


The logo features a red swoosh above the word "Enterprise" in a bold, white, sans-serif font. Below "Enterprise" is the phrase "Threat Shield" in a smaller, white, sans-serif font.

Enterprise Threat Shield

Version 4.0

SurfControl Enterprise Threat Shield *Administrator's Guide*

The background of the lower half of the cover is a blue-tinted image of a globe with a grid overlay, set against a sky with light rays.

Enterprise Threat Protection™

NOTICES

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

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 and/or additional marks herein are registered trademarks of SurfControl plc. and/or its affiliates in the US and/or other countries. All other registered and unregistered trademarks herein are the sole property of their respective owners.

©2007 SurfControl, Inc. All rights reserved.

Version 4.0

The BSD License

Copyright (c) 1998 - 2002, Paul Johnston & Contributors

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 author 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 product includes software developed by The Apache Software Foundation: <http://www.apache.com>

This product contains the Dynamic Child Window Repositioning Framework by Hans Bühler, obtained from www.codeguru.com.

Copyright (c) 1998-2006 The OpenSSL Project. All rights reserved.

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. 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.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY EXPRESSED 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 OpenSSL PROJECT OR ITS 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 product includes cryptographic software written by Eric Young(eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

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

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. 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.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``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 AUTHOR 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.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE."

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2007, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved. Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

Copyright (C) 1998-2003 Daniel Veillard. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE DANIEL VEILLARD BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of Daniel Veillard shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from him.

Copyright (c) 1996-2001 - Rosimildo da Silva

(C) Copyright Greg Colvin and Beman Dawes 1998, 1999.

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING

FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This file includes copyrights by Rik Hemsley, The Leland Stanford Junior University, University of Washington, and Samuel R. Blackburn.

The file contains the following copyright and usage terms.

// The copyright notice below refers to the original base 64 code.

// Some modifications are Copyright (C) 1998, 1999 Rik Hemsley rik@kde.org

/*

* Original version Copyright 1988 by The Leland Stanford Junior University

* Copyright 1998 by the University of Washington

*

* Permission to use, copy, modify, and distribute this software and its

* documentation for any purpose and without fee is hereby granted,

* provided that the above copyright notices appear in all copies and that

* both the above copyright notices and this permission notice appear in

* supporting documentation, and that the name of the University of

* Washington or The Leland Stanford Junior University not be used in

* advertising or publicity pertaining to distribution of the software

* without specific, written prior permission. This software is made

* available "as is", and THE UNIVERSITY OF WASHINGTON AND THE LELAND

* STANFORD JUNIOR UNIVERSITY DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED,

* WITH REGARD TO THIS SOFTWARE, INCLUDING WITHOUT LIMITATION ALL IMPLIED

* WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND

* IN NO EVENT SHALL THE UNIVERSITY OF WASHINGTON OR THE LELAND STANFORD

* JUNIOR UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL

* DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR

* PROFITS, WHETHER IN AN ACTION OF CONTRACT, TORT (INCLUDING NEGLIGENCE)

* OR STRICT LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR

* PERFORMANCE OF THIS SOFTWARE.

*

*/

This file includes copyrights by Rik Hemsley, The Leland Stanford Junior University, University of Washington, and Samuel R. Blackburn.

The file contains the following copyright and usage terms.

// The copyright notice below refers to the original base 64 code.

// Some modifications are Copyright (C) 1998, 1999 Rik Hemsley rik@kde.org

/*

* Original version Copyright 1988 by The Leland Stanford Junior University

* Copyright 1998 by the University of Washington

*
* Permission to use, copy, modify, and distribute this software and its
* documentation for any purpose and without fee is hereby granted,
* provided that the above copyright notices appear in all copies and that
* both the above copyright notices and this permission notice appear in
* supporting documentation, and that the name of the University of
* Washington or The Leland Stanford Junior University not be used in
* advertising or publicity pertaining to distribution of the software
* without specific, written prior permission. This software is made
* available "as is", and THE UNIVERSITY OF WASHINGTON AND THE LELAND
* STANFORD JUNIOR UNIVERSITY DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED,
* WITH REGARD TO THIS SOFTWARE, INCLUDING WITHOUT LIMITATION ALL IMPLIED
* WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND
* IN NO EVENT SHALL THE UNIVERSITY OF WASHINGTON OR THE LELAND STANFORD
* JUNIOR UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL
* DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR
* PROFITS, WHETHER IN AN ACTION OF CONTRACT, TORT (INCLUDING NEGLIGENCE)
* OR STRICT LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
* PERFORMANCE OF THIS SOFTWARE.

