods: user name, workstation name or IP address.

SurfControl recommends monitoring by user because:

- Monitoring by workstation name only identifies the machine requesting the data, not the user who originated the request.
- Monitoring by user name is more convenient in a workplace where employees share or swap machines frequently.
- Monitoring by user name enables you to filter users based on NT Users and Groups.
- Monitoring by user name makes it easier to track users that frequently log on to multiple machines.

Web Filter displays user names with the following precedence:

- 1 User name resolved with **NetWareEUM**.
- 2 User name resolved with **EUM**.
- 3 User name based on **NetBIOS** query.
- 4 Workstation ID.
- 5 IP address.

EUM

EUM accesses Windows NT, Windows 2000 and 2003 security auditing data to resolve user names. This provides Web Filter with the ability to monitor traffic on a routed network by user name. EUM provides Web Filter with continuous, accurate reporting of logon activity by user name.



Note: SurfControl recommends using EUM for user name resolution.

For example, when jsmith attempts to access <http://www.cnn.com>, Web Filter sees jsmith's IP address in the HTTP request. EUM provides the missing link by receiving data from the domain controllers regarding jsmith's identity.

METHODS OF INSTALLING EUM

You can install EUM in one of two ways:

- 1 Install an EUM Agent on your domain controllers or Novell NetWare NDS Tree Server.
- 2 Install an EUM Login Agent on your network that can monitor all users via a login script. ([page 21](#))

Installing the EUM Agent on your Domain controllers works well in a LAN environment where all users log on to the Windows domain. If you do not have access to, or do not wish to install the EUM Agent on your domain controller, you can use the EUM Login Agent.

THE EUM AGENT ON DOMAIN CONTROLLERS

You can install the EUM Agent on domain controllers which have the following operating systems:

- Windows NT
- Windows 2000
- Windows 2003 (Standard and Enterprise)
- Windows 2003 x64 (Standard and Enterprise)

There is also a version of the EUM Agent that works with Novell NetWare. This is explained further in "[NetWareEUM](#)" on [page 20](#).

During the installation, the configuration file **scua.ini** is installed into the **c:\Surfcontrol User Agent** folder on each domain controller. This file contains connection information about your Web Filter server(s) and identifies ignored users, which are specified during the installation. Additional domain controllers and/or ignored users can also be added to your EUM Agent configuration at a later date. For further details about installing the EUM Agent and post configuration tasks, refer to the following sections:

- "[Installing the EUM Agent on Domain Controllers](#)" on [page 73](#)
- "[Making changes to the EUM Agent configuration](#)" on [page 75](#)

EUM on Windows 2000 and 2003 Domain Controllers

Web Filter uses Microsoft's Sub-Authentication to resolve user names on a Windows 2000 or 2003 server. The EUM agent is installed on to Windows 2000 and 2003 domain controllers as a file called **ScSubAuth.dll**. If you are installing EUM on to a Windows 2003 x64 operating system, the file **ScSubAuth_AMD64.dll** is loaded on to the domain controller.

EUM on Windows NT Domain Controllers

Web Filter installs the EUM User Agent (UA) on Windows NT domain controllers as a service (SurfControl User Agent service; ScUserAgent.exe). During EUM installation, Web Filter configures NT domain controllers to record Successful Logons to the security log (event 528). If you make changes to this audit policy and disable event 528 logs (Successful Logon), EUM will not work correctly.

Confirm that event 528 logs are enabled by performing the following:

- 1 From the Web Filter server, select **User Manager for Domains** from the **Programs > Administrative Tools** menu.
- 2 From the menu, select **Policies Audit**. Confirm that **Audit these Events** is checked.
- 3 Ensure security logs are set to overwrite as needed. Do not manually clear the security logs.

Before Installation

Prior to installing the EUM UA on to an NT domain controller, ensure the trust relationships are set up for multiple domain environments.



Note: The trust relationship should be configured so that Web Filter is Trusted, and all other domains are Trusting.

During installation, Web Filter installs the EUM UA on to each domain controller. Before installing EUM, ensure the following:

- The Web Filter server must have a static IP address.
- The installer must be logged into the Web Filter server as a user with domain administration rights.
- For a successful automatic installation, Web Filter must be able to see the domains that require EUM. Make sure Web Filter is located in the appropriate domain.
 - In a two-way trusted environment, the Web Filter server can be located in any domain.
 - If a one-way model is in use, the Web Filter server should be located in the master domain (this enables Web Filter to see all other domains).
- For Windows NT domain controllers, make sure the security logs of all domain controllers are set to overwrite events as needed.
- By default, EUM uses port 61695 to communicate with the Web Filter server. Perform the following steps to change the port:
 - i Add the following key to the SurfControl registry:
`HKEY_LOCAL_MACHINE\SOFTWARE\JSB\SurfControlScout\UserAgentPort`
 - ii Add the key as a DWORD and specify a decimal value. The default is 61695.
 - iii Stop and start the Web Filter service.
 - iv Update the scua.ini file on the domain controllers to reflect the port changes.
- SurfControl recommends installing EUM when there are few or no users on the network or when a forced logoff can be scheduled.

- During installation, you'll be prompted to identify specific user accounts that UA should ignore. You should only use this option for accounts similar to SMS or service accounts (for example, backup.exe, anti-virus updates, servers).



Caution: Ignoring valid user accounts will result in mis-identification.

NETWAREEUM

Web Filter also enables you to monitor users by their Novell NetWare user name. The Novell version of EUM is called NetWareEUM. NetWareEUM works in the same way as EUM. Web Filter installs a User Agent on to each Novell NDS tree server.



Caution: Web Filter does not support Novell 4.x. If you need to resolve Novell 4.x users, authenticate all users on an NT or 2000 domain controller and use EUM to resolve the user names.

Before installing NetWareEUM, ensure the following:

- 1 Install NetWare's Client 32 (as Preferred TCP/IP Protocol) on to the server. SurfControl recommends doing this before installing Web Filter.
- 2 Network must be using Novell 5 or 6 over IP.
- 3 The Web Filter server must have a static IP address.
- 4 You need to manually edit the `scua.ini` file to add the host name or IP address and port number of any Web Filter servers. See ["Add Web Filter Servers to NetWare EUM" on page 78](#) for more details.
- 5 By default, NetWareEUM uses port 61696 to communicate with the Web Filter server. Perform the following steps to change the port:
 - i Add the following key to the registry:
`HKEY_LOCAL_MACHINE\SOFTWARE\JSB\SurfControlScout\NWUserAgentPort`
 - ii Add the key as a DWORD, specify a decimal value (default is 61696).
 - iii Stop and start the Web Filter service.

SurfControl recommends installing NetWareEUM when there are few or no users on the network or when a forced logoff can be scheduled.

Ignoring Users in NetWare EUM

Users such as administrative groups, other NetWare servers or users using ZENworks need to be ignored by the NetWare server where Web Filter is installed. This requires the `scua.ini` file to be edited.

Ignoring other NetWare servers can prevent caching problems, especially when setting the Logging level to 2. See ["Logging Levels" on page 21](#) for more details.

Logging Levels

A log file `surflog.txt` will be created and stored in the same directory as the `scua.ini` and `nweum.nlm` files. In a default installation this is located in: `C:\Program Files\SurfControl\Web Filter\NetWare`.

In the `scua.ini` file you can set the logging level for events to be stored in this file. The default logging level is 1. The levels are shown in the table below :

Table 2-2 Logging Levels

Value	Logging detail
0	No logging.
1	Important events - Startup, Shutdown, Errors, connection with Web Filter installations, connection failures, disconnections.
2	Login events such as Ignored Users.
3	Combination of levels 1 and 2.

THE EUM LOGIN AGENT

The Login Agent enables you to use the EUM without having to install anything on your domain controllers. It works by saving a supplied program (`ScEumLoginAgent.exe`) and a configuration file (`EumLogin.ini`) to a location on your network that is accessible to all users. You must then perform the following steps to enable the login agent to work.

Installing the Login Agent on NT Domains

- 1 Manually configure the `EumLogin.ini` file.
- 2 Create a new log on script, or modify an existing one to call the `ScEumLoginAgent.exe`.
- 3 Use the `/INTLOGOFF` parameter to allow log on and log offs to be handled by the same script. See ["Configuring a Logon and Logoff Script" on page 24](#) for more details.

Installing the Login Agent on Windows 2000 and 2003

- 1 Manually configure the `EumLogin.ini` file.
- 2 Create a new log on script, or modify an existing one, to call the `ScEumLoginAgent.exe`. See ["Configuring a Logon and Logoff Script" on page 24](#) for more details.
- 3 Add traffic from the `ScEumLoginAgent` program as an exception to the Windows Firewall (Windows Server 2003 and above) that allows the `ScEumLoginAgent` program to operate. See ["Add an Exception to the Windows Firewall" on page 24](#) for more details.

Login Agent Location

The Login Agent program and configuration file can be found in the following location in a default install:

`C:\Program Files\SurfControl\Web Filter\EnterpriseUserMonitoring\LoginAgent`

The EumLogin.ini file

Below is a copy of the supplied .ini file

```
[Surfcontrol_Servers]

# The [Surfcontrol_Servers] section of the EumLogin.ini file is used to set the
# server names to be used for each instance of SurfControl Web Filter.

#Servers=SERVERNAME,127.0.0.1

[SERVERNAME]

# Section name section, which specifies the SurfControl Web Filter server and its
# listening port number. The ServerName can be an IP Address or Computer Name
# value e.g.

# Port=61695

# NetwarePort=61696

#[127.0.0.1]

#Port=61695

#NetwarePort=61696

[Continuous_Mode]

# This is the interval by which the Login EXE will send login details to SWF servers
# when in continuous mode. Value is in seconds e.g.

# Interval=900

Interval=900

[Retry_Connection]

# Number of times we will attempt to connect to SWF service e.g.

# Retry=5

Retry=5
```

How to Configure the File

The table below describes the various sections of the EumLogin.ini file and how to enter your information.

Table 2-3 The EumLogin.ini file sections

Section	What to enter
[Surfcontrol_Servers]	<p>Enter the name, or IP address, of each server in your organization that Web Filter is installed on. The format is:</p> <p>Servers=Servername1,Servername2,127.0.0.1</p> <p>Note: Do not leave spaces between the server names.</p>
[SERVERNAME]	<p>For each server specified in [Surfcontrol_Servers], make an entry along with the default Web Filter listening port (61695) for Windows or the default port (61696) for Netware.</p> <p>For example, the format for a Windows 2000 or 2003 domain is:</p> <p>[Servername1] Port=61695</p> <p>[Servername2] Port=61695</p> <p>[127.0.0.1] Port=61695</p> <p>The format for a Netware domain is:</p> <p>[Servername1] NetwarePort=61696</p> <p>[Servername2] NetwarePort=61696</p> <p>[127.0.0.1] NetwarePort=61696</p>
[Continuous_Mode]	<p>The Login Agent runs in continuous mode. The agent will send log on and log off details to the servers specified in [Surfcontrol_Servers] at a specified interval (in seconds). The default setting is 900 seconds.</p> <p>The format is:</p> <p>Interval=900</p>
[Retry_Connection]	<p>If a connection to any of the servers specified in the [Surfcontrol_Servers] section is dropped, the Login Agent will try to reconnect. This entry specifies how many times the agent will attempt to reconnect.</p> <p>If the connection is not re-established after the number of times specified, the agent will wait for the interval specified in the [Continuous_Mode] section before attempting to connect again. The maximum value is 5. If you enter a value higher than 5 the Login Agent will only try 5 times.</p> <p>The format is:</p> <p>Retry=5</p>

Configuring a Logon and Logoff Script

You need to create a new logon and logoff script, or modify an existing one, to call the EUM Login agent (`ScEumLoginAgent.exe`). The EUM Login Agent file should be placed in an area on the network which is accessible to all users.



Note: A logoff script is not required for NT domains.

The following command line parameters can be used in the logon script:

- `/INTLOGOFF` - This enables log on and log off activity to be handled by a single agent. This parameter must only be used in environments such as an NT domain, where separate scripts are not supported.
- `/NETWARE` - This command line parameter is used in a Netware environment. Use this in the logon script to return the Netware user name to the EUM Login Agent. This will ensure that the default Netware port (61696) is loaded from the `EumLogin.ini` file. If this parameter is not specified, the Windows username will be returned by default to the EUM Logon Agent.
- `/NOCONT` - Use this to run the agent in non-continuous mode. The agent will send the user name details once to the server(s) and then terminate. If this parameter is not used, the agent will run in continuous mode. This parameter should not be used in an NT domain.
- `/TRACEMODE` - Use this command line parameter if you are experiencing problems with the agent. Trace messages will be stored in a log file called `EumLoginTrace.log`. This file will be stored in the logged on user's temporary folder. The location of this folder is determined by the following:
 - The path specified by the `TMP` environment variable.
 - The path specified by the `TEMP` environment variable.
 - The path specified by the `%USERPROFILE%` environment variable.
 - The Windows directory.

The following command line parameter is used in the logoff script:

- `/LOGOUT` - To be used if the agent is called by a logoff script. If this parameter is not used, the agent will assume it is a logon script.

Add an Exception to the Windows Firewall

The Windows Firewall will prevent the `ScEumLoginAgent` application from sending traffic to the network. To allow the EUM Login Agent to function requires an Active Directory group policy to be created or updated to add the traffic from the application as an exception to the firewall. For more details on these options consult our Knowledge Base article 1775.

