



Version 5.5

SurfControl Web Filter

Installation Guide



NOTICES

Copyright © 2006 SurfControl plc. All rights reserved.

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

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

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

Copyright (c) 2003, VeriSign Inc.

All rights reserved.

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

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

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

This software is licensed under the BSD open source license. For more information visit www.opensource.org.

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

Copyright 2001-2004 Apache Foundation

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>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.

Comments on this Guide?

COMMENTS ON THIS GUIDE?

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

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

Version 5.5

October 2006

TECHNICAL SUPPORT

For the latest support information on SurfControl products, visit

<http://www.surfcontrol.com>

- Search our Knowledge Base - Our searchable database is constantly being updated and may be the quickest means to answering your questions regarding your SurfControl product.
- If your question or problem is not answered in the Documentation or the Knowledge Base, fill out an Online Support Request Form.
- Telephone Support - If you would like to speak with a Technical Support Representative, our excellent SurfControl Technical Support is just a phone call away.

SURFCONTROL SALES

For product and pricing information, or to place an order, contact SurfControl. To find your nearest SurfControl office, please visit our website.

<http://www.surfcontrol.com>

CONTENTS

Notices	i
Comments on this Guide?	ii
Technical Support	iii
SurfControl Sales	iii
Contents	v
INTRODUCTION	1
Standalone Windows Edition	2
Pass-by filtering technology	2
System Requirements	3
INSTALLATION DECISIONS	5
Introduction	6
Network Considerations	6
User Name Resolution	6
Database Considerations	6
Other Considerations	6
Network Considerations	7
Hub versus switch	7
Network placement	9
Multiple NIC support	12
User Name Resolution	14
EUM	15
Methods of Installing EUM	15
The EUM Agent on Domain Controllers	16
NetWareEUM	18
The EUM Login Agent	20
Database Considerations	23
SQL Server Express	23
SQL Server	25
Database Authentication	27
Other Considerations	28
Content	28
Categorization Options	28
E-mail Notifications	29
Remote Administration Client	30
Privacy Edition Considerations	30
INSTALLATION ORDER	31
Introduction	32
Installation Procedures	33
Changes to the Server	34

Contents

CONFIGURING WEB FILTER	39
Introduction	40
Configuration Wizard	41
Post Installation Tasks.....	49
All Installations	49
Network Dependent	49
User Name Resolution	50
Installing the EUM Agent on Domain Controllers	51
Installing the EUM Login Agent on your Network	53
Installing NetWareEUM	54
Install SurfControl Report Central	56
Network Card Configuration	56
Installing the Remote Administration Client	58



Chapter 1

Introduction

Standalone Windows Edition
System Requirements

page 2
page 3

STANDALONE WINDOWS EDITION

SurfControl Web Filter for Windows:

- Utilizes pass-by technology (no latency).
- Provides for 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 violates a set of rules (like unacceptable destination or unauthorized IP source.), the filtering software injects 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

Table 1-1 gives the minimum and recommended specifications for installing SurfControl Web Filter and SurfControl Report Central.

Table 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)	Windows 2000 Server Windows 2000 Advanced Server Windows Server 2003 Standard Edition Windows Server 2003 Enterprise Edition	
Network	Up to three Network Interface Cards (NICs) in promiscuous mode.	
Supported database platforms (with latest Service Packs)	Microsoft SQL Server Express (Requires Windows Installer 3.1 if installing on a Windows 2000 computer) Microsoft SQL Server 2000 Microsoft SQL Server 2005 Note: SurfControl recommends that you install SQL Server Express or SQL Server before installing Web Filter.	
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. 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 6.0
Applications	Adobe Acrobat Reader 6 for viewing reports and documentation in pdf format.	

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

- A single Web Filter remote administration client installed.
- SRC installed on 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.msp#>

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



Chapter 2

Installation decisions

Introduction	page 6
Network Considerations	page 7
Multiple NIC support	page 12
User Name Resolution	page 14
Database Considerations	page 23
Other Considerations	page 28

INTRODUCTION

You must make decisions on the following before installing SurfControl Web Filter. You will need this information when running the Configuration Wizard. See “Configuration Wizard” on page 41 for more details:

NETWORK CONSIDERATIONS

- 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)?

See “Network Considerations” on page 7 for more details.

USER NAME RESOLUTION

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

See “User Name Resolution” on page 14 for more details.

DATABASE CONSIDERATIONS

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

See “Database Considerations” on page 23 for more details.

OTHER CONSIDERATIONS

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

See “Other Considerations” on page 28 for more details.

NETWORK CONSIDERATIONS

SurfControl Web Filter is modular in design, which allows maximum flexibility in network configuration. The location where you place the Web Filter server depends on your network's configuration.

Web Filter uses a sniffer engine to monitor Internet traffic. Therefore, the location of the Web Filter server is critical. Web Filter can only monitor and block the Internet traffic it can see. Routers, switches, and gateways may prevent Web Filter from seeing certain parts of your network. You must 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 (see Figure 2-1), Web Filter is able to intercept the request and filter accordingly.

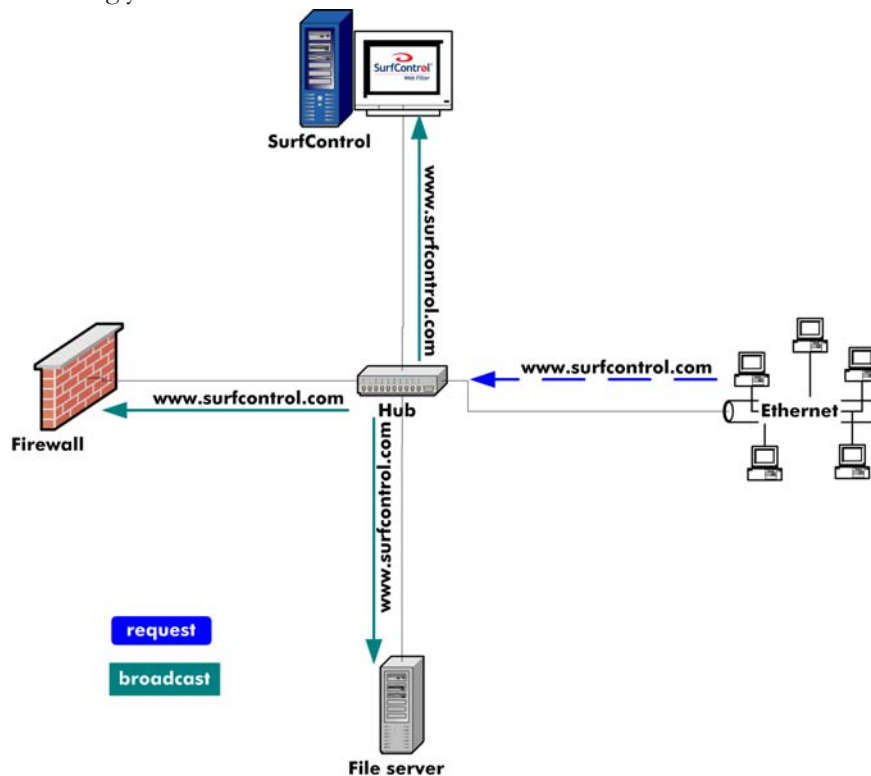


Figure 2-1 Web Filter connected to a hub

Switch

In order for Web Filter to see a request through a switch, span or mirror the port connecting the network to the Internet gateway to Web Filter's port. See Figure 2-2 for an example.