*

*/

Note the following block referring to resale of WFC code.

/*

** Author: Samuel R. Blackburn

** Internet: wfc@pobox.com

**

** You can use it any way you like as long as you don't try to sell it.

**

** Any attempt to sell WFC in source code form must have the permission

** of the original author. You can produce commercial executables with

** WFC but you can't sell WFC.

**

** Copyright, 2000, Samuel R. Blackburn

**

** \$Workfile: soap_parameter2.cpp \$

** \$Revision: 1.1 \$

** \$Modtime: 11/09/01 7:45 \$

** \$Reuse Tracing Code: 1 \$

*/


```
#
# This file is part of the Abyss library
#
# Redistribution and use in source and binary forms, with or without
# modification, are permitted provided that the following conditions
# are met:
# 1. Redistributions of source code must retain the above copyright
# notice, this list of conditions and the following disclaimer.
# 2. 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.
# 3. The name of the author may not be used to endorse or promote products
# derived from this software without specific prior written permission.
#
# THIS SOFTWARE IS PROVIDED BY THE AUTHOR 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 AUTHOR 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.
```

*****/

The following copyright text and usage terms are in the file.

/*

* Sun RPC is a product of Sun Microsystems, Inc. and is provided for
* unrestricted use provided that this legend is included on all tape
* media and as a part of the software program in whole or part. Users
* may copy or modify Sun RPC without charge, but are not authorized
* to license or distribute it to anyone else except as part of a product
* or program developed by the user.

*

* SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE
* WARRANTIES OF DESIGN, MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

*

* Sun RPC is provided with no support and without any obligation on the

* part of Sun Microsystems, Inc. to assist in its use, correction,
* modification or enhancement.
*
* SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE
* INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC
* OR ANY PART THEREOF.
*
* In no event will Sun Microsystems, Inc. be liable for any lost revenue
* or profits or other special, indirect and consequential damages, even if
* Sun has been advised of the possibility of such damages.
*
* Sun Microsystems, Inc.
* 2550 Garcia Avenue
* Mountain View, California 94043
*/
/*
* Generic DES driver interface
* Keep this file hardware independent!
* Copyright (c) 1986 by Sun Microsystems, Inc.
*/

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1995-2006 International Business Machines Corporation and others

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

CONTENTS

Notices	i
THREAT SHIELD MANAGER	1
Overview	3
Terminology used	3
What can be configured within the Threat Shield Manager?	4
The Threat Shield Manager Interface	5
Launching the Manager	5
File Menu	6
Apply Rules	6
Open Threat Shield Reporter	6
Update software	6
Exit	6
View Menu	7
Rule Objects tree	7
Rules table	7
Rule Menu	8
New	8
Delete	8
Raise rule priority	8
Lower rule priority	8
Tools Menu	9
Workstation activity	9
Workstation Deployment and Status	9
Activating the Deployment Process	11
Stand Alone mode	12
Change Account Information	13
Settings	13
Help	21
Detection Technologies	22
The Threat Shield Toolbar	23
Key Points	24
THREAT SHIELD OBJECTS	25
Overview	26
Terminology used	26
What can be configured in these panes?	26
Creating a policy	27
Who	28
Adding Who objects	28
Configuring Who objects	29
Content	30
Signature Databases	30
Adding a Content object	31
Configuring Content objects	31
The Threat Shield DB Editor	33
Sending an item to SurfControl	34
Updating SurfControl-supplied Databases	34

FileWatch	39
Adding a FileWatch object	39
Configuring FileWatch objects	40
FileWatch and removable devices	43
WriteWatch	44
Adding WriteWatch objects.....	44
Configuring WriteWatch objects.....	45
Removable Drive Data Loss Protection	46
.exeWatch	48
Adding .exeWatch objects	48
Configuring .exeWatch objects	49
Defining Message Formats	51
BrowseWatch	54
Adding BrowseWatch objects	55
Configuring BrowseWatch objects	55
Exclusions	56
Adding Exclusions objects	56
Configuring Exclusions objects	57
Excluding Files, Directories and Web sites	57
Key Points	59