The Knowledge Base can be found at: <http://kb.surfcontrol.com>

DATABASE CONSIDERATIONS

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

- Which database platform you plan to use (SQL Server Express or SQL Server).
- If the network location of the database will be local or remote to the Web Filter server.
- How Web Filter will connect to the database (Windows or SQL authentication).

The following sections describe these considerations in more detail.

DATABASE PLATFORMS

Web Filter uses SQL Server Express, or a fully-licensed version of SQL Server 2000 or 2005. You should ensure your choice of database platform is installed and running, before attempting to install Web Filter. SurfControl recommends that you use SQL Server rather than SQL Server Express for the following reasons:

- SQL Server allows greater scalability.
- SQL Server enables you to fine-tune database performance.
- SQL Server is more suitable for environments with heavy Web traffic.
- SQL Server does not have a specified database size limitation, whereas SQL Server Express has a maximum database size of 4GB.

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 Web 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.
- 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.
- You must perform the steps outlined below after installing SQL Server Express, and before installing Web Filter.

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:

- 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 get 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 already installed on your network, you should plan to create the database on that server (you can create and configure the database during the installation process). 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:

- 1 Install SQL Server on the designated server; this can be the same machine as the Web Filter server.
- 2 If you are installing SQL Server on your Web Filter server, make sure your server has the minimum specifications listed in the table below.

Table 2-4 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.

- 3 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.



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.

Reasons to Install SQL Server on a Dedicated Server

Use SQL Server 2000 or 2005 on a dedicated remote 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 2-5 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 LOCATION

If your network requires multiple Web Filter servers, you have the option to install the database in a location which is local or remote to the Web Filter server.

- **Local database** - Stores data for a single Web Filter server in a single database on the Web Filter server.
- **Remote database** - Stores the data from one or more Web Filter collectors in a single database on a separate server. If you choose to use the remote database option, you can manage your policy from one location, plus you have the ability to run reports from a single repository. This means that policy

changes made on one collector are replicated to the other collectors, removing the need for separate policy creation at each collector.

However, the size of a remote database grows in direct relation to the number of Web Filter servers that write to it. Depending on the size of your environment and the amount of Internet traffic, a remote database can require more frequent database administration. SurfControl recommends using Windows Authentication for performance and security reasons. Therefore, remote databases require specific security settings for communication between the Web Filter server and the database.

DATABASE SIZE

The size of your Web Filter database depends on:

- The amount of traffic your employees generate.
- The amount of traffic Web Filter is monitoring.
- The number of protocols Web Filter is monitoring.
- The number of users Web Filter is monitoring.

Make sure the SQL Server has as much RAM as the anticipated size of the database. Microsoft's policy for optimal performance recommends a 1:1 ratio between database size and RAM. For example, a 1GB database requires 1GB RAM.



Note: SurfControl estimates that 5000 users generate approximately 1 GB of data per month.

DATABASE CONNECTIVITY

Web 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 Data Source Names (DSN), therefore, any Web Filter client or server on the network can access the database without creating a link through the ODBC driver.

DATABASE AUTHENTICATION

Web Filter supports both Windows authentication and SQL authentication. SurfControl recommends Windows authentication because it is easier to use and compliant with Microsoft's security recommendations. If you choose SQL authentication, any configured connections must be re-established if the username or password of the SQL user account (e.g. SA) changes. With Windows authentication, you can change the username and password without having to reconfigure the database connection.

Windows Authentication

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

SQL Authentication

If you choose to use SQL authentication, you will need to create a SQL Server login specifically for Web Filter. This login is required for creating the database and should be used for all Web Filter database activities. If you choose to connect to the SQL database using SQL authentication, make sure the SQL Server database is configured to support SQL Server and Windows NT authentication.

DEPLOYMENT SCENARIOS

There are three common scenarios for deploying Web Filter on your network, which are dependent on your database architecture. The typical scenarios are:

- A single Web Filter server with a local database.
- A single Web Filter server connecting to a remote database.
- Multiple Web Filter servers (collectors) connecting to one remote centralized database.

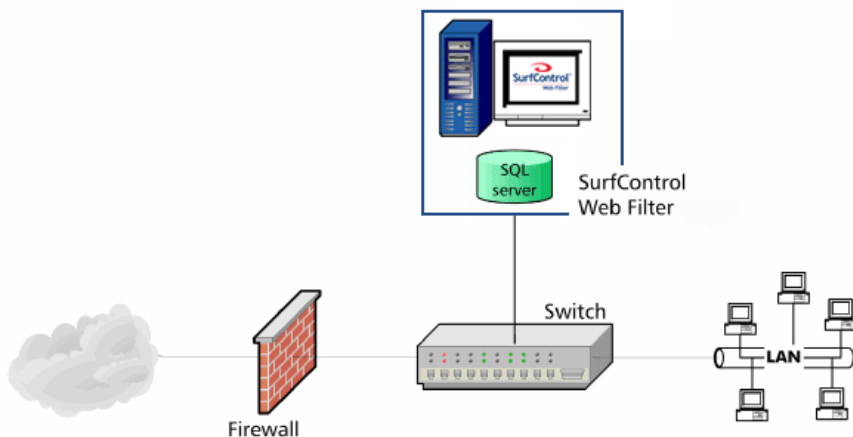


Note: The following sections are basic guidelines. Actual recommended deployment also depends on Internet usage patterns, which can vary significantly from company to company.

WEB FILTER CONNECTED TO A LOCAL DATABASE

The server recommendations in this section are based on the number of users and server resources for Web Filter connected to a local SQL Server installation.

Figure 2-10 Web Filter with SQL Server installed locally



Web Filter components

The table below recommends how to deploy each Web Filter additional component if the database is local.

Table 2-6 Web Filter component recommendations

Web Filter Component	Recommendation
Mobile Filter	Install on a separate server, and place in the DMZ
SurfControl Report Central (SRC)	Install on the Web Filter server
Virtual Control Agent (VCA)	Install on the Web Filter server

<500 users

The tables below show the Web Filter component and server recommendations for an environment with less than 500 users. For this size of environment, SurfControl recommends using SQL Server Express on the Web Filter server.

Table 2-7 Web Filter Server recommendations: Local database (<500 users)

Server component	Recommendation
Processor	Pentium IV, 2.0 GHz
RAM	2GB
Network Interface Cards (NICs)	2 NICs (one for monitoring, one for blocking)
Hard drive	10 GB free
Operating System (with latest service packs)	Microsoft Windows 2000 Server Microsoft Windows 2003 Server
Database	SQL Server Express, installed on the Web Filter server

500-2500 users

The table below shows SurfControl's server recommendations for an environment with 500-2500 users. In this size of environment, SurfControl recommends the following:

- Use a fully licensed version of SQL Server.
- Configure SQL Server to use a maximum of 1.5 GB of RAM.

Table 2-8 Web Filter Server recommendations: Local database (500 - 2500 users)

Server component	Recommendation
Processor	Pentium IV, 2.2 GHz
RAM	2 GB or more
Network Interface Cards (NICs)	2 NICs (one for monitoring, one for blocking)
Hard drive	HDD (10,000+ RPM), 20 GB free
Operating System (with latest service packs)	<ul style="list-style-type: none"> • Microsoft Windows 2000 Server • Microsoft Windows 2000 Advanced Server • Microsoft Windows Server 2003
Database	Microsoft SQL Server 2000 or 2005, installed on the Web Filter server

2500-5000 users

The table below shows SurfControl's server recommendations for an environment with 2500-5000 users. In this environment, SurfControl recommends the following:

- Use a fully licensed version of SQL.
- Configure SQL to use CPU1, CPU2, and CPU3 (by default, Web Filter will use the primary CPU - CPU0).
- Configure SQL to use a maximum of 1.5 GB of RAM.

Table 2-9 Web Filter Server recommendations: Local database (2500 - 5000 users)

Server component	Recommendation
Processor	Dual Xeon, 2.0 GHz
RAM	4 GB or more
Network Interface Cards (NICs)	2 NICs (one for monitoring, one for blocking)
Hard drive	HDD (10,000+ RPM), 40 GB free

Server component	Recommendation
Operating System (with latest service packs)	<ul style="list-style-type: none"> Microsoft Windows 2000 Server Microsoft Windows 2000 Advanced Server Microsoft Windows Server 2003
Database	Microsoft SQL Server 2000 or 2005, installed on the Web Filter server

5000-10,000 users

The table below shows SurfControl's server recommendations for an environment with 5000 -10,000 users. SurfControl recommends the following for this size of environment:

- Use a fully licensed version of SQL.
- Configure SQL to use CPU1, CPU2, and CPU3 (by default, Web Filter will use the primary CPU - CPU0).
- Configure SQL to use a maximum of 3.5 GB of RAM.

Table 2-10 Web Filter Server recommendations: Local database (5000 - 10,000 users)

Server component	Recommendation
Processor	Dual Xeon, 2.8 GHz
RAM	4 GB or more
Network Interface Cards (NICs)	2 NICs (one for monitoring, one for blocking)
Hard drive	HDD (10,000+ RPM), 80 GB free
Operating System (with latest service packs)	<ul style="list-style-type: none"> Microsoft Windows 2000 Server Microsoft Windows 2000 Advanced Server Microsoft Windows Server 2003
Database	Microsoft SQL Server 2000 or 2005 Enterprise Edition, installed on the Web Filter server

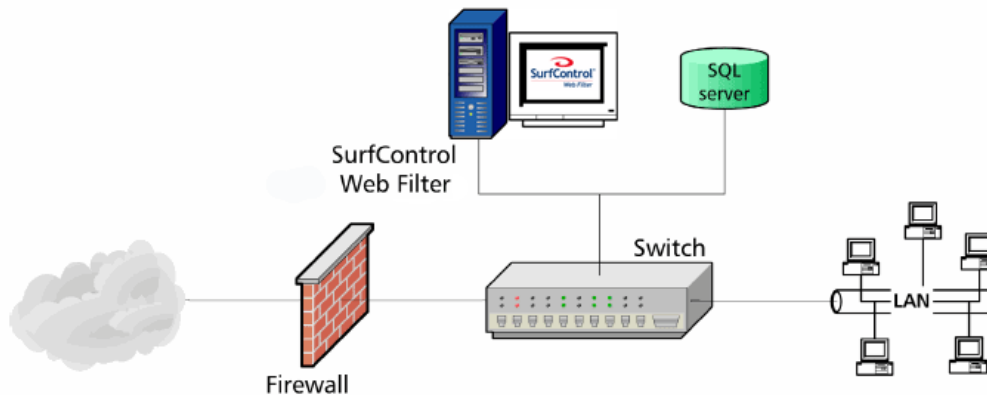
WEB FILTER CONNECTED TO A REMOTE DATABASE

The server specifications in this section relate to the following two scenarios:

- A single Web Filter server connecting to a remote database.
- Multiple Web Filter servers (collectors) connecting to one remote centralized database.

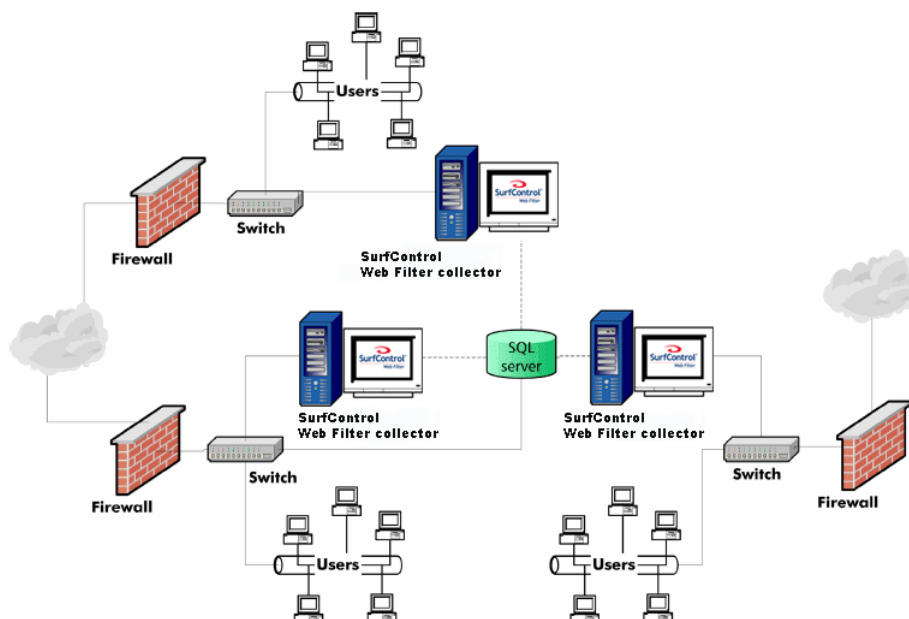
If you have installed Web Filter with a remote SQL Server installation, the following recommendations are based on the number of users and server resources. Specifications are given for both the Web Filter server and the remote SQL Server and apply to both scenarios. The figure below shows Web Filter connecting to a remote database.

Figure 2-11 Single Web Filter server with SQL Server installed remotely



The following figure shows Web Filter in a multi-collector environment with one remote database

Figure 2-12 Multiple Web Filter collectors connected to one centralized remote database



Web Filter components

The table below recommends how to deploy each Web Filter additional component if the database is remote to the Web Filter server.