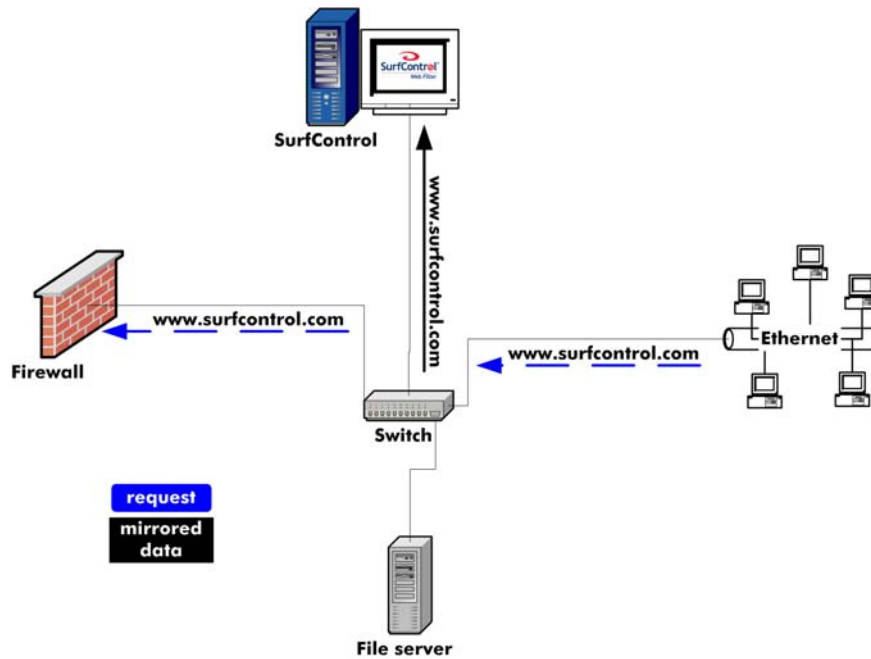


Figure 2-2 Web Filter connected to a Switch

If your switch is uni-directional and does not allow broadcasting and monitoring on the mirrored or spanned port, a second NIC is required. See “Multiple NIC support” on page 12 for more details.

For further information on configuring spanned ports, see 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.



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

Figure 2-3 shows Web Filter deployed in a small network:

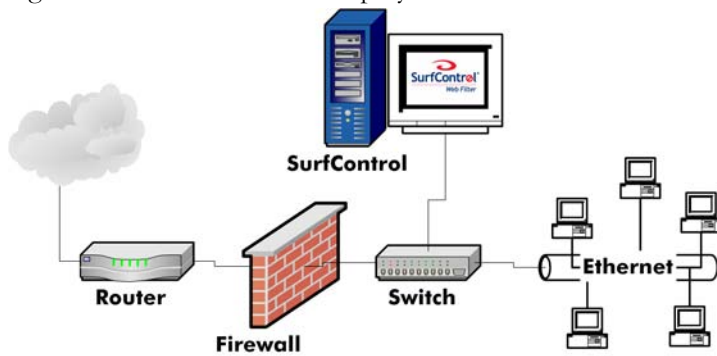


Figure 2-3 Web Filter in a single-segment network

Figure 2-4 shows a single Web Filter deployed in a larger network:

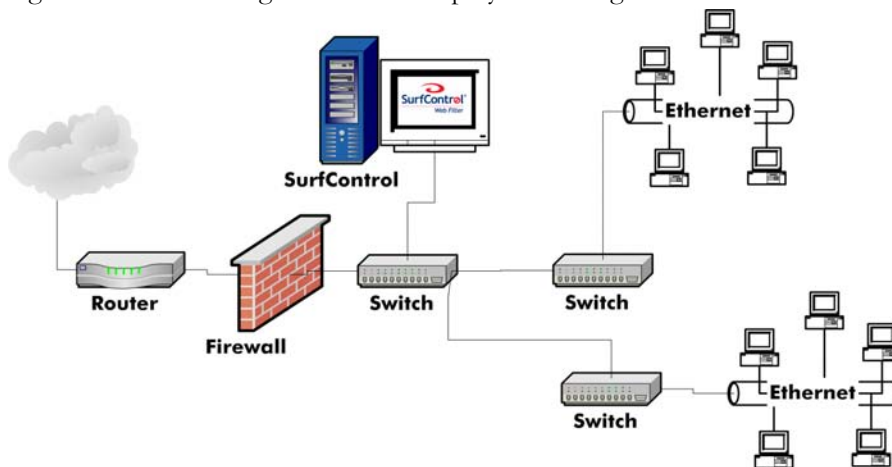


Figure 2-4 Web Filter in a multi-segment network

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 (Figure 2-5) or to install separate Web Filter servers for separate segments of the network (Figure 2-6):