CREATING AND USING RULES 61

Overview	62
Terminology used	62
The Rules Section	63
Default Rules	63
Creating Custom Rules	66
The Rules Table.....	66
Designing a rule	66
Putting the rule together.....	67
Rule priority.....	67
Managing rules	68
Enable or disable a rule	68
Rename a rule	68
Change a Rule's Priority	68
Change a rules configuration	69
Delete a rule.....	69
Key Points	70

THREAT SHIELD REPORTER 71

Overview	72
Terminology used	72
What can the Reporter be used for?	72
Launching the Threat Shield Reporter	73
Using Threat Shield Reporter	74
Creating a Quick Report	75
Access Rights	76
Report Types	76
Configuring Report Parameters	78
Creating a New Report	80
Modifying Report Parameters	81

Key points	82
TROUBLESHOOTING	83
Existing AV and AS products blocking the Agent	84
Client based firewalls	85
MS File and Printer Sharing	86
APPENDIX	87
A - Using Group Policy	88
Before you start.....	88
Step 1 - Create an MST file	88
Step 2 - Create a group policy	89
Using remote install on Clients running Windows Vista.....	90
Uninstalling Threat Shield Agents.....	90
B - Ports	91
INDEX	93

Threat Shield Manager

Overview.....	page 3
The Threat Shield Manager Interface.....	page 5
File Menu	page 6
View Menu	page 7
Rule Menu	page 8
Tools Menu.....	page 9
Help.....	page 21
Detection Technologies	page 22
The Threat Shield Toolbar	page 23
Key Points	page 24

1 THREAT SHIELD MANAGER

OVERVIEW

This chapter explains how to use the Threat Shield Manager to monitor clients. Threat Shield Manager is the user interface for configuring policy rules and is the 'front end' of the Threat Shield server. It also communicates with the Threat Shield Agent, sending configuration changes to it as it initiates or when the client polls the server.

TERMINOLOGY USED

The following terminology is used in this chapter:

Threat Shield Agent

The Threat Shield Agent runs as a stealth application on each workstation and is initiated from the Threat Shield server. Users see no evidence of it unless a rule is triggered. This depends on the action set up as a response to this event such as a message being displayed. Threat Shield Agent gathers rule configuration from Threat Shield Manager then uses this to enforce rules when they are triggered. This also happens when an initiated or scheduled scan of the client is performed.

Threat Shield Agent does not have to be installed on each workstation, and if you uninstall Enterprise Threat Shield the Agent is terminated automatically by the server. If a server is uninstalled, and the Agent is not stopped, it will terminate as soon as it polls the server and realizes that it no longer exists. The Threat Shield Agent is responsible for the following operations:

- Searching for defined content files in a schedule set by Threat Shield Manager.
- Maintaining real-time rules regarding the running of different types of applications.
- Monitoring network areas for the adding of new files.
- Reporting its current situation and findings to Threat Shield Server.
- Responding to Threat Shield Server requests, such as configuration changes and requests for real-time information.

Threat Shield Agent is initiated remotely on NT family workstations.

Threat Shield Server

Threat Shield Server is the real-time control center of the Threat Shield Agents. It runs continuously, providing server functionality to the clients while Threat Shield Manager is used to configure it as required.