Table 2-11 Web Filter component installation recommendations

Web Filter Component	Recommendation
Mobile Filter	Install on a separate server, and place in the DMZ
SurfControl Report Central (SRC)	Install on the Web Filter server
Virtual Control Agent (VCA)	Install on the Web Filter server

500-2500 users

The tables below show SurfControl's Web Filter server recommendations for an environment with 500-2500 users, and the remote SQL Server recommendations.

Table 2-12 Web Filter server recommendations: Remote database (500-2500 users)

Server component	Recommendation
Processor	Pentium IV, 2.0 GHz
RAM	1 GB
Network Interface Cards (NICs)	2 NICs (one for monitoring, one for blocking)
Hard drive	HDD (10,000+ RPM), 10 GB free
Operating System (with latest service packs)	<ul style="list-style-type: none"> Microsoft Windows 2000 Server Microsoft Windows 2000 Advanced Server Microsoft Windows Server 2003

Table 2-13 SQL Server Recommendations (500-2500 users)

Server component	Recommendation
Processor	Pentium IV, 2.2 GHz
RAM	2 GB or more
Network Interface Cards (NICs)	1 NIC
Hard drive	HDD (10,000+ RPM), 20 GB free

Server component	Recommendation
Operating System (with latest service packs)	<ul style="list-style-type: none"> Microsoft Windows 2000 Server Microsoft Windows 2000 Advanced Server Microsoft Windows Server 2003
Database	Microsoft SQL Server 2000 or 2005

2500-5000 users

The tables below show the Web Filter server recommendations for an environment with 2500-5000 users, and for the remote SQL Server.

Table 2-14 Web Filter server recommendations: Remote database (2500-5000 users)

Server component	Recommendation
Processor	Xeon, 2.0 GHz
RAM	1 GB
Network Interface Cards (NICs)	2 NICs (one for monitoring, one for blocking)
Hard drive	HDD (10,000+ RPM), 20 GB free
Operating System (with latest service packs)	<ul style="list-style-type: none"> Microsoft Windows 2000 Server Microsoft Windows 2000 Advanced Server Microsoft Windows Server 2003

Table 2-15 SQL Server Recommendations (2500-5000 users)

Server component	Recommendation
Processor	Dual Xeon, 2.0 GHz
RAM	2 GB or more
Network Interface Cards (NICs)	1 NIC
Hard drive	HDD (10,000+ RPM), 40 GB free
Operating System (with latest service packs)	<ul style="list-style-type: none"> Microsoft Windows 2000 Advanced Server Microsoft Windows Server 2003 Enterprise Edition
Database	Microsoft SQL Server 2000 or 2005

5000-10,000 users

The tables below show the Web Filter server recommendations for an environment with 5000-10,000 users, and for the remote SQL Server.

Table 2-16 Web Filter Server Recommendations: Remote database (5000-10,000 users)

Server component	Recommendation
Processor	Xeon, 2.8 GHz
RAM	1 GB
Network Interface Cards (NICs)	2 NICs (one for monitoring, one for blocking)
Hard drive	HDD (10,000+ RPM), 20 GB free
Operating System (with latest service packs)	<ul style="list-style-type: none"> Microsoft Windows 2000 Advanced Server Microsoft Windows Server 2003 Enterprise Edition

Table 2-17 SQL Server Recommendations (5000-10,000 users)

Server component	Recommendation
Processor	Dual Xeon, 2.8 GHz
RAM	4 GB or more
Network Interface Cards (NICs)	1 NIC
Hard drive	HDD (10,000+ RPM), 80 GB free
Operating System (with latest service packs)	<ul style="list-style-type: none"> Microsoft Windows 2000 Advanced Server Microsoft Windows Server 2003 Enterprise Edition
Database	Microsoft SQL Server 2000 or 2005 Enterprise Edition

OTHER CONSIDERATIONS

This section contains general information that you should be aware of when installing and configuring SurfControl Web Filter.

INTERNET THREAT DATABASE

SurfControl's Internet Threat Database is the premier category database in the filtering industry and provides the most accurate, current, and relevant content listing available. The Internet Threat Database includes:

- 55 well organized categories.
- Over 24 million destinations, including more than 3.5 billion web pages.
- International content, including 70 languages and over 200 countries.
- Daily updates (more than 100,000 new destinations a week).
 - The Internet Threat Database is stored in an encrypted, size optimized file called `SurfControl Categories.csf`.
 - Incremental updates (up to 60 MB) are stored in an encrypted file called `SurfControl Categories.cdb`.
 - With Web Filter, you can manually categorize destinations; these are added to the `SurfControl Manual Categories.ucf` file.
 - VCA categorized destinations are added to the `SurfControl VCA Categories.ucf` file.

Web Filter checks the categorization files in the following order:

- 1 Manually categorized sites (`SurfControl Manual Categories.ucf`)
- 2 Incremental updates (`SurfControl Categories.cdb`)
- 3 Internet Threat Database (`SurfControl Categories.csf`)
- 4 VCA categorized sites (`SurfControl VCA Categories.ucf`)

CATEGORIZATION OPTIONS

You can select whether to send feedback on uncategorized sites back to SurfControl, and how Web Filter categorizes your own domains.

Internet Threat Database Improvement Program

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

Company & Intranet

You can enter your company domains and Intranet site addresses during the Configuration Wizard so that Web Filter categorizes them as **Company & Intranet**.

You can change the **Internet Threat Database Improvement Program** and **Company & Intranet** settings From the **Web Filter Settings** in the Enterprise Manager. See the *Administrator's Guide* for more details.

E-MAIL NOTIFICATIONS

Web Filter includes the ability to automatically notify the system administrator when any of the following events occur:

- **Service running status changes** - If the status of any of the Web Filter services changes (for example, from Running to Stopped).
- **Internet Threat Database license reminders** - If the Internet Threat Database license is close to expiring.
- **Scheduled task failures** - If any scheduled tasks fail to run.
- **Catch up mode notifications** - If Web Filter enters network overload due to the volume of Internet traffic received.
- **Unlicensed product reminders** - If you haven't licensed the product. This is a default reminder and will be sent if you choose to enable the feature (by identifying a mail server and recipient).

If you decide to enable e-mail notifications, you will need to know the hostname or IP address of your mail server and will need to identify an administrator that will receive the notifications.

SURFCONTROL REPORT CENTRAL

SurfControl Report Central (SRC) is Web Filter's reporting module, and allows you to run a wide range of reports through a web interface. SRC can be installed on the Web Filter server. If you want to install SRC on a separate server, make sure that server meets the minimum SRC system requirements. See the Report Central *Starter Guide* for more information.

VIRTUAL CONTROL AGENT

The Virtual Control Agent (VCA) is an optional component that dynamically categorizes URLs that are not in SurfControl's URL Category List. The VCA runs as a service, typically on the Web Filter server. However, you can install the VCA on a separate server. This is done by installing the full version of Web Filter on a separate server and disabling all other services.



Note: SRC and the VCA are typically installed on the Web Filter server, though you may choose to install these on separate servers. For example, you may want to move the individual components off the Web Filter server if you are already using a remote database, and your user count is nearing the maximum of what your Web Filter server can handle.

MOBILE FILTER

SurfControl Mobile Filter allows you to filter remote users, such as employees using company laptops. There is an option to install Mobile Filter during the Web Filter installation. It is deployed on a server in the demilitarized zone (DMZ), and on the client computers to be filtered by Mobile Filter.

Once the Mobile Filter server is installed and configured, SurfControl Web Filter detects these users and displays them as objects in the WHO tab of the Rules Administrator. Using either the Mobile Filter server or the Web Filter Rules Administrator, you can add these users to your filtering rules. See the Mobile Filter *Starter Guide* for more details.

REMOTE ADMINISTRATION CLIENT

System administrators can remotely administer Web Filter by installing the Remote Administration Client. From the client installation you can:

- View monitored traffic.
- Create and edit rules.
- Run reports.
- Start and stop the Web Filter Service.
- Start and stop the Scheduler Service.
- Access the Real-Time Monitor.
- Manage your Mobile Filter Clients.

Before installation, make sure the Remote Administration client computer meets the minimum requirements listed in the table below:

Table 2-18 Remote Administration Client minimum requirements

Component	Minimum	Recommended
Processor	Intel Pentium III	Intel Pentium IV
Memory	256 MB RAM	512 MB RAM
Supported Operating Systems (with latest Service Packs)	Windows 2000 Professional or Server Windows 2000 Advanced Server Windows Server 2003 Standard and Enterprise Editions Windows XP Professional Windows Vista Business and Enterprise Editions	
Network	Ethernet card	
Disk Space	5 GB free	
Web browser	MS Internet Explorer 5.0	MS Internet Explorer 6.0

PRIVACY EDITION CONSIDERATIONS

In certain European countries, there are laws which forbid the browsing details of users to be seen by monitoring software, unless express permission is given by a manager and a union representative. The Privacy Edition of SurfControl Web Filter enables companies in those countries to comply with this legislation.

You can only upgrade from the previous Privacy edition (5.0) to version 5.5. You cannot upgrade from any standard version of Web Filter to the Privacy edition. For more details on the Privacy Edition features, see the *Administrator's Guide*.

2

INSTALLATION DECISIONS *Other Considerations*

Installing Web Filter

Introduction	page 44
Installing SQL Server Express (optional)	page 45
Installing SurfControl Web Filter	page 46
Configuring Web Filter	page 53
Installing Service Pack 3.....	page 66

INTRODUCTION

The following sections show you how to install Web Filter Service Pack 3 along with instructions on how to install SQL Server and Web Filter version 5.5, if you have not already installed these products. There are three steps to installing Web Filter Service Pack 3:

- **Install SQL Server** - You must install SQL Server before installing Web Filter V5.5. If you have not installed SQL Server already then go to "[Installing SQL Server Express \(optional\)](#)" on page 45.
- **Install Web Filter V5.5** - Once you have installed SQL Server you need to install Web Filter V5.5. If you have installed SQL Server but not Web Filter V5.5 then go to "[Installing SurfControl Web Filter](#)" on page 46.
- **Install Service Pack 3** - Once you have installed SQL Server and Web Filter V5.5 you are ready to install Service Pack 3. See "[Configuring Web Filter](#)" on page 53.

This chapter explains how to install SurfControl Web Filter. There are six stages to the installation process, which are explained in the table below:

Table 3-1 Installation Process

Database platform preparation	If you have chosen SQL Server Express as your database platform, download and install it from the Microsoft Web site. See " Installing SQL Server Express (optional) " on page 45.
Product preparation	If you plan to monitor NetWare user names , install the NetWare client on to the Web Filter server .
Product installation and Configuration Wizard	Install Web Filter (complete installation) on the Web Filter server .
Remote Administration	If you want to administrate the Web Filter server from a remote location, install the Remote Administration client on the remote computer. Install the VCA client if required.
Post installation	If you plan to monitor Windows users by user name, install EUM, either by: <ul style="list-style-type: none"> • Installing the EUM Agent on all your domain controllers or NetwareEUM on to your NDS servers. • Installing the EUM Login Agent on your network and editing the supplied configuration file.
Report Central	Download and install SurfControl Report Central from: http://www.surfcontrol.com .

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 installing 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.aspx>



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 may be requested to restart the server after installing SQL Express.

INSTALLING SURFCONTROL WEB FILTER

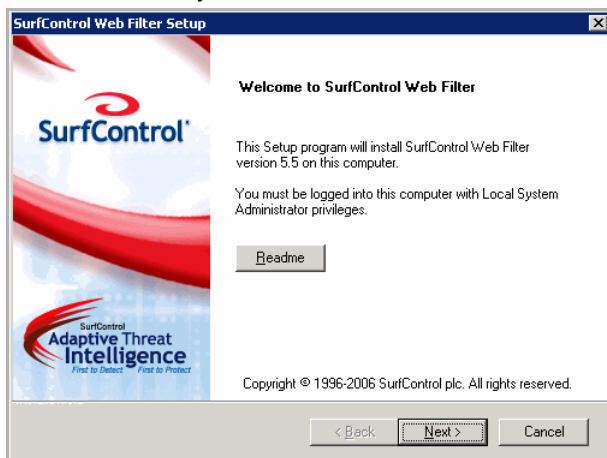
You can cancel the installation of Web Filter at any time by clicking **Cancel**. You will have to restart the installation process if you decide to run the install again at a later date.



Caution: The Microsoft firewall service is temporarily stopped and restarted during the Web Filter installation process, and as a result will interrupt Web browsing.