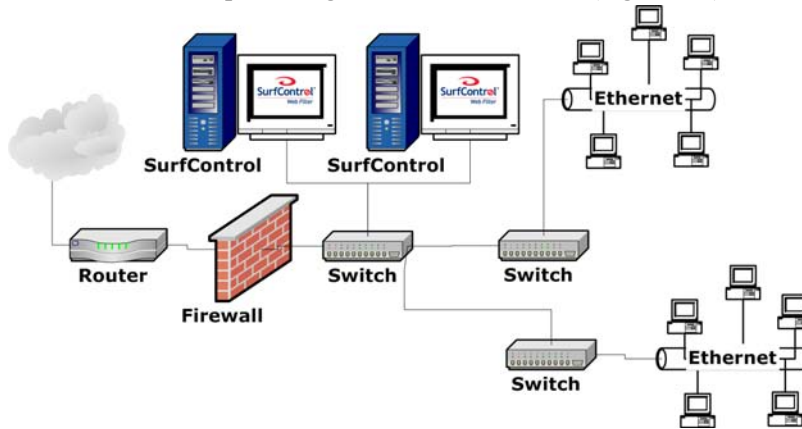


Figure 2-5 Multiple collectors at the firewall

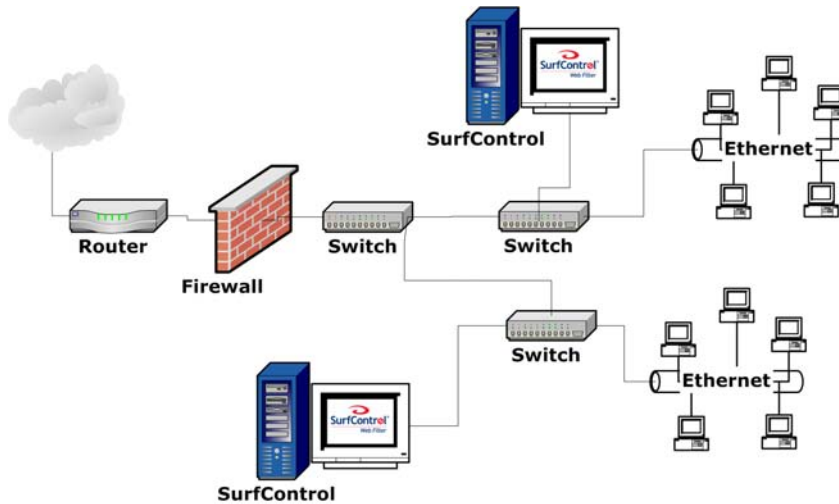


Figure 2-6 Multiple collectors for separate segments

Figure 2-7 shows Web Filter deployed in an enterprise network with multiple Internet gateways:

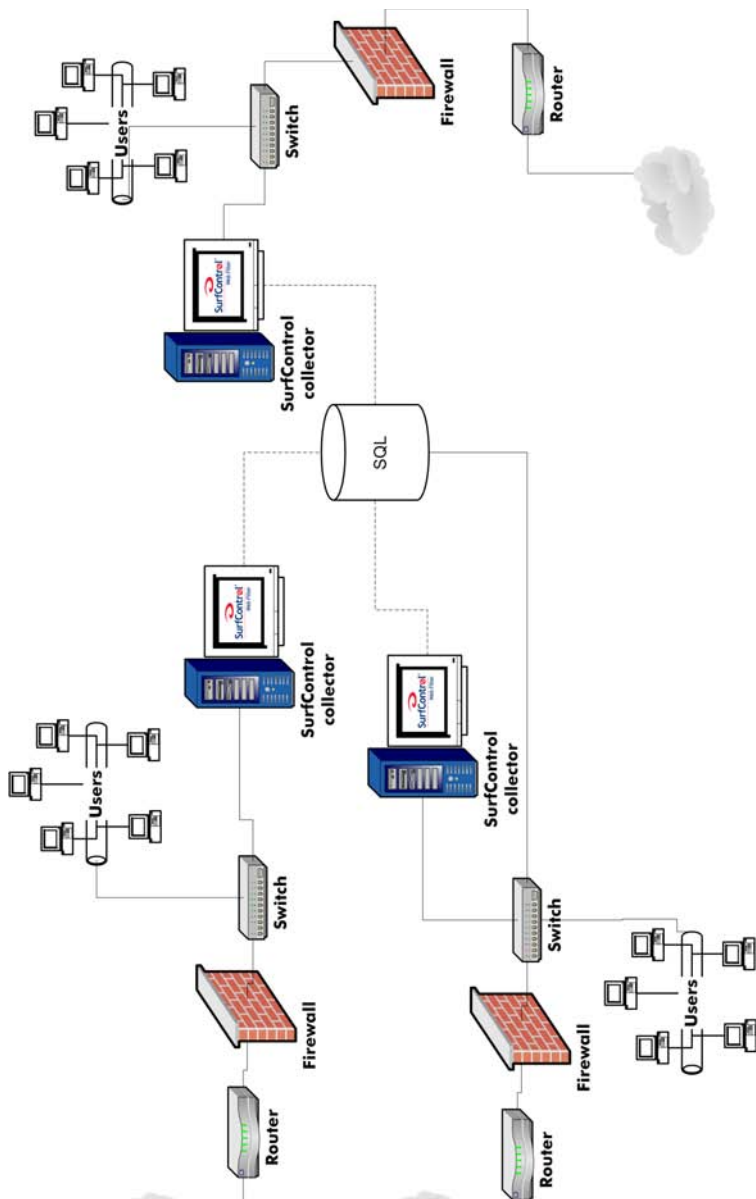


Figure 2-7 Web Filter in an enterprise environment

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. 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 Web Filter 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.

USER NAME RESOLUTION

By default, SurfControl Web Filter doesn't monitor user names. The **Configuration Wizard** gives you the following ways to monitor your users by name:

- By issuing a NetBIOS query based on the MAC address.
- By installing the supplied **Enterprise User Monitor (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 names is more convenient in a workplace where employees share or swap machines frequently.
- Monitoring by user names allows you to filter users based on NT Users and Groups.
- Monitoring by user name makes it easier to track users that frequently logon 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

By accessing Windows NT and Windows 2000/2003 security auditing data to resolve user names, EUM gives Web Filter for NT/2000/2003 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 2 ways:

- 1 By installing an EUM Agent on your domain controllers or Novell NetWare NDS Tree Server.
- 2 By installing an EUM Login Agent on your network that can monitor all users via a login script.



Note: The EUM Login Agent and scripts can not be used in a Novell NetWare environment.

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.

For more details on installing the EUM Agent on your domain controllers, see “The EUM Agent on Domain Controllers” on page 16.

For more details on installing the EUM Login Agent, see “The EUM Login Agent” on page 20.

THE EUM AGENT ON DOMAIN CONTROLLERS

You can install the EUM Agent on Windows 2000/2003 or NT domain controllers. There is also a version of the EUM Agent that works with Novell NetWare.

EUM on Windows 2000/2003 Domain Controllers

The EUM agent installs onto Windows 2000/2003 domain controllers as a dll (ScSubAuth.dll).

When EUM is installed onto a Windows 2000/2003 server, Web Filter uses Microsoft's Sub-Authentication to resolve user names. After installing EUM on a Windows 2000/2003 domain controller, you must restart the domain controller.

EUM on Windows NT Domain Controllers

Web Filter installs the EUM User Agent (UA) onto 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 no longer operate properly.

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 onto an NT domain controller, ensure the trust relationships are set up for multiple domain environments (in this case, Web Filter is Trusted, all other domains are Trusting).