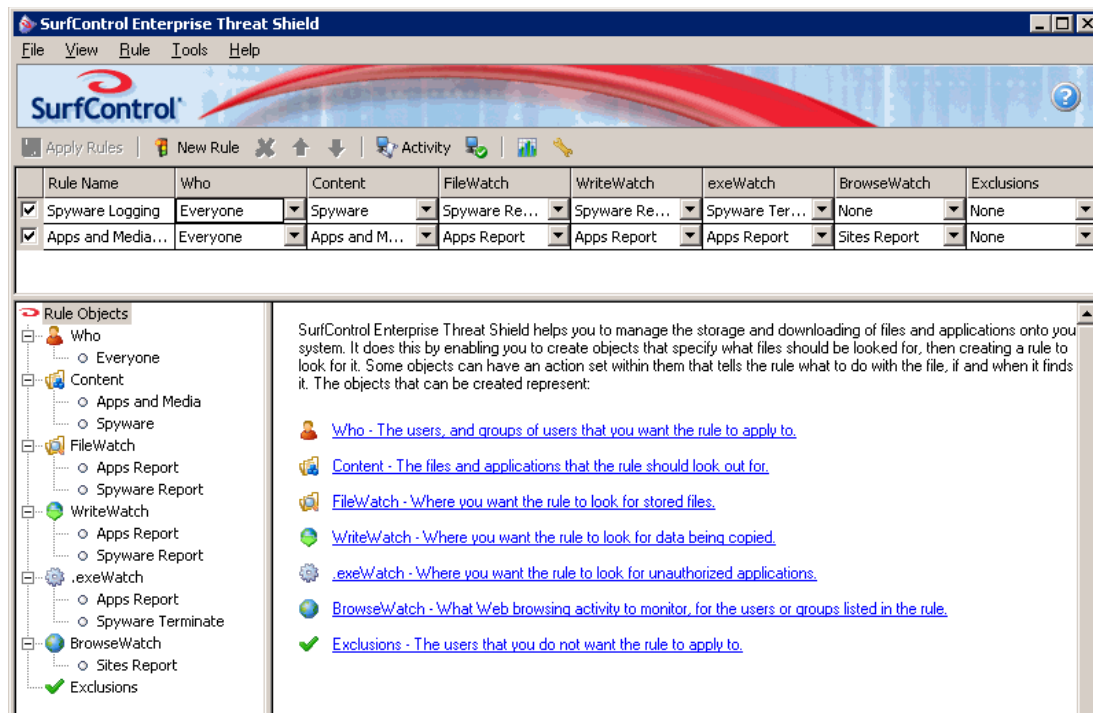
Threat Shield Server communicates with the Threat Shield Agent through the network, sending rule configuration changes to a client when its Agent initiates, or when the client polls the server.

Threat Shield Server is responsible for the following operations:

- Initiating the clients and keeping them running.
- Transmitting updated dynamic rule configurations to the clients.
- Collecting the handling events and messages sent by the clients, and displaying or archiving the received information in various formats (Threat Shield Server is not visible to the user).

WHAT CAN BE CONFIGURED WITHIN THE THREAT SHIELD MANAGER?

Threat Shield Manager is the user interface for configuring policy rules:



Threat Shield Manager enables you to:

- Set the rule configurations that are used to manage the content databases and monitor clients.
- Receive reports of any rule being triggered from the Threat Shield Agent.
- Define the objects of rules, then use these objects to build rules.

THE THREAT SHIELD MANAGER INTERFACE

The Threat Shield Manager is composed of the following:

- **Menu Bar** - The menu bar gives you access to menus from which you can interact with the Threat Shield Agent and monitor workstations.
- **Toolbar** - Shortcuts to functions offered by the menu bar.
- **Rule Section** - A table listing any rules that have been created where you can use drop-down lists to add objects that you have created. See [Chapter 3 'Creating and using rules' on page 61](#) for instructions on how to create and edit rules.
- **Rule Objects Tree** - This shows your objects in a tree-like structure which can be expanded or contracted. See [Chapter 2 'Threat Shield Objects' on page 25](#) for instructions on how to create and edit objects.
- **Threat Shield objects pane** - Initially a pane with links to each object, on clicking a link a tabbed interface appears where you can create or edit objects. See [Chapter 2 'Threat Shield Objects' on page 25](#) for instructions on how to create and edit objects.

LAUNCHING THE MANAGER

Start the Threat Shield Manager in one of the following ways:

- Click the Enterprise Threat Shield desktop icon .
- Choose **Start > Programs > SurfControl > Enterprise Threat Shield > Threat Shield Manager**.

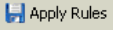
You can either use the default configuration that is supplied with the product, or change the current configuration.

FILE MENU

The File menu enables you to save settings, open the Reporter, update software and close the Threat Shield Manager.

APPLY RULES

Once you finish defining rules, you can transmit the configuration data to all of the clients. The client will then enforce the rules and inform the server if rules are triggered.