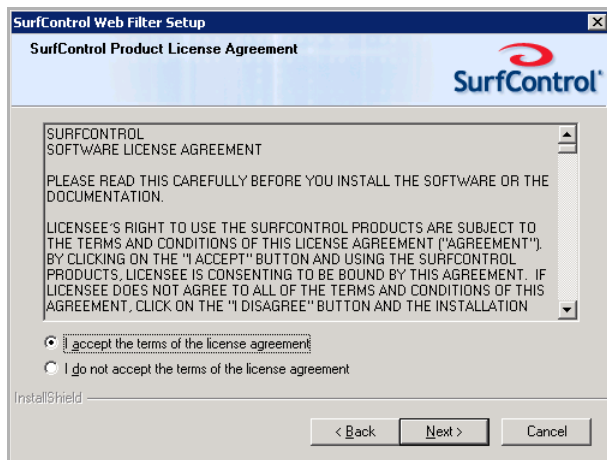
If you have an available Microsoft SQL Server, or you have installed SQL Server Express, you can install Web Filter V5.5:

- 1 Download Web Filter V5.5 from the SurfControl website then navigate to this file and double-click **setup.exe**. This will start the installation process.
- 2 The first screen you will see is the **Welcome** screen:



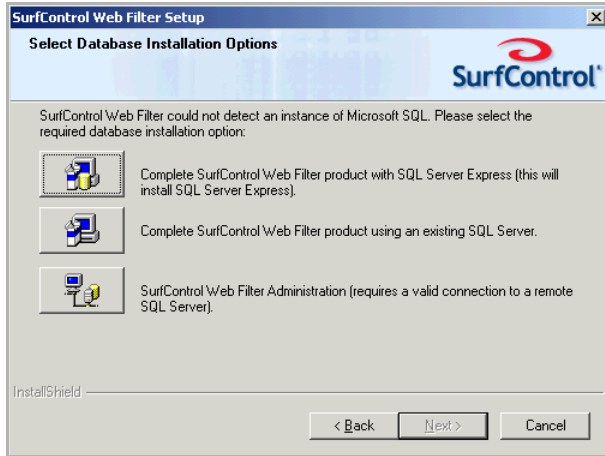
Click **Next**.

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






Select **I accept the terms of the license agreement**.

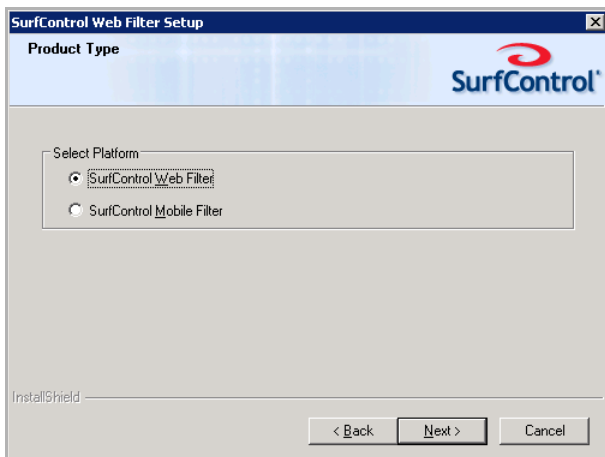
- 4 Click **Next**.
- 5 If the setup program does not detect a suitable database, you will see the **Select Database Installation Options** screen:



Note: If you have already installed SQL Server Express or SQL Server, this screen will not display.

- 6 Click one of the following depending on how you want to install Web Filter:
 -  – 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.
- 7 Click **Next**.

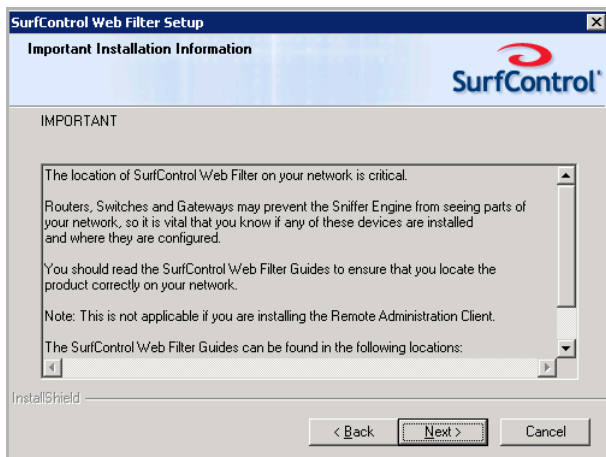
- 8 The **Product Type** screen is displayed:



Select **SurfControl Web Filter**.

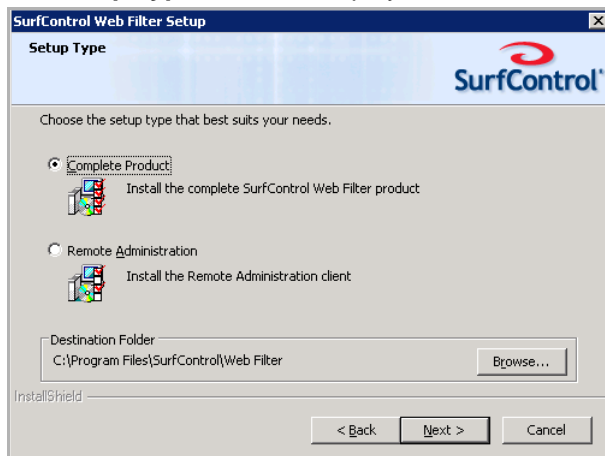
- 9 Click **Next**.

- 10 You will now see a screen which gives you important information about the location of Web Filter on your network. Prior to starting the installation, you should have determined the appropriate network configuration for Web Filter. This information is critical to the successful functioning of Web Filter and should be read carefully:



When you have read this information, click **Next**.

11 The **Setup Type** screen is displayed:



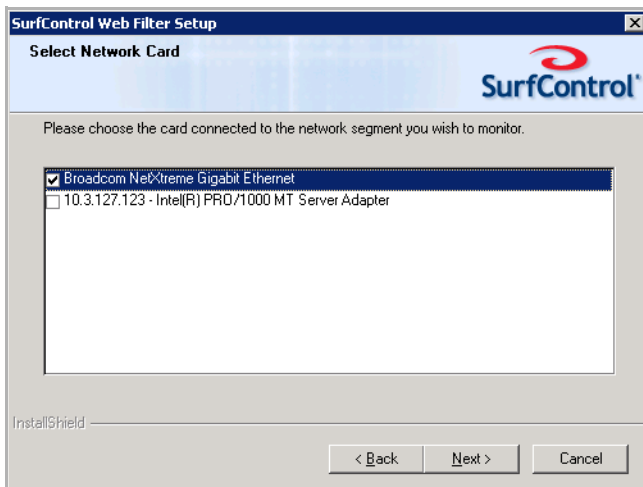
This screen enables you to specify how you want Web Filter to be installed:

- **Complete Product** - Select this option to install the complete SurfControl Web Filter program.
- **Remote Administration** - This enables you to access and manage the Web Filter server from any machine on your network.

The setup program installs Web Filter to a default path of `c:\program files\SurfControl\Web Filter`. If you want to install Web Filter to a different location on the server, click **Browse** and navigate to the location.

12 Once you have selected your setup type, click **Next**.

13 If you have multiple network cards (NICs) installed, the **Select Network Card** screen is displayed:



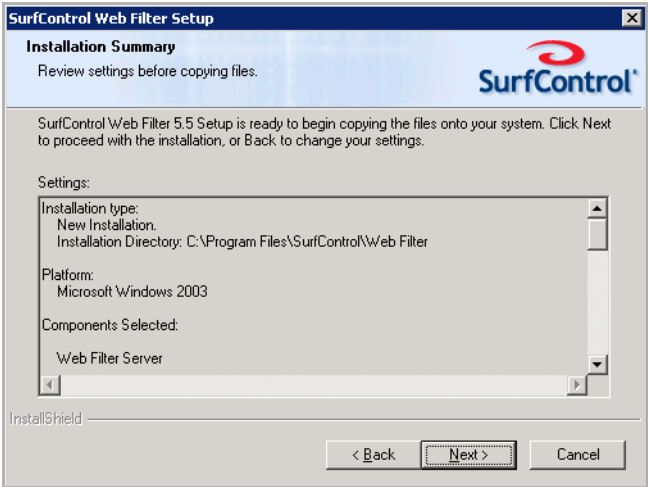
Select the card you want to be bound to the Web Filter Service, so that it will monitor Internet traffic.

14 Click **Next**.

3 INSTALLING WEB FILTER

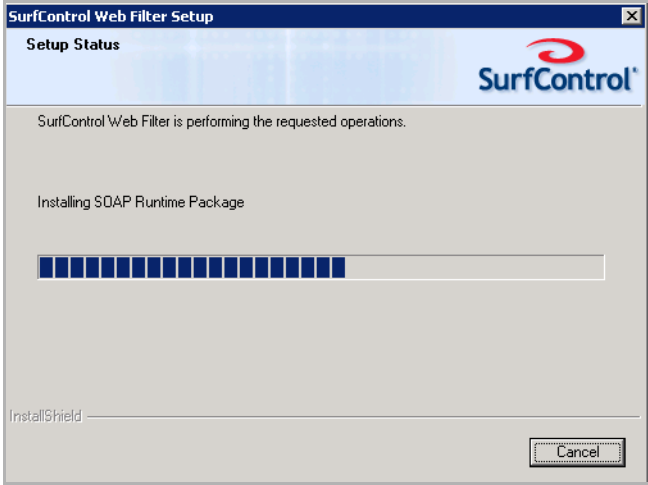
Installing SurfControl Web Filter

15 You will now see a screen giving you a summary of the installation options you have chosen:



Review your settings before starting the installation. When you are ready, click **Next**.

16 A status bar will indicate that the Web Filters are being copied to the server:



- 17 Once the files are copied across an Install Wizard Complete screen will indicate that Web Filter has been successfully installed:



Click **Finish**.


The **Configuration Wizard** will start automatically. See "[Configuring Web Filter](#)" on page 53 for more details.




Note: If you are asked to restart your computer the Configuration Wizard will begin automatically after the computer has restarted.

CHANGES TO THE SERVER

Installing Web Filter makes changes to the server:

- The WebFilter icon  can be seen in the Notification area at startup. This enables you to 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 WebFilter icon  becomes grayed out.



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

- The necessary registry entries.
- The SurfControl_WebFilter database (default name `SurfControl_WebFilter`).
- The following services:
 - Web Filter service
 - Scheduler service
 - Remote Administration service
 - Audit Logger service
 - Virtual Control Agent service (license-holders only)
 - Corporate Network Detection Service (CNDS)

CONFIGURING WEB FILTER

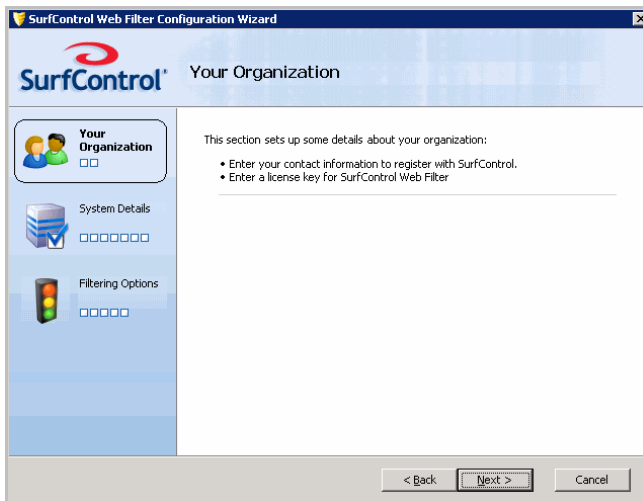
The wizard will launch after you have finished the complete installation process on your Web Filter server. Perform the following steps to complete the Configuration Wizard:

- 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**.

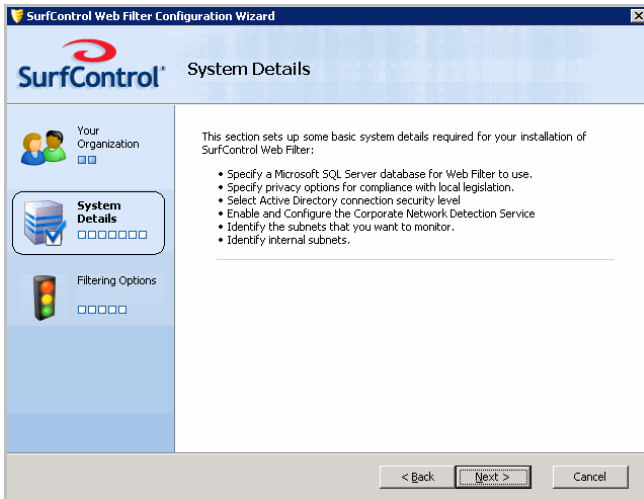
- 3 The **Customer Information** screen is displayed.

Fill in your details to register with SurfControl. Registered users can schedule live updates of the Internet Threat Database.

- 4 Click **Next**.
- 5 The **Licensing** screen is displayed.

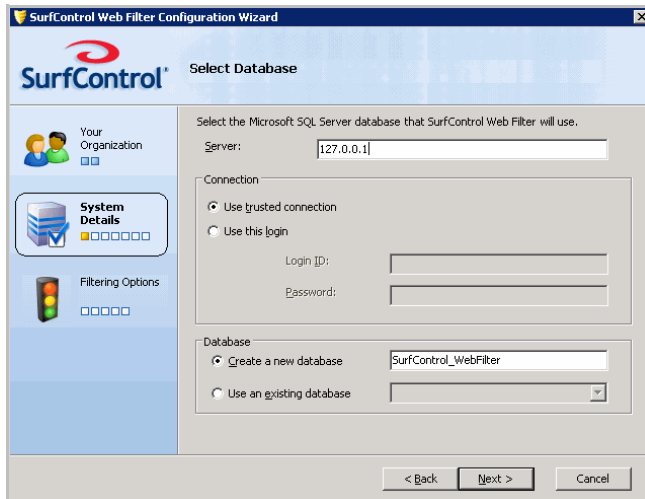
- If you are an evaluating customer, select **I am evaluating SurfControl Web Filter** and Click **Next**.
- If you have purchased a Web Filter license, select **I have purchased a license** and enter your license key. Click **Next**.
- If you have purchased Web Filter but do not have a license key, contact SurfControl Sales.