Installing EUM

During installation, Web Filter installs the EUM UA onto 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.
- In order 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 allows 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:

- 1 Add the following key to the SurfControl registry:

HKEY_LOCAL_MACHINE\SOFTWARE\JSB\SurfControlScout\UserAgentPort

- 2 Add the key as a DWORD, specify a decimal value (default is 61695).
 - 3 Stop and start the Web Filter service.
 - 4 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 specify specific user accounts that UA should ignore; you should only use the ignore option for accounts similar to SMS or service accounts (for example, backup.exe, anti-virus updates, servers).



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

NETWAREEUM

Web Filter also provides the ability 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 onto each Novell NDS tree server.



Warning: 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:

- Install NetWare's Client 32 (as Preferred TCP/IP Protocol) onto the server. SurfControl recommend you do this before installing Web Filter.
- Network must be using Novell 5 or 6 over IP.
- The Web Filter server must have a static IP address. 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 55 for more details.
- By default, NetWareEUM uses port 61696 to communicate with the Web Filter server. Perform the following steps to change the port:
 - 1 Add the following key to the registry:
`HKEY_LOCAL_MACHINE\SOFTWARE\JSB\SurfControlScout\NWUserAgentPort`
 - 2 Add the key as a DWORD, specify a decimal value (default is 61696).
 - 3 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 19 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. This holds details of various events. 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 levels are as in Table 2-1. The default logging level is 1:

Table 2-1 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 allows 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 by all users. You then have to perform the following processes to enable the login agent to work.

- 1 Manually configure the `EumLogin.ini` file.
- 2 Create a new log on and log off script, or modify an existing one, to call the `ScEumLoginAgent.exe`.
- 3 Add traffic from the `ScEumLoginAgent` program as an exception to the Windows Firewall that allows the `ScEumLoginAgent` program to operate.

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

[127.0.0.1]
Port=61695

[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

Table 2-2 describes the various sections of the EumLogin.ini file and how to enter your information.

Table 2-2 The EumLogin.ini file sections

Section	What to enter
[Surfcontrol_Servers]	<p>You need to enter the name or IP address of each server Web Filter is installed upon in your organization.</p> <p>The format is:</p> <p>Servers=Servername1,Servername2,127.0.0.1</p> <p>Note: <i>Do not leave spaces between the server names.</i></p>
[SERVERNAME]	<p>For each server specified in [Surfcontrol_Servers], you need to make an entry along with the default Web Filter listening port (61695).</p> <p>The format is:</p> <p>[Servername1] Port=61695</p> <p>[Servername2] Port=61695</p> <p>[127.0.0.1] Port=61695</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 connection to any of the servers specified in [Surfcontrol_Servers] is dropped, the Login Agent will try to re-connect. This entry specifies how many times the agent will attempt to re-connect. If connection is not re-established after the number of times specified, the agent will wait for the interval specified in [Continuous_Mode] 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 Log On and Log Off Script

You need to create a new log on and log off script, or modify an existing one, to call the `ScEumLoginAgent.exe` agent.



Note: A log off script is not required for NT domains.

The following parameters can be used:

`/LOGOUT` - to be used if the agent is called by a log off script. If this parameter is not used, the agent will assume the script is for a log on.

`/NOCONT` - use this parameter 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 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.

Add an Exception to the Windows Firewall

The Windows Firewall will prevent the `ScEumLoginAgent` program from sending traffic to the network. To allow the agent to function requires either the user to allow access via a prompt, or an Active Directory group policy will need to be created or updated that adds the traffic from the program 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 begin installing Web Filter, you should decide:

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

SurfControl Web Filter uses SQL Server Express, or a fully-licensed version of SQL Server 2000 or 2005. If you plan to use either platform, ensure the software is installed and running before attempting to install Web Filter.

Your choice of platform will not affect how well Web Filter performs, but using SQL Server rather than SQL Server Express allows more flexibility and the ability to fine-tune database performance. It is also more suitable for environments with heavy Web traffic.

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 DSNs. Therefore, any Web Filter client or server on the network can access the database without creating a link through the ODBC driver.

SQL SERVER EXPRESS

If you are not using SQL Server, you need to install SQL Server Express. SurfControl recommends you install your database platform before installing Web Filter.

Using SQL Server Express

If you want to use SQL Server Express, be aware of the following:

- You must install **.NET Framework 2.0** before installing SQL Server Express.
- If installing on a **Windows 2000** computer, you must install **Windows Installer 3.1** before installing SQL Server Express.
- You must install SQL Server Express as a **Default Instance** when prompted during installation.
- You must install the **Database and Connectivity Components** when prompted during installation.
- You must perform the steps outlined in Procedure 2-1 before installing Web Filter.
- By default, SQL Server Express runs as a Network Service. When performing a database archive or restore, it needs to run with a local admin account to be able to access drive c.
- Microsoft specifies that the maximum size for a SQL Server Express database is **4 GB**.

You can use the Windows OSQL utility from the command prompt to access data tables. For more details about the OSQL utility, visit www.microsoft.com.

For more information on SQL Server Express, visit:

<http://www.microsoft.com/sql/editions/express/default.msp>

Procedure 2-1: Post SQL Server Express Installation Configuration**Step Action**

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>. This explains the steps in more detail.

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

SQL SERVER

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



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

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

Install SQL Server on the designated server; this can be the same machine as the Web Filter server.



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

- 1 Make sure your server has the minimum resources listed in Table 2-3.

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

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

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

Reasons to Install SQL Server on a Dedicated Server

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

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

Considerations for large environments

Make sure your dedicated SQL Server has the minimum resources listed in Table 2-4:

Table 2-4 SQL Server minimum requirements for large environments

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

DATABASE AUTHENTICATION

Web Filter supports both Windows authentication and SQL authentication.

SurfControl recommends Windows authentication due to ease of use. With SQL authentication if a password is changed, any configured connections would have to be re-established. With Windows authentication they would still work. This is also in line with Microsoft's security recommendations.

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.

OTHER CONSIDERATIONS

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

CONTENT

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 19 million destinations, including more than 3 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 us 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.

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.
- Set up scheduled events.

You can also install the SurfControl Mobile Filter Administrator.

Before installation, make sure the Remote Administration client computer meets the minimum requirements listed in Table 2-5:

Table 2-5 Remote Administration Client minimum requirements

	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 XP Windows Server 2003 Standard Edition Windows Server 2003 Enterprise Edition	
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, laws have been passed forbidding users browsing details to be seen by monitoring software without express permission from a manager and a union representative. The Privacy Edition of SurfControl Web Filter allows 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*.



Chapter 3

Installation order

Introduction	page 32
Installation Procedures	page 33
Changes to the Server	page 34
Installing SQL Server Express (optional)	page 34
Installing SurfControl Web Filter	page 35

INTRODUCTION

This chapter explains how to install SurfControl Web Filter. There are six stages to the installation process.

Table 3-1 Installation Workflow

Stage	Description
Database platform preparation	If you have chosen SQL Server Express for your database platform, download and install it from the Microsoft Web site. See Procedure 3-1 on page 34.
Product preparation	If you plan to monitor NetWare user names , install the NetWare client onto 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. • Installing the EUM Login Agent on your network and editing the supplied configuration file.
	If you plan to monitor Netware user names, install NetwareEUM onto all NDS servers.
Report Central	Download and install SurfControl Report Central from www.surfcontrol.com .

INSTALLATION PROCEDURES


This section contains the following procedures:

- 1 Installing SQL Server Express (optional) - Procedure 3-1.
- 2 Installing Web Filter - Procedure 3-2.


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 install again at a later date.

CHANGES TO THE SERVER

Installing Web Filter makes the following changes to your server:

- Places an icon in the Notification Area at startup .

From this icon, you can start and stop the Web Filter and Scheduler services and configure the Web Filter service settings. You can also serialize the product from the About dialog box.


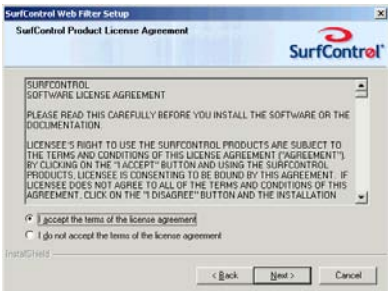
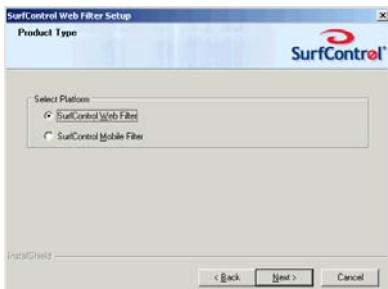

If the Web Filter Service has been stopped the icon is grayed out .

In a Web Filter Administration client installation the gray icon is placed in the Notification Area, to indicate that the service is not running locally.
- Adds necessary registry entries.
- Creates the SurfControl_WebFilter database.
- Adds the following services:
 - Web Filter service
 - Scheduler service
 - Remote Administration service
 - Audit Logger service
 - Virtual Control Agent service (license-holders only)
 - Corporate Network Detection Service (CNDS)



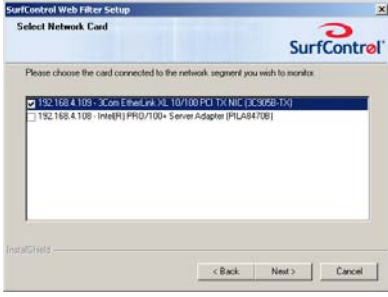
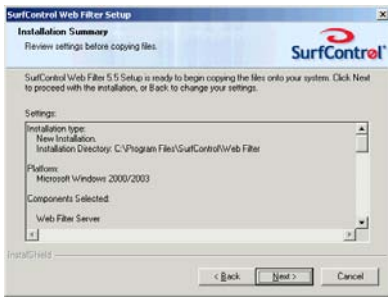
Procedure 3-1: Installing SQL Server Express (optional)

Step	Action
1	If you plan to use SQL Server Express for your database, you must install it in the following order before installing Web Filter.
2	Download and install .NET Framework 2.0 from http://msdn.microsoft.com/netframework/ 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.mspx <i>Note: You must install the Database and Connectivity Components when prompted during installation.</i>
4	Perform Post SQL Server Express Installation Configuration as described on page 24.
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.
6	You will need to restart the server before installing SurfControl Web Filter.

Procedure 3-2: Installing SurfControl Web Filter

Step	Action	
1	Locate the SurfControl Web Filter executable file (setup . exe).	
2	Double-click setup . exe to start the installation process.	
3	The Welcome screen is displayed. Click Next .	
4	The License Agreement screen is displayed. Select I accept the terms of the license agreement . Click Next .	
5	The Product Type screen is displayed. Select SurfControl Web Filter . Click Next .	
6	The Important Installation Information screen is displayed. Prior to starting the installation, you should have determined the appropriate network configuration for Web Filter. Click Next .	

Procedure 3-2: Installing SurfControl Web Filter

Step	Action	
7	<p>If the setup program does not detect a suitable database, the Select Database Installation Options screen is displayed. You can either:</p> <ul style="list-style-type: none"> 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. <p>If you have already installed SQL Server Express or SQL Server, this screen will not display.</p> <p>Click Next.</p>	
8	<p>The Setup Type screen is displayed.</p> <p>Select Complete Product.</p> <p>The setup program installs Web Filter to a default path of c:\program files\SurfControl\Web Filter. If you want to install Web Filter in a different location on the server, click Browse to choose a new path.</p> <p>Click Next.</p>	
9	<p>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 and will monitor Internet traffic.</p> <p>Click Next.</p>	
10	<p>The Installation Summary screen is displayed.</p> <p>Review your settings before starting the installation. When you are ready, click Next to begin copying the Web Filter files.</p>	

Procedure 3-2: Installing SurfControl Web Filter

Step	Action	
11	you have successfully installed Web Filter. Click Finish . The Configuration Wizard will start automatically. See "Configuration Wizard" on page 41 for more details.	 A screenshot of the SurfControl Web Filter Setup wizard. The window title is "SurfControl Web Filter Setup". The main content area displays the SurfControl logo and the text "InstallShield Wizard Complete". Below this, it says "Setup has finished installing SurfControl Web Filter on your computer." At the bottom of the window, there are three buttons: "Back", "Finish", and "Cancel".

3

INSTALLATION ORDER *Introduction*



Chapter 4

Configuring Web Filter

Introduction

page 40

Configuration Wizard

page 41

Post Installation Tasks

page 49

Introduction



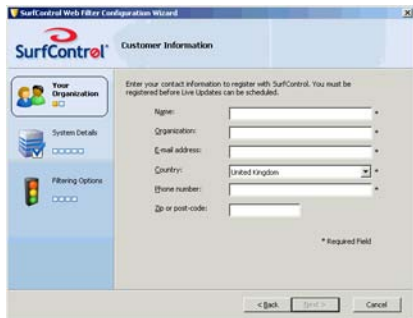
This chapter explains how to use the Configuration Wizard.

The Configuration Wizard helps you configure Web Filter quickly and easily so that you can protect your system against Internet threats as quickly as possible.



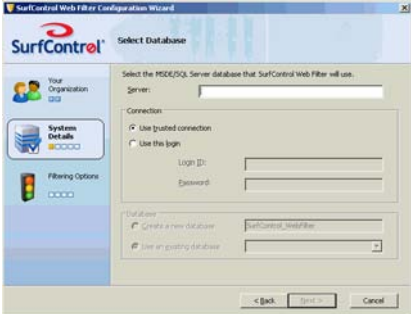
Configuration Wizard

The wizard will launch after you have finished the complete installation process on your Web Filter server. Follow Procedure 4-1.