- The **System Details** screen is displayed. This screen outlines the information you will have to enter in this section.



Click **Next**.

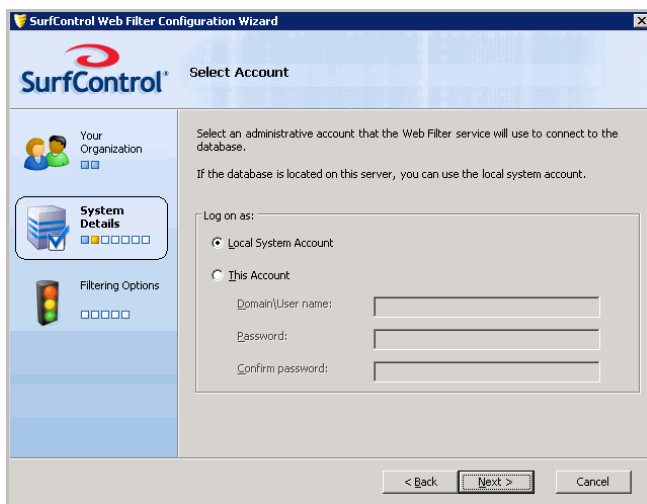
- The **Select Database** screen is displayed.



- Enter the name or IP address of the server where your SQL Server Express or SQL Server database is located into the **Server** text box.
- Specify how you want Web Filter to connect to the database by selecting a **connection** option. Web filter can either log in using your database's SA username and password, or using a trusted connection.
- In the Database section, specify whether you want to use an existing Web Filter database, or create a new one.

- Click **Next**.

9 The **Select Account** screen is displayed.

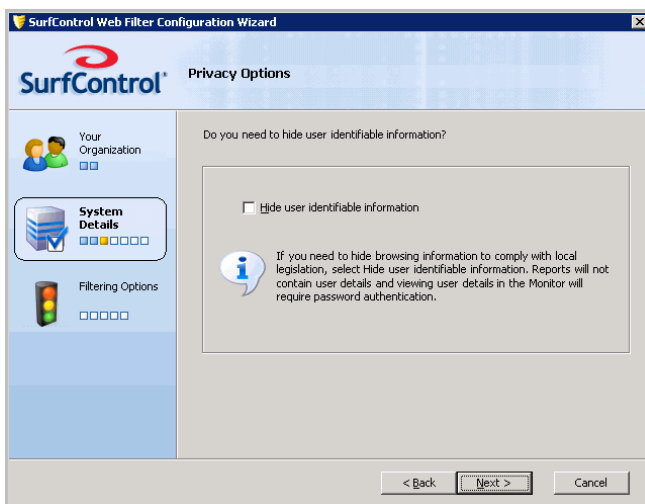


Choose how Web Filter will log on to your database:

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

10 Click **Next**.

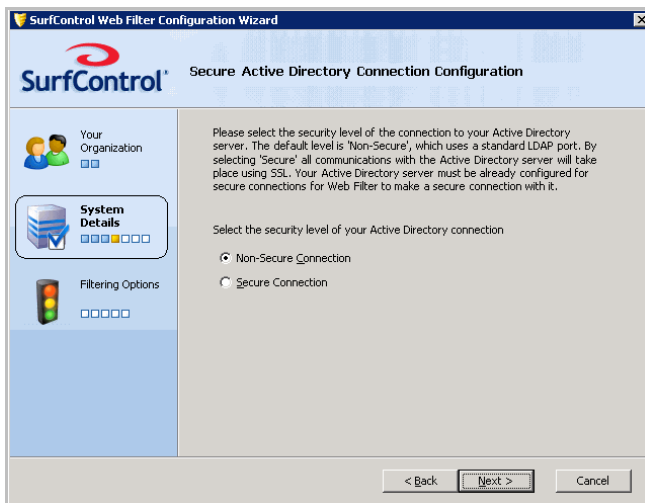
11 If you did not select a database in Step 6 you will now see the **Privacy Options** screen:



This enables you to specify that user information needs to be hidden to comply with regional legislation. Select **Hide user identifiable information**.

12 Click **Next**.

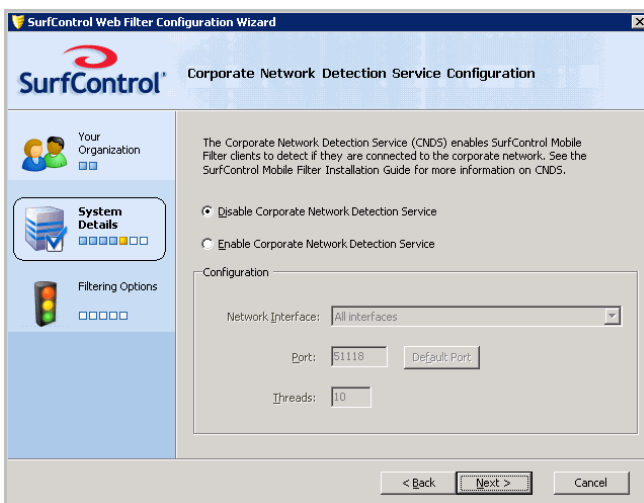
13 The **Secure Active Directory Connection Configuration** screen is displayed.



By default a non-secure connection is made to your Active Directory server. To change this to a secure SSL connection, select **Secure Connection**.

14 Click **Next**. Web Filter will attempt to make a secure connection.

15 You will now see the **Corporate Network Detection Service Configuration (CNDS)** screen:



This service is used by SurfControl Mobile Filter to detect when clients are connected to a corporate Web Filter server, which then takes over the filtering of the connected device from. This service must be installed on the Web Filter server. Choose a CNDS configuration option:

- Select **Disable Corporate Network Detection Service** (the default option), if you do not plan to install Mobile Filter.

- Select **Enable Corporate Network Detection Service** if you are installing Mobile Filter. For more information on this service, consult the SurfControl Mobile Filter *Starter Guide*.



Note: SurfControl recommends leaving the configuration options at the default setting, unless advised to change them by Technical Support. You can change these settings after installation from the **Start > All Programs > SurfControl Web Filter > Configure Corporate Network Detection Service** menu.

16 Click **Next**.

17 The **Subnets** screen is displayed.

You can reduce the load on a single Web Filter server, or balance the load between multiple Web Filter servers.

For a Single server:

- i Identify any external traffic subnets (intranet Web servers for example).
- ii Click **Add** and enter the IP address and subnet mask.
- iii Select **Do not monitor traffic to or from these subnets**.

For Multiple Servers:

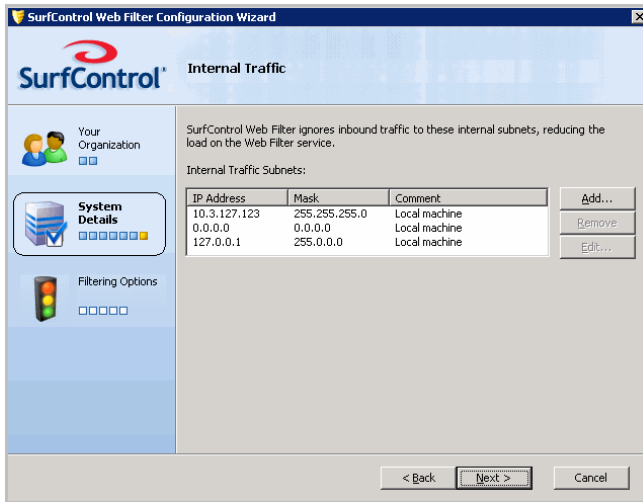
- i Identify one server and set up as a single server.
- ii For subsequent servers, identify the subnets you **DO** want to monitor.
- iii Click **Add** and enter the relevant IP addresses and subnet masks.
- iv For these subnets, select **Only monitor traffic to or from these subnets**.

18 Click **Next**.



Note: These settings can be changed in the Subnets tab in the Web Filter Service Settings following installation.

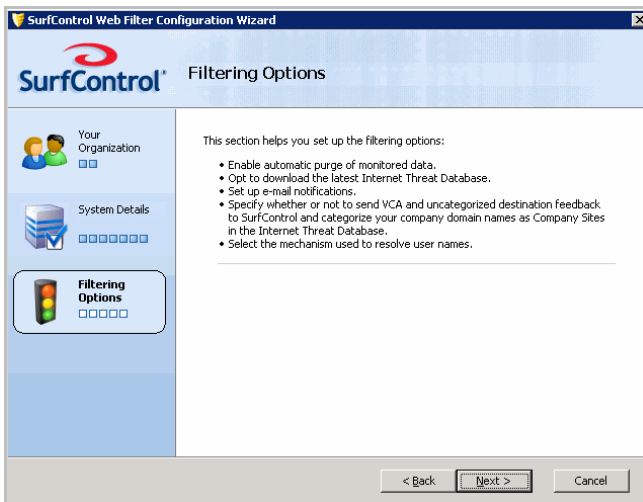
19 The **Internal Traffic** screen is displayed.



Web Filter detects the internal subnets on your monitoring and blocking network interface card (NIC). The Web Filter server ignores inbound traffic to these internal subnets, reducing the load on the Web Filter.

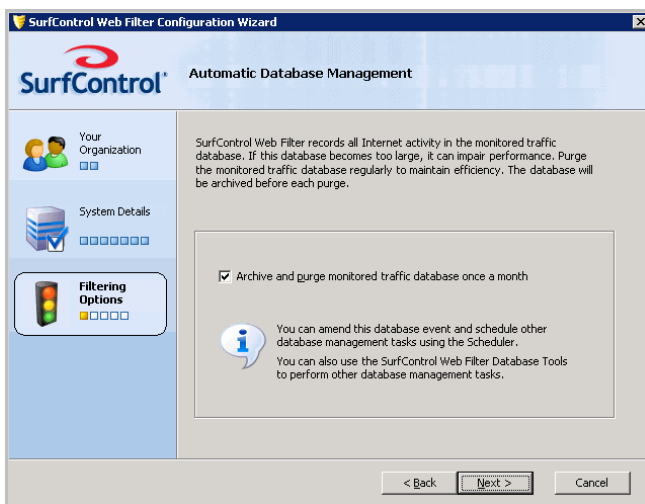
- Click **Add** if you wish to add further internal subnets.
- Click **Remove** or **Edit** to remove or configure the subnets detected by Web Filter.
- Click **Next**.

20 The **Filtering Options** screen is displayed. This screen outlines the information you will enter in this section.



Click **Next**.

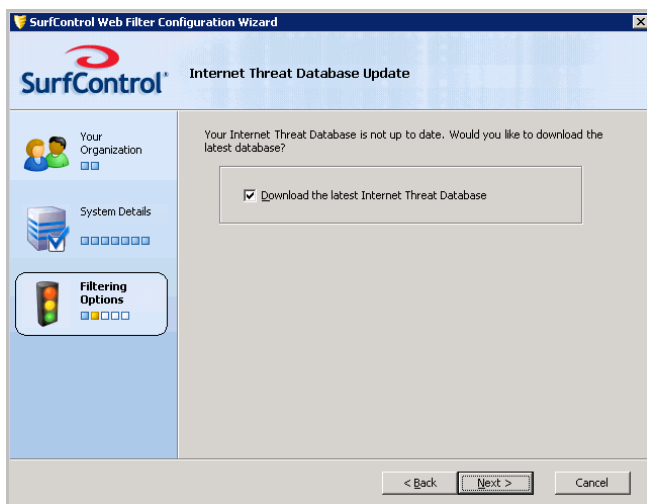
21 The **Automatic Database Management** screen is displayed.



If you want the Web Filter database to be purged automatically, select **Archive and purge monitored traffic database once a month**.

22 Click **Next**.

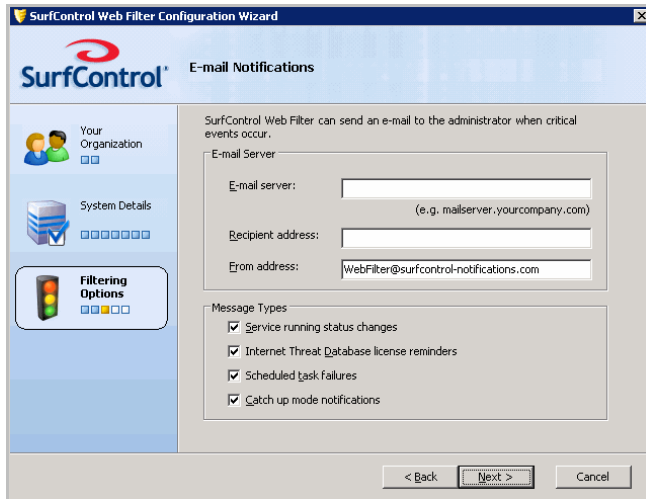
23 The **Internet Threat Database Update** screen is displayed:



For maximum protection you need the latest threat information. Select **Download the latest Internet Threat Database**.