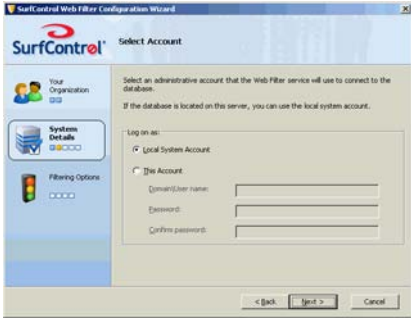


Procedure 4-1: Using the Configuration Wizard

Step	Action	
1	As soon as the setup program is complete, the Configuration Wizard will start. Click Next .	
2	The Your Organization screen is displayed. This 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. Click Next .	



Procedure 4-1: Using the Configuration Wizard

Step	Action	
4	<p>The Licensing screen is displayed.</p> <p>If you are an evaluating customer, select I am evaluating SurfControl Web Filter. Click Next.</p> <p>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.</p>	
5	<p>The System Details screen is displayed.</p> <p>This screen outlines the information you will enter in this section.</p> <p>Click Next.</p>	
6	<p>The Select Database screen is displayed. Fill in the fields as follows:</p> <p>Server: enter the name or IP address of the server where your SQL Server Express or SQL Server database is located.</p> <p>Connection: specify how you want Web Filter to connect to the database. Web filter can either log in using your database's SA username and password, or using a trusted connection.</p> <p>Database: specify whether you want to use an existing Web Filter database, or create a new one.</p> <p>Click Next.</p>	




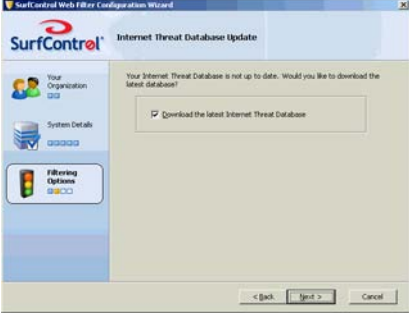
Procedure 4-1: Using the Configuration Wizard

Step	Action	
7	<p>The Select Account screen is displayed.</p> <p>You need to choose how Web Filter will log on to your database.</p> <p>If your database is located on the same server as Web Filter, you can select Use Local System Account.</p> <p>If your database is hosted remotely on another server, you need to select This Account.</p> <p>You need to enter the Domain and User name, with the corresponding Password for that user.</p> <p>Click Next.</p>	
8	<p>The Privacy Options screen is displayed.</p> <p>Note: <i>This screen will not appear if you selected an existing database in Step 7.</i></p> <p>If you need to hide user information to comply with regional legislation, select Hide user identifiable information.</p> <p>Click Next.</p>	
9	<p>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. Web Filter will attempt a secure connection when you click Next.</p>	


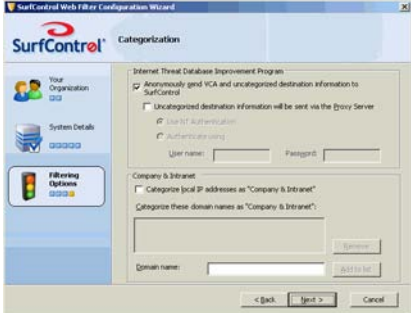
Procedure 4-1: Using the Configuration Wizard

Step	Action	
10	<p>The Corporate Network Detection Service Configuration screen is displayed.</p> <p>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 device from the Mobile Filter client. This service must be installed on the Web Filter server. If you don't plan to install Mobile Filter, select Disable Corporate Network Detection Service (the default option).</p> <p>If you are installing Mobile Filter, you can select Enable Corporate Network Detection Service.</p> <p>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.</p> <p>For more information on this service, consult the SurfControl Mobile Filter <i>Installation Guide</i>.</p> <p>Click Next.</p>	
11	<p>The Subnets screen is displayed. You can reduce the load on a single Web Filter server, or balance the load on multiple Web Filter servers.</p> <p>Single server</p> <p>Identify any external traffic subnets (intranet Web servers for example). Click Add and enter the IP address and subnet mask.</p> <p>Select Do not monitor traffic to or from these subnets.</p> <p>Multiple Servers</p> <p>Identify one server and set up as a single server. For subsequent servers, identify the subnets you DO want to monitor. Click Add and enter the relevant IP addresses and subnet masks.</p> <p>For these subnets, select Only monitor traffic to or from these subnets.</p> <p>Note: <i>These settings can be changed from the Subnets tab in the Web Filter Service Settings following installation.</i></p> <p>Click Next.</p>	

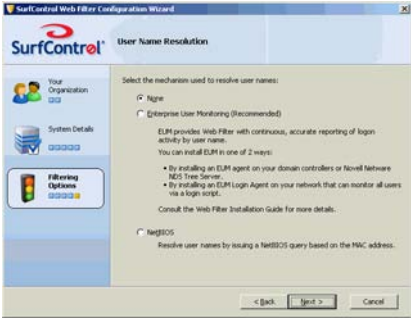
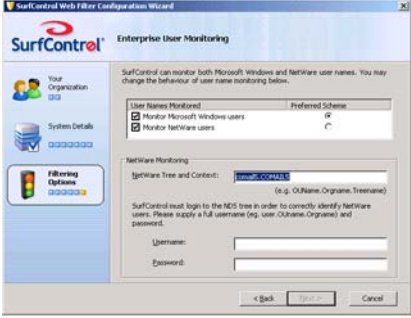
Procedure 4-1: Using the Configuration Wizard

Step	Action	
12	<p>The Internal Traffic screen is displayed.</p> <p>Web Filter detects the internal subnets on your monitoring and blocking network card (NIC).</p> <p>The Web Filter server ignores inbound traffic to these internal subnets, reducing the load on the Web Filter.</p> <p>Click Add if you wish to add further internal subnets.</p> <p>You can also Remove or Edit the subnets detected by Web Filter.</p> <p>Click Next.</p>	
13	<p>The Filtering Options screen is displayed.</p> <p>This screen outlines the information you will enter in this section.</p> <p>Click Next.</p>	
14	<p>The Automatic Database Management screen is displayed.</p> <p>To purge the Web Filter database automatically once a month, select;</p> <p>Archive and purge monitored traffic database once a month.</p> <p>Click Next.</p>	
15	<p>The Internet Threat Database Update screen is displayed.</p> <p>For maximum protection you need the latest threat information. Select Download the latest Internet Threat Database.</p> <p>Click Next.</p>	






Procedure 4-1: Using the Configuration Wizard

Step	Action	
16	<p>The E-mail Notifications screen is displayed.</p> <p>Web Filter can notify the systems administrator when system events occur. Fill in the fields as follows:</p> <p>E-mail Server: enter the name or IP address of the e-mail server for your domain. Web Filter will use this e-mail server to send notifications.</p> <p>Recipient address: enter the e-mail address of the systems administrator.</p> <p>From address: enter the address that the notification e-mails will be sent from.</p> <p>Now specify which Message Types you want to be notified of. Choose any or all of the following:</p> <ul style="list-style-type: none"> • Service running status changes • Internet Threat Database license reminders • Scheduled task failures • Catch up mode notifications <p>When you have made your choices, click Next.</p>	
17	<p>The Categorization screen is displayed.</p> <p>When Web Filter encounters an uncategorized Web destination, it can send the details anonymously to SurfControl. This helps to improve the effectiveness of the Internet Threat Database for future updates.</p> <p>Clear the Anonymously send VCA and uncategorized destination information to SurfControl check box to opt out of sending this information.</p> <p>If you access the Internet via a proxy server, you can set the authentication for sending information via this method.</p> <p>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.</p> <p>Click Add to add your domain (without entering the http://www prefix).</p> <p>Click Next.</p>	

Procedure 4-1: Using the Configuration Wizard

Step	Action	
18	<p>The User Name Resolution screen is displayed. By default, no User Name Resolution is selected. You have the following choices:</p> <ul style="list-style-type: none"> Enterprise User Monitoring (recommended) NetBIOS <p>Note: <i>You can change the way you resolve user names following installation from the Web Filter Settings in the Enterprise Manager > Maintenance options.</i></p> <p>Click Next.</p>	
19	<p>If you are installing on a Novell NetWare environment, and selected Enterprise User Monitoring in step 17, the Enterprise User Management screen is displayed. You have the following options:</p> <ul style="list-style-type: none"> User Names Monitored - you can monitor by either Windows or NetWare users, or both (the default). You can also select which is your preferred scheme. 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. <p>Note: <i>If you select not to monitor users by EUM in step 17, this screen will not be displayed. You can select to monitor by EUM and enter these details from the User Name Resolution tab in the Web Filter Settings following installation. See Chapter 9 of the Administrator's Guide for more details.</i></p> <p>Click Next.</p>	

Procedure 4-1: Using the Configuration Wizard

Step	Action	
20	<p>The Ready to Configure screen is displayed.</p> <p>In the box you can see a list of the tasks that the Configuration Wizard will do to configure Web Filter.</p> <p>Click Start.</p>	
21	<p>The Configuring screen is displayed.</p> <p>A blue arrow shows the task currently in progress. As each task is completed, you will see a green check.</p> <p>If there is a problem with a task, you will see a warning icon  next to it.</p> <p>You can either go Back to change your settings, or Skip the task and move on to the next one.</p> <p>If there is a serious problem, you will see the  icon. If this happens, the Skip button will be disabled and you must go back to correct your settings.</p> <p>Note: <i>If you skip a task, Web Filter may not filter traffic effectively.</i></p>	
22	<p>The Configuration Complete screen is displayed.</p> <p>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.</p> <p>Click Finish.</p> <p>Web Filter is now ready to start protecting your system from Internet Threats.</p>	

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**. See page 50 for more details.
- Install **SurfControl Report Central**. See page 56 for more details.

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 on how EUM works, see “User Name Resolution” on page 14.



You can install EUM in the following ways:

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

INSTALLING THE EUM AGENT ON DOMAIN CONTROLLERS

Procedure 4-2: Installing EUM on Domain Controllers		
Step	Action	
1	Make sure that the Web Filter server has a static IP address.	
2	Make sure you have administrative privileges on all domain controllers where the User Agent will be installed.	
3	Make sure the Web Filter server is located in the correct domain.	
4	Make sure the firewall or router allows traffic through the provisioned port (default is 61695).	
5	For Windows NT domain controllers, make sure the security logs of the domain controllers are set to overwrite events, as needed.	
6	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.	
7	From the Start menu, launch EUM installation (Start > Programs > SurfControl Web Filter > Enterprise User Monitoring > Install Enterprise User Monitoring).	
8	The SurfControl Enterprise User Monitoring Installation screen is displayed. Click Next .	
9	The Hostname screen is displayed. Enter the IP address of the Web Filter server. Note: <i>SurfControl recommends entering the IP address instead of the hostname.</i> Enter the port the User Agent and the Web Filter service should use to communicate (the default is 61695). Click Next .	
10	The Domain List screen is displayed. Select the domains you want to receive user data from. Click Next .	

Procedure 4-2: Installing EUM on Domain Controllers

Step	Action	
11	<p>The Ignore User Accounts screen is displayed.</p> <p>Select the user accounts whose logons/logoffs do not need to be reported, for example, Systems Management Server (SMS) and antivirus accounts.</p> <p>Click Next.</p>	
12	<p>The Select Domain Controllers screen is displayed.</p> <p>Select the domain controllers whose user's logon and logoff activity Web Filter needs to monitor (this identifies the domain controllers where the UA will be installed).</p> <p>Note: <i>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.</i></p> <p>Click Next.</p>	
13	<p>Installation onto Microsoft Windows 2000 domain controllers requires a restart; SurfControl recommends performing a manual restart.</p>	
14	<p>You have successfully installed Enterprise User Monitoring.</p>	

INSTALLING THE EUM LOGIN AGENT ON YOUR NETWORK

Procedure 4-3: Installing the EUM Login Agent on your Network

Step	Action
1	The Login Agent program and configuration file can be found in the following location in a default install: <code>C:\Program Files\SurfControl\Web Filter\EnterpriseUserMonitoring\LoginAgent</code>
2	Copy the Login Agent program (<code>ScEumLoginAgent.exe</code>) and configuration file (<code>EumLogin.ini</code>) to a folder on your network that is accessible by all users.
3	Edit the configuration file (<code>EumLogin.ini</code>). For details on the settings, see "How to Configure the File" on page 21.
4	Create or edit an existing log on and log off script to call the <code>ScEumLoginAgent.exe</code> program. The following parameters can be used: /LOGOUT - to be used if the agent is called by a log off script. If this parameter is not used, the agent will assume the script is for a log on. /NOCONT - use this parameter 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. /TRACEMODE - use this parameter if you are experiencing problems with the agent. Trace messages will be stored in a log file called <code>EumLoginTrace.log</code> . This file will be stored in the logged on user's temporary folder. The location of this folder is determined by the following: <ul style="list-style-type: none"> • 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.
5	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 for more details.