24 Click **Next**.

25 The **E-mail Notifications** screen is displayed:

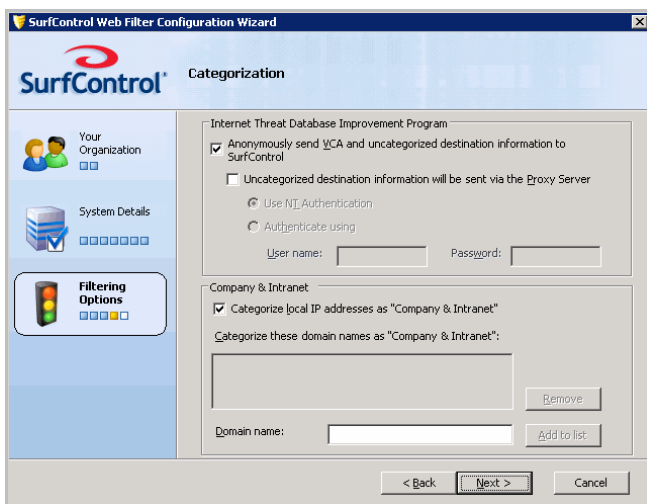


Web Filter can notify you when system events occur. Fill in the fields as follows:

- i Enter the name or IP address of the e-mail server for your domain into the **E-mail Server** text box. Web Filter will use this e-mail server to send notifications.
- ii Enter the e-mail address of the person who will receive the e-mails (normally the systems administrator), into the **Recipient address** text box.
- iii Enter the e-mail address which the notification e-mails will be sent from, into the **From address** text box.
- iv Now specify which **Message Types** you want to be notified of. Choose any or all of the following:
 - **Service running status changes** - Select this option if you would like to be notified about changes in the Web Filter Service status.
 - **Internet Threat Database license reminders** - Select this option if you want to be notified about the category database subscription expiration.
 - **Scheduled task failures** - Select this option if you want to be alerted about any scheduled tasks which fail to run.
 - **Catch up mode notifications** - If the Web Filter service becomes overloaded, monitoring will be restricted to HTTP traffic. If the overload becomes critical, monitoring will be temporarily suspended. An e-mail will be sent when Web Filter enters and exits catch up mode.

26 When you have made your choices, click **Next**.

27 The **Categorization** screen is displayed:

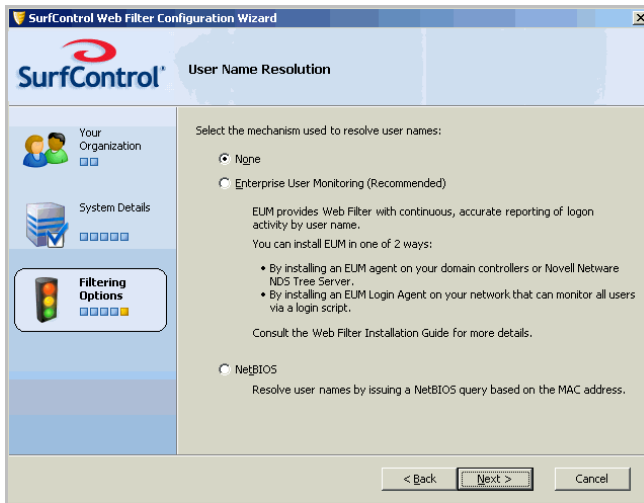


When Web Filter encounters an uncategorized Web destination, it can send the details anonymously to SurfControl, to help improve the effectiveness of the Internet Threat Database.

- i Select the **Anonymously send VCA and uncategorized destination information to SurfControl** check box, if you want to send this information anonymously to SurfControl. Clear the check box if you want to opt out of sending this information.
- ii If your computer accesses the Internet via a proxy server, select the **Uncategorized destination information will be sent via the proxy server** check box.
 - Select **Use NT Authentication** if you want the proxy server to validate the VCA by using NT authentication.
 - If you want to use a different user name and password to access the proxy server, select **Authenticate using** and enter the logon credentials.
- iii 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.
- iv Click **Add** to add your domain (without entering the http://www prefix).

28 Click **Next**.

29 The **User Name Resolution** screen is displayed:



By default, User Name Resolution is not selected. Choose one of the following:

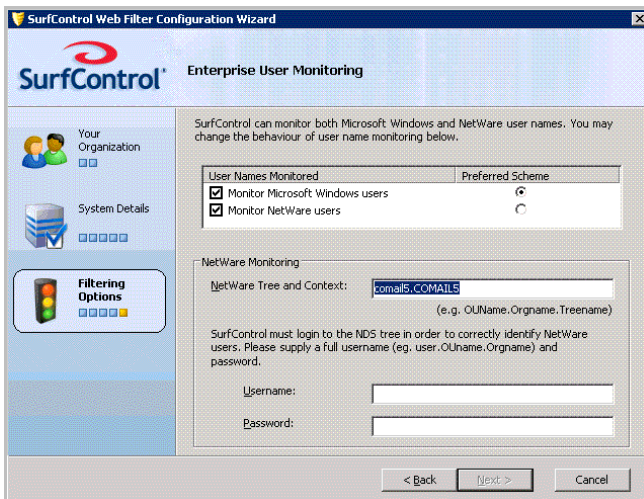
- Enterprise User Monitoring (recommended)
- NetBIOS

30 Click **Next**.



Note: You can change the way you resolve user names following installation from the Web Filter Settings in the Enterprise Manager > Maintenance options.

31 If you are installing on a **Novell NetWare** environment, and selected **Enterprise User Monitoring** in step 17, the **Enterprise User Monitoring** screen is displayed.



You have the following options:

- **User Names Monitored** - Monitor by either Windows or NetWare users, or both (the default). You can also select which is your preferred scheme.

3

INSTALLING WEB FILTER Configuring Web Filter

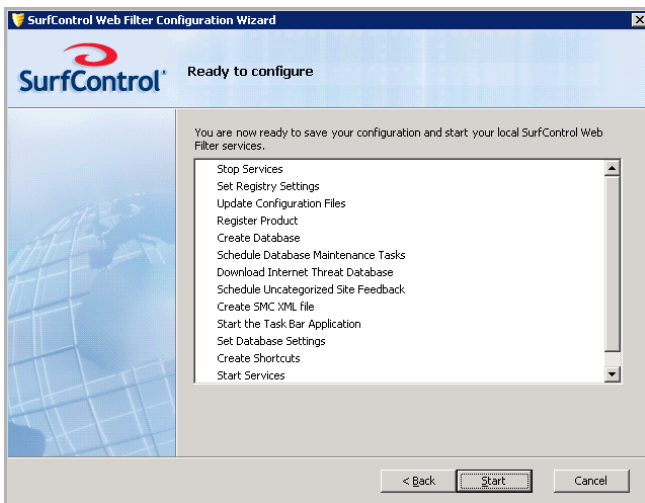
- **NetWare Monitoring** - Your NetWare Tree and Context details are automatically displayed in this field.
- **Username and Password** - You need to enter a valid NDS tree username and password to enable Web Filter to identify NetWare users.



Note: You can select EUM during the installation process, and enter the details once the installation is complete. Information can be entered into the User Name Resolution tab in the Web Filter Settings. See Chapter 9 of the *Administrator's Guide* for more details.

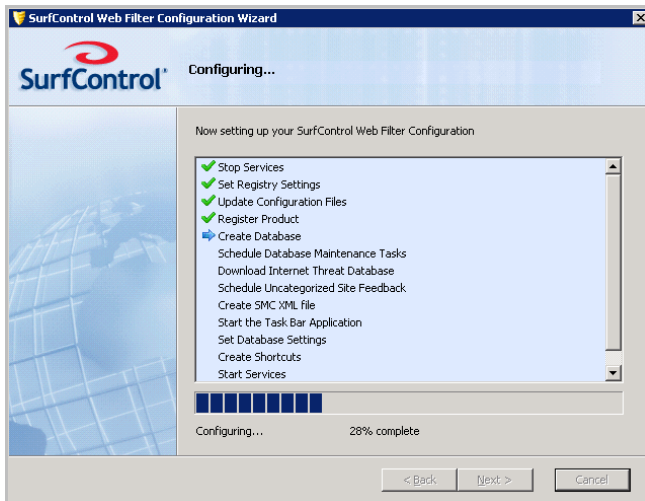
32 Click **Next**.

33 The **Ready to Configure** screen is displayed. In the box you can see a list of the tasks that the Configuration Wizard will do to configure Web Filter.





Click **Start**.

34 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 or one of the following:

- 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, Web Filter may not filter traffic effectively.

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



36 Click **Finish**.

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 www.surfcontrol.com.

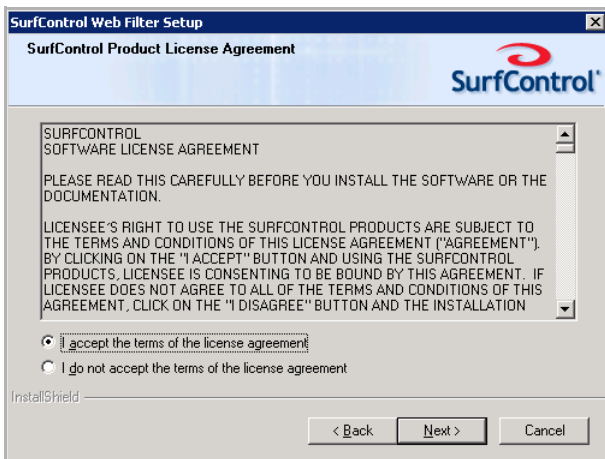
INSTALLING SERVICE PACK 3

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. You will now see the Welcome screen:

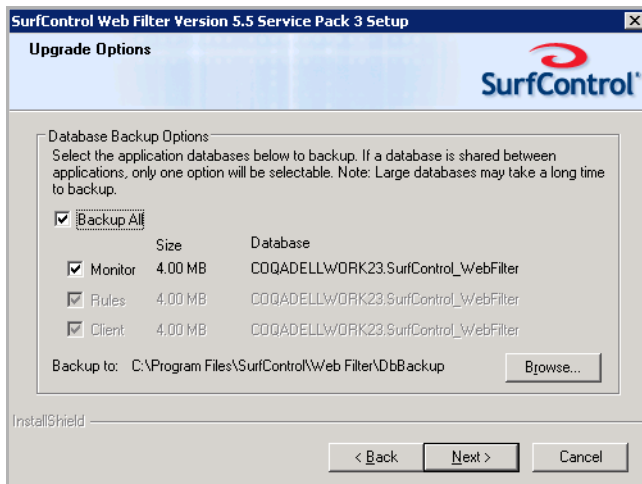


- 3 Click **Next**.
- 4 When you see the **License Agreement** screen, select **I accept the terms of the license agreement**:



- 5 Click **Next**.

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



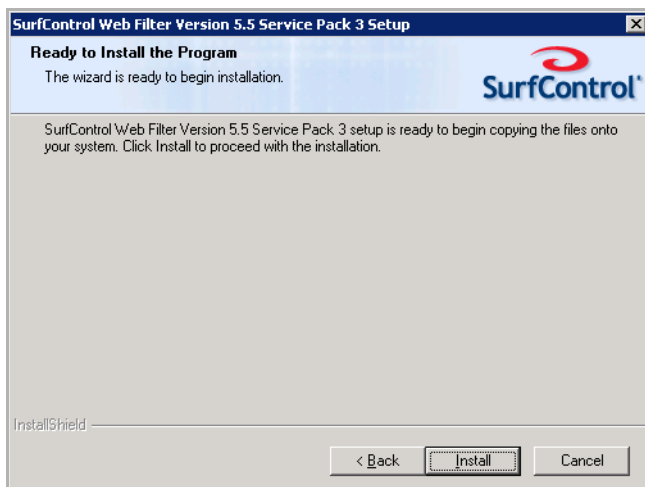
This will enable you to 'roll back' to your previous database, should this be necessary:

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



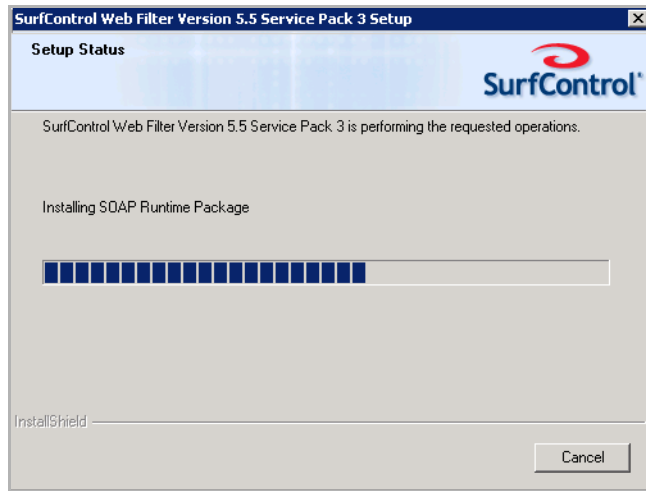
Note: If a database is shared with more than one application, you will only be able to select one of the applications that uses it.