INSTALLING NETWARE EUM

Procedure 4-4: Installing EUM on NetWare

Step	Action
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). Note: <i>When creating the directory, use DOS 8.3 naming conventions.</i>
4	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.
5	From the NetWare Server console, load the NLM by entering: <pre>Load sys:\nweum\nweum.nlm</pre> and pressing enter Note: <i>The system will not allow you to load the NLM if a copy is already running.</i>

Procedure 4-5: Automatically loading the NetWare EUM

Step	Action
1	To automatically load the NetWare EUM every time the server is restarted edit the <code>sys:\system\autoexec.ncf</code> file.
2	You can edit this file using any text editor from the workstation or from the NetWare Server by typing: <pre>Load edit sys:\system\autoexec.ncf</pre>
3	Add the following line at the end of the file: <pre>load sys:\nweum\nweum.nlm</pre>
4	Save the file.

Procedure 4-6: Unloading the NetWare EUM

Step	Action
1	From the NetWare Server console, type: <pre>unload nweum.nlm</pre>

Procedure 4-7: Add Web Filter Servers to NetWare EUM

Step	Action
1	Unload the NetWare EUM as in Procedure 4-6.
2	Add the following details to the <code>surfcontrol_services</code> section of the <code>scua.ini</code> file The format should be: <code>machine_name_or_IP_Address=Port number</code> Note: <i>the default port number is 61696. 61695 is used by Win 2000/2003 EUM architecture.</i>
3	Save the <code>scua.ini</code> file.
4	Re-load the NetWare EUM as in Procedure 4-5.

Procedure 4-8: Ignored users in NetWare EUM

Step	Action
1	Unload the NetWare EUM as in Procedure 4-6.
2	Edit the [Ignored Users] section of the <code>scua.ini</code> file. The format for adding ignored users is as follows: <code>unique_user_key=fully_qualified_username_in_the_NDS_tree</code> For example: <code>user1=admin.NW_5_1_SURF</code> <code>user2=tester.accounting.NW_5_1_SURF</code>
3	Save the <code>scua.ini</code> file.
4	Re-load the NetWare EUM as in Procedure 4-5.



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.

Procedure 4-9: NIC Configuration

Step	Action	
Single NIC configuration		
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). Note: <i>The properties of the SurfControl Network Protocol Device Driver will only be available on those servers that have:</i> <ul style="list-style-type: none"> - 2 or more NICs - and the driver 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. Click OK .	
6	Click OK again to close the NIC Properties dialog box.	

Procedure 4-9: NIC Configuration

Step	Action
Configure multiple NICs to monitor and block	
7	Select Properties for the Monitoring NIC (this is the NIC you bound to the Web Filter service during installation).
8	Clear all items (including Internet Protocol (TCP/IP)), except the SurfControl Network Protocol Device Driver .
9	Select Properties for the SurfControl Network Protocol Device Driver .
10	Make sure Monitor this adapter is selected; this indicates that this NIC is responsible for monitoring.
11	Make sure Redirect blocking packets to is selected and choose the blocking NIC from the drop-down list box. Click OK to continue.
12	Click OK again to continue.
13	Select Properties for the Blocking NIC.
14	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.
15	Select Properties for the SurfControl Network Protocol Device Driver .
16	Make sure Monitor this adaptor is not selected. Make sure Redirect blocking packets to is not selected.
17	Click OK .


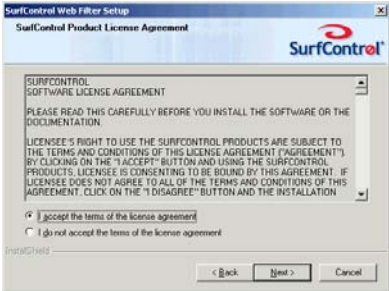


Installing the Remote Administration Client


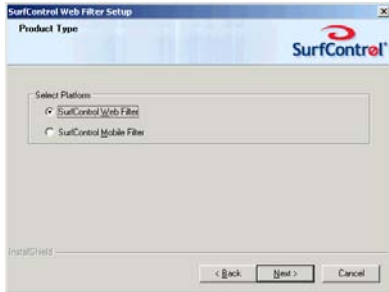

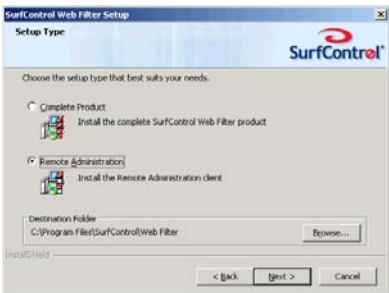
From the Remote Administration Client installation you can:

- 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.
- Set up scheduled events.

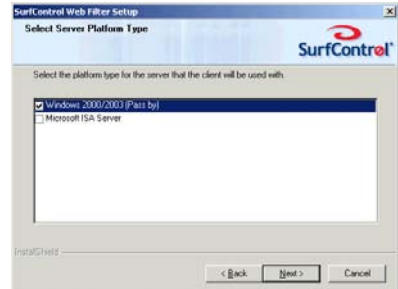
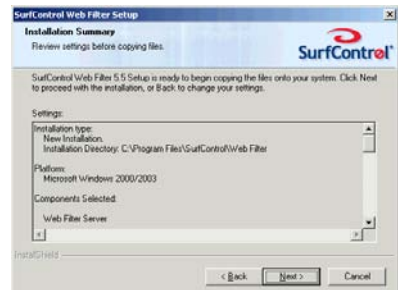

Procedure 4-10: Installing the Remote Administration Client

Step	Action	
1	Locate the downloaded SurfControl Web Filter file (<code>setup.exe</code>).	
2	Double-click <code>setup.exe</code> to start the installation process.	
3	The InstallShield Wizard loads.	
4	The SurfControl Web Filter Setup screen is displayed. Click Next .	
5	The License Agreement screen is displayed. Select I accept the terms of the license agreement . Click Next .	

Procedure 4-10: Installing the Remote Administration Client

Step	Action	
6	The Select Database Installation Options screen is displayed. Select Web Filter Remote Administration .	
7	The Product Type screen is displayed. Select SurfControl Web Filter. Click Next .	
8	The Important Installation Information screen is displayed. Click Next .	
9	The Setup Type screen is displayed. Select Remote Administration . Click Next .	

Procedure 4-10: Installing the Remote Administration Client

Step	Action	
10	The Select Server Platform Type screen is displayed. Select Windows 2000/2003 (Pass By). Click Next .	
11	The Installation Summary screen is displayed. Review your settings before starting the installation. Click Next .	
12	The InstallShield Wizard Complete screen is displayed. Click Finish .	
13	You have successfully installed the SurfControl Web Filter Remote Administration . The Configuration Wizard will start automatically. Note: <i>The Configuration Wizard for the Remote Administration is a subset of the Complete Product version.</i>	