- 7 Click **Next**.
- 8 You will now see a screen informing you that the wizard is ready to install the service pack:

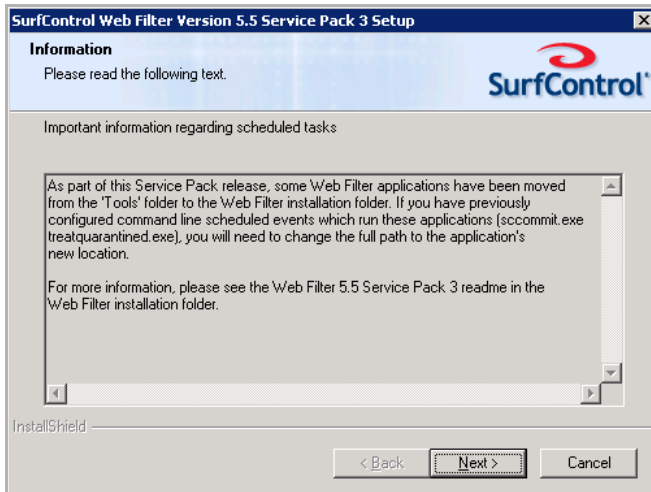


3 INSTALLING WEB FILTER Installing Service Pack 3

- 9 Click **Install** to start the installation. A progress bar will indicate 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.

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

3 **INSTALLING WEB FILTER**

Installing Service Pack 3

Further Configuration

Post Installation Tasks	page 72
User Name Resolution	page 73
Install SurfControl Report Central	page 79
Network Card Configuration.....	page 80
Installing the Remote Administration Client.....	page 83

POST INSTALLATION TASKS

Following the installation of Web Filter, there are a number of tasks you may need to perform. Some apply to all installations, others are dependent on your network configuration.

ALL INSTALLATIONS

The following procedures should be performed after configuring Web Filter.

- How to perform **User Name Resolution** ([page 73](#))
- Install **SurfControl Report Central** ([page 79](#))

NETWORK DEPENDENT

The following procedure may be necessary, depending on how your network and Web Filter servers are set up.

- **Configuring multiple Network Interface Cards (NICs)**
If Web Filter detected more than one card on your server during installation, you will need to configure your cards correctly.
- **Install the Remote Administration version of Web Filter**
This allows you to access the Web Filter server from any machine on your network.

USER NAME RESOLUTION

By default, SurfControl Web Filter resolves user names by issuing a NetBIOS query based on the MAC address. Web Filter also includes the **Enterprise User Monitor (EUM)** utility for resolving user names in a routed network. In a NetWare environment you also have the option to monitor Novell User Names.

For more details about how EUM works, see "[User Name Resolution](#)" on page 17.

You can install EUM in the following ways:

- Install the **EUM Agent** on all your domain controllers.
- Install the **EUM Login Agent** on your network.
- Install **NetWareEUM** on your NDS Tree Servers.

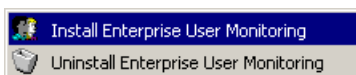
INSTALLING THE EUM AGENT ON DOMAIN CONTROLLERS

Before proceeding with the EUM Agent installation, check the following:

- Make sure that the Web Filter server has a static IP address.
- Make sure you have administrative privileges on all domain controllers where the User Agent will be installed.
- Make sure the Web Filter server is located in the correct domain.
- Make sure the firewall or router allows traffic through the provisioned port (default is 61695).
- For Windows NT domain controllers, make sure the security logs of the domain controllers are set to **overwrite events as needed**.
- Try to perform this procedure when there are few or no users on the network, or when a forced logoff can be scheduled. This ensures the fastest, most accurate detection of users.

To install the EUM Agent on to your Domain Controllers:

- 1 From the Start menu, launch the EUM installation wizard (**Start > Programs > SurfControl Web Filter > Enterprise User Monitoring > Install Enterprise User Monitoring**).

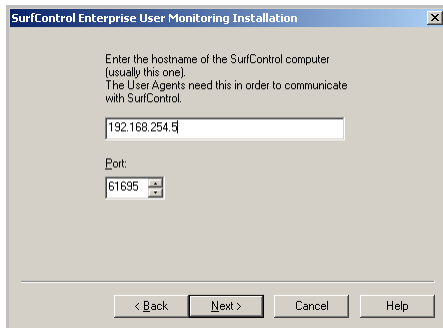


- The **SurfControl Enterprise User Monitoring Installation** screen is displayed.



Click **Next**.

- The **Hostname** screen is displayed.



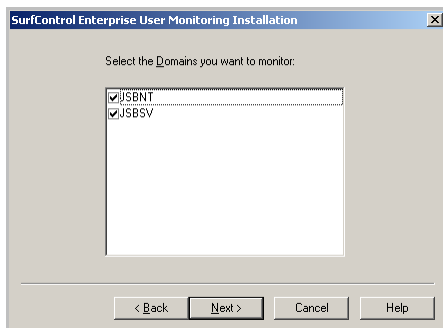
- Enter the IP address of the Web Filter server.



Note: SurfControl recommends entering the IP address instead of the hostname.

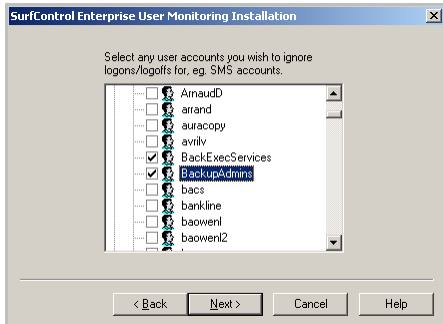
- Enter the port the User Agent and the Web Filter service should use to communicate (the default is 61695).

- Click **Next**.
- The **Domain List** screen is displayed.



Select the domains you want to receive user data from.

- 6 Click **Next**.
- 7 The **Ignore User Accounts** screen is displayed.



Select the user accounts whose logon activity do not need to be reported, for example, Systems Management Server (SMS) and antivirus accounts.

- 8 Click **Next**.
- 9 The **Select Domain Controllers** screen is displayed. Select the domain controllers whose user's logon and logoff activity Web Filter needs to monitor. (This identifies the domain controllers where the User Agent will be installed).
- 10 Click **Next**. You should now have successfully installed Enterprise User Monitoring.



Note: Installation of the EUM UA on to Microsoft Windows 2000 domain controllers will require a restart. SurfControl recommends performing a manual restart of the domain controller.



Note: Failure to install EUM on all domain controllers can compromise the accuracy of user name resolution. If a domain controller is authenticating users, but not passing that data to Web Filter, user activity may be recorded under another user name.

Making changes to the EUM Agent configuration

After installing the EUM Agent, you may want to add further domain controllers to your EUM Agent configuration, specify more users that the EUM Agent should ignore, or specify how long your domain controllers should wait before sending configuration information to the Web Filter server(s).

The EUM Agent on the domain controller will wait ten minutes before checking for any changes made in the scua.ini file. The frequency of this can be changed by altering a registry setting on individual domain controllers. To change this value, perform the following:

- 1 On the domain controller, launch the Windows registry.
- 2 Depending on your operating system, navigate to one of the following keys:
 - **Windows 2000 and 2003**
HKLM\SOFTWARE\JSB\SurfControl SubAuth\ConfigReRead

- **Windows NT**

HKLM\SOFTWARE\JSB\SurfControl EUM\ConfigReRead

- 3 Edit the **ConfigReRead** value to the desired amount in seconds. By default, this value is set to 600 seconds (10 minutes).

There are two ways to add domain controllers or ignored users to the EUM Agent configuration:

- Use the EUM Installation Wizard.
- Manually edit the **scua.ini** file on each domain controller.

Using the EUM installation wizard. To start the wizard, follow the instructions in the [Installing the EUM Agent on Domain Controllers](#) section. The installation wizard will automatically detect if the EUM Agent is already installed, and you can select additional domain controllers and/or ignored users to add to your existing EUM configuration.

Manually edit the scua.ini file. By default, the scua.ini file contains the host name and listening port number of the Web Filter server from which you initially installed the EUM Agent, and any ignored users you specified during the installation. You can add extra Web Filter servers to the file, if you want user login information to be returned from your domain controllers to multiple Web Filter servers. Below is an example of the scua.ini file:

```
[surfCONTROL_Services]

192.168.4.125=61695

192.168.4.119=61695

192.168.4.215=61695

[ignored_users]

domain\user1.test=1

domain\user2.test=1

domain\user3.test=1
```

To manually edit the file:

- 1 On the domain controller, open the **c:\Surfcontrol User Agent\scua.ini** file.
 - To add a new Web Filter server, type an entry underneath the `[surfCONTROL_Services]` section, in either one of the following formats:

```
hostname=61695

ip_address=61695
```

- To manually add an ignored user, type an entry underneath the `[ignored_users]` section, in the following format:

```
domain\user.name=1
```

- 2 Save the **scua.ini** file.

INSTALLING THE EUM LOGIN AGENT ON YOUR NETWORK

The Login Agent program and configuration file can be found in the following location in a default install:
C:\Program Files\SurfControl\Web Filter\EnterpriseUserMonitoring>LoginAgent

- 1 Copy the Login Agent program (ScEumLoginAgent.exe) and configuration file (EumLogin.ini) to a folder on your network that is accessible to all users.
- 2 Edit the configuration file (EumLogin.ini). For details on the settings, see ["How to Configure the File" on page 23](#).
- 3 Create or edit an existing logon and logoff script to call the ScEumLoginAgent.exe program. See ["Configuring a Logon and Logoff Script" on page 24](#).



Note: If installing on Windows Server 2003, you will need to configure the Windows Firewall to accept traffic sent from the Login Agent Program. Please consult our Knowledge Base article 1775 on the SurfControl web site for more details.

INSTALLING NETWAREEUM

The following section contains various sets of instructions for installing and configuring EUM in a Netware environment.

Installing EUM on NetWare

- 1 Ensure Novell Client 32 was installed on the Web Filter server prior to Web Filter installation.
- 2 From the Web Filter server, log on to the Novell server with administrative rights.
- 3 Go to the SYS volume and create a directory (for example, nweum).
- 4 When creating the directory, use DOS 8.3 naming conventions.
- 5 Under this directory, copy the files nweum.nlm and scua.ini from the Web Filter server (in a default installation they are located in C:\Program Files\SurfControl\Web Filter\Netware) to the Novell server.
- 6 From the NetWare Server console, load the NLM by entering:

```
Load sys:\nweum\nweum.nlm
and pressing enter.
```



Note: The system will not allow you to load the NLM if a copy is already running.

Automatically loading the NetWare EUM

To automatically load the NetWare EUM every time the server is restarted you will need to edit the `sys:\system\autoexec.ncf` file. You can edit this file using any text editor from the workstation or from the NetWare Server:

- 1 To load the file, type:

```
Load edit sys:\system\autoexec.ncf
```

- 2 Add the following line at the end of the file:

```
load sys:\nweum\nweum.nlm
```

- 3 Save the file.

Unloading the NetWare EUM

From the NetWare Server console, type: `unload nweum.nlm`

Add Web Filter Servers to NetWare EUM

- 1 Unload the NetWare EUM as described above.
- 2 Add the details to the `surfcontrol_services` section of the `scua.ini` file in the following format:
 - `Machine_name_or_IP_Address=Port number`
 - The default port number is 61696. Win 2000 and 2003 EUM architecture uses the port number 61695 by default.
- 3 Save the `scua.ini` file.
- 4 Reload the NetWare EUM as described in [Automatically loading the NetWare EUM](#) above.

Ignored users in NetWare EUM

- 1 Unload the NetWare EUM as described above.
- 2 Edit the [Ignored Users] section of the **scua.ini** file. The format for adding ignored users is as follows:
`unique_user_key=fully_qualified_username_in_the_NDS_tree`
For example:
`user1 = admin.NW_5_1_SURF`
`user2 = tester.accounting.NW_5_1_SURF`
- 3 Save the **scua.ini** file.
- 4 Reload the NetWare EUM as described in [Automatically loading the NetWare EUM](#) above.

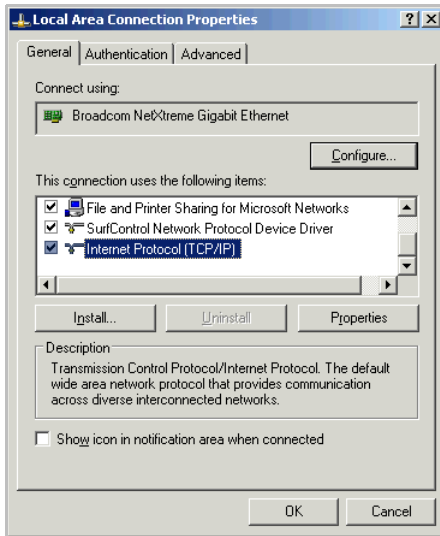
INSTALL SURFCONTROL REPORT CENTRAL

To produce reports on the Internet traffic monitored by Web Filter, you need to install SurfControl Report Central, either from a product DVD, or as a download from www.surfcontrol.com.

NETWORK CARD CONFIGURATION

Perform the following procedure if you have more than one Network Card (NIC) installed on your Web Filter server. First configure the single NIC:

- 1 Open the Properties dialog box for the Monitoring and Blocking NIC from your Network Connections (the one you bound to the Web Filter service during installation).

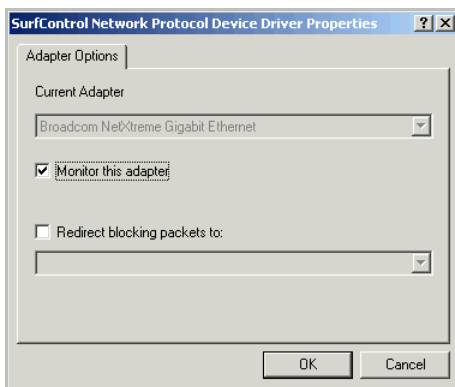


- 2 Make sure all necessary components are checked (including the Internet Protocol and SurfControl Network Protocol Device Driver).

The properties of the SurfControl Network Protocol Device Driver will only be available on servers that have the following:

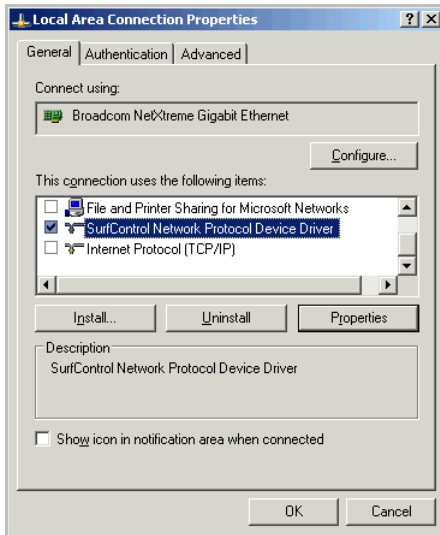
- Two or more NICs
- A driver which is bound to 2 NICs

- 3 Select Properties for the SurfControl Network Protocol Device Driver.

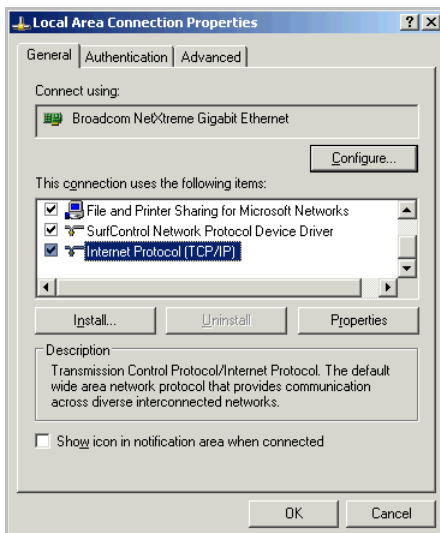


- 4 Make sure **Monitor this adapter** is selected. This indicates that this NIC is responsible for monitoring.
- 5 Make sure **Redirect blocking packets to** is not selected; this indicates that the Monitor NIC is also responsible for blocking.

- 6 Click **OK**.
- 7 Click **OK** again to close the NIC Properties dialog box.
- 8 Select Properties for the Monitoring NIC (this is the NIC you bound to the Web Filter service during installation).



- 9 Clear all items (including **Internet Protocol (TCP/IP)**), except the SurfControl Network Protocol Device Driver.
- 10 Select Properties for the SurfControl Network Protocol Device Driver.
- 11 Make sure **Monitor this adapter** is selected. This indicates that this NIC is responsible for monitoring.
- 12 Make sure **Redirect blocking packets to** is selected and choose the blocking NIC from the drop-down list box.
- 13 Click **OK** to continue.
- 14 Click **OK** again to continue.
- 15 Select Properties for the Blocking NIC.



4

FURTHER CONFIGURATION *Network Card Configuration*

16 Make sure **Internet Protocol (TCP/IP)** is selected.

This NIC is also responsible for blocking, for performing all DNS queries, for transferring data to the database and for receiving EUM data.

17 Select Properties for the SurfControl Network Protocol Device Driver.

18 Make sure **Monitor this adaptor** is not selected.

19 Make sure **Redirect blocking packets to** is not selected.

20 Click **OK**.

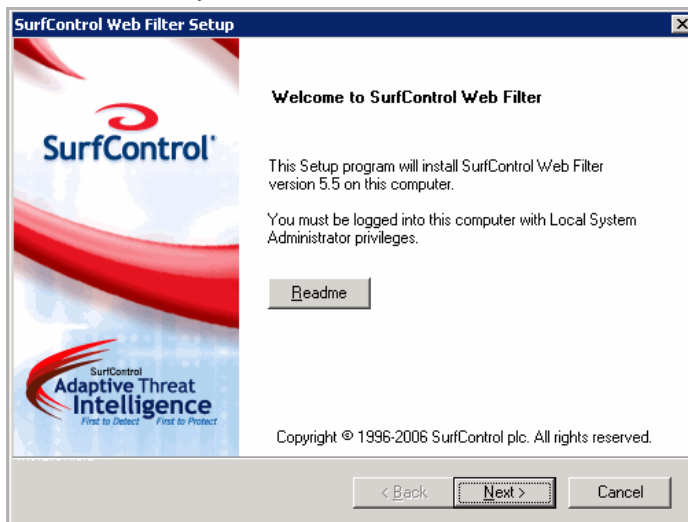
INSTALLING THE REMOTE ADMINISTRATION CLIENT

From the Remote Administration Client installation you can:

- View monitored traffic.
- Create and edit rules.
- Run reports.
- Start and stop the Web Filter Service.
- Start and stop the Scheduler Service.
- Access the Real-Time Monitor.

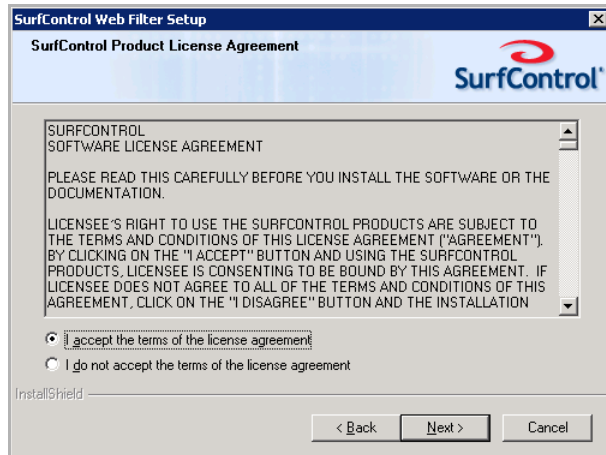
To install the Remote Administration Client:

- 1 Download Web Filter V5.5 from the SurfControl website then navigate to this file and double-click **setup.exe**. This will start the installation process.
- 2 The first screen you will see is the **Welcome** screen:



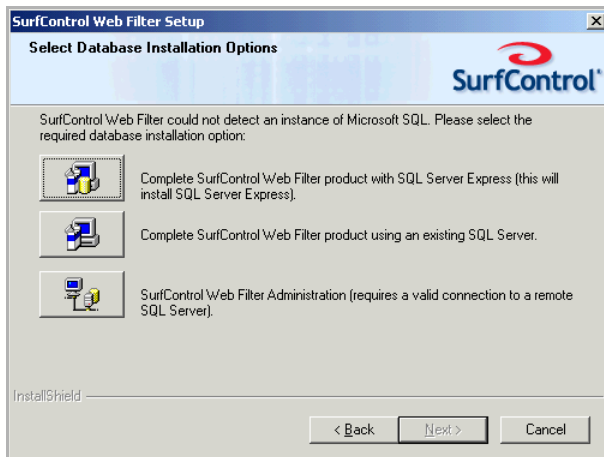
Click **Next**.

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



You need to accept the License Agreement for the installation to continue. Select **I accept the terms of the license agreement** and click **Next**.

- 4 If the setup program does not detect a suitable database, you will see the **Select Database Installation Options** screen:



Note: If you have already installed SQL Server Express or SQL Server, this screen will not display.

- 5 Click one of the following depending on how you want to install Web Filter:



– Install the complete product which will also install SQL Server Express.

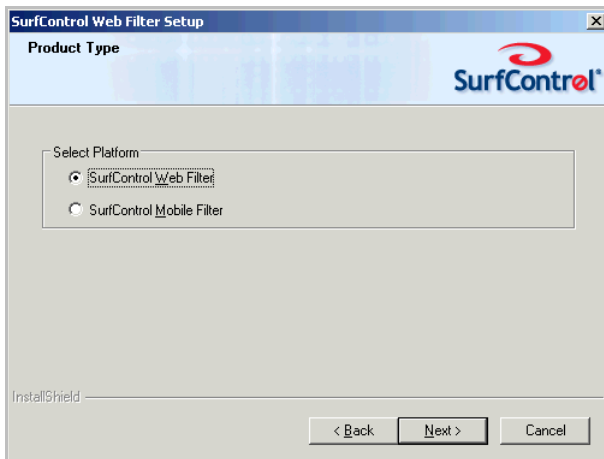


– Install the complete product using an existing SQL Server database.



– Install the Remote Administration version of Web Filter.

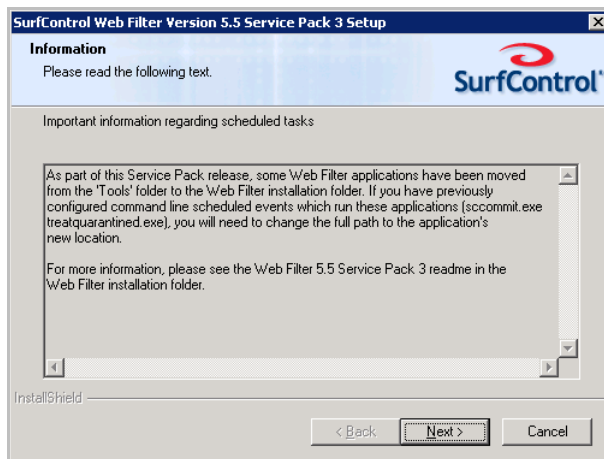
6 The **Product Type** screen is displayed:



Select SurfControl Web Filter.

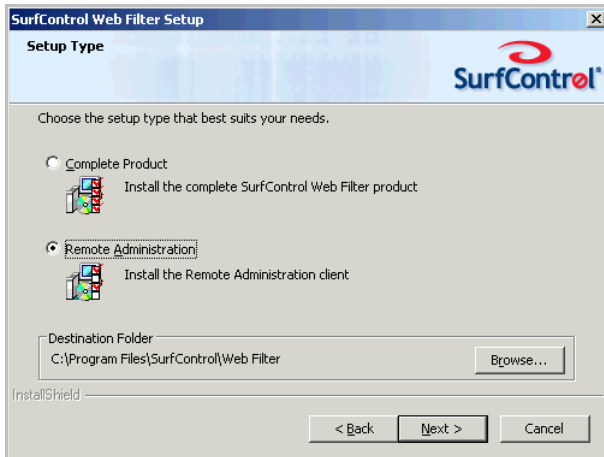
7 Click **Next**.

8 The **Important Installation Information** screen is displayed:



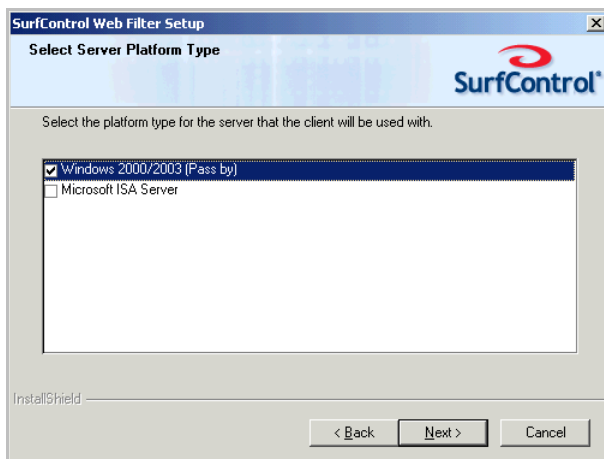
Click **Next**.

- 9 The **Setup Type** screen is displayed:



Select **Remote Administration**.

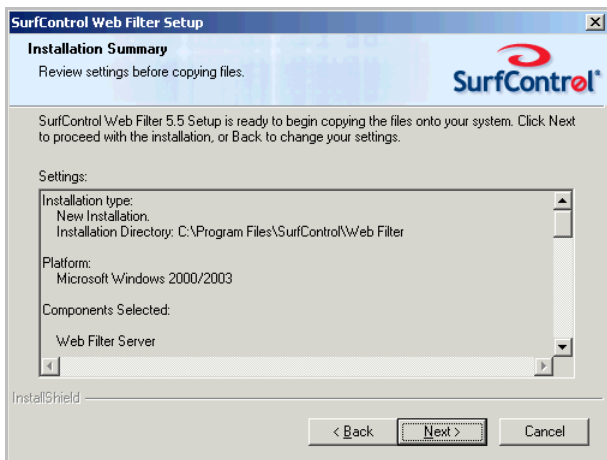
- 10 Click **Next**.
- 11 The **Select Server Platform Type** screen is displayed:



Select **Windows 2000/2003 (Pass By)**.

- 12 Click **Next**.

13 The **Installation Summary** screen is displayed. Review your settings before starting the installation.:



14 Click **Next**.

15 The **InstallShield Wizard Complete** screen is displayed.



Click **Finish**. The **Configuration Wizard** will start automatically.



Note: The Configuration Wizard for the Remote Administration is a subset of the Complete Product version.

The Remote Administration Client and Windows Vista

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

If your Remote Administration client is installed on Windows Vista, and UAC is enabled, each remote Web Filter application will need the permission of an elevated user to start. This means that you will either have to be logged in as Administrator, or as a standard user who knows the Admin password.

4

FURTHER CONFIGURATION *Installing the Remote Administration Client*



Appendix

Contact Technical Supportpage 90
Sales and Feedbackpage 92



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