To transmit the configuration click the **Apply Rules** toolbar icon , or select the **Apply Rules** option from the **File** menu. This action saves the configuration so that it can be transmitted to all clients (agents).

When Threat Shield Agent is initiated, it requests a configuration from the server. Clicking the Apply Rules button saves changes to the server so that they can be picked up by the clients. This information is also transferred when the client next polls the server.

If you attempt to exit the application without having saved the current changes, you are reminded to do so.

OPEN THREAT SHIELD REPORTER

Threat Shield Reporter analyzes the data collected by Threat Shield. It enables you to create a variety of reports that can be displayed in graphical and tabular format.

UPDATE SOFTWARE

Enables you to update the Enterprise Threat Shield software version via the Internet.

EXIT

Enables you to exit the Threat Shield Manager application. If the configuration file was not saved, a message is displayed.

VIEW MENU

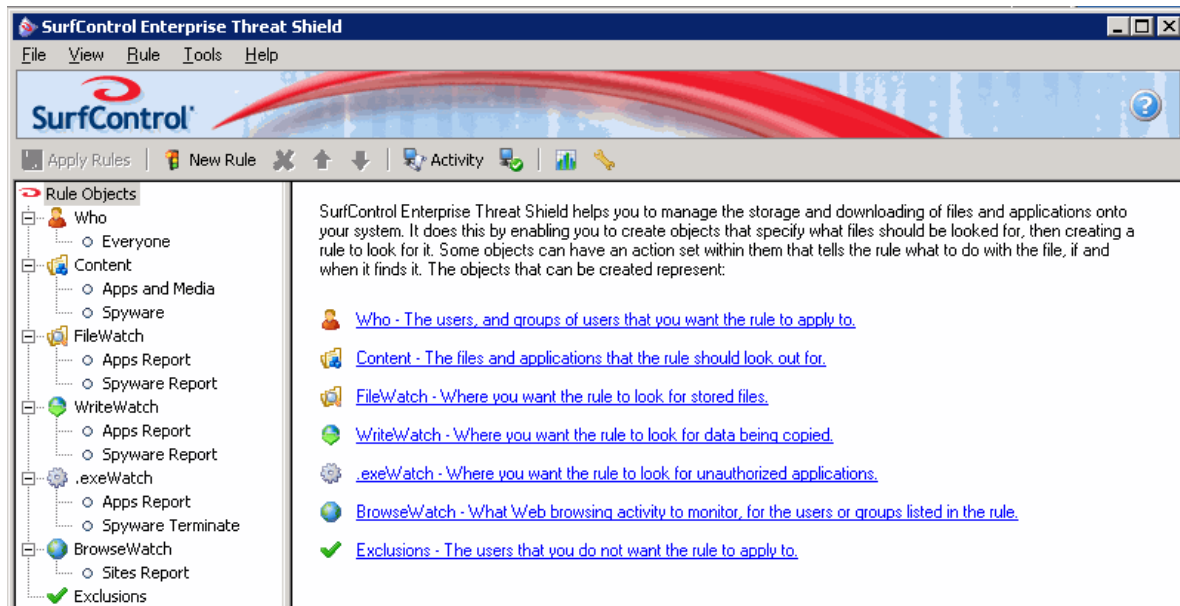
The View menu enables you to show or hide the:

- Rule Objects tree
- Rules table

RULE OBJECTS TREE

Selecting the Rule Objects tree option enables you to show the Rule Objects tree and object details in the Threat Shield Manager main window.

Figure 1 - 1 Showing the Rule Objects tree and hiding the Rules table



RULES TABLE

Alternate clicks of the Rules table menu option enable you to show or hide the Rules table in the Threat Shield Manager main window.

Figure 1 - 2 Showing the Rules table and hiding the Rule Objects tree

Rule Name	Who	Content	FileWatch	WriteWatch	exeWatch	BrowseWatch	Exclusions
<input checked="" type="checkbox"/> Spyware Logging	Everyone	Spyware	Spyware Rep...	Spyware Rep...	Spyware Ter...	None	None
<input checked="" type="checkbox"/> Apps and Media...	Everyone	Apps and Media	Apps Report	Apps Report	Apps Report	Sites Report	None

RULE MENU

The Rule Menu enables you to:

- Create new rules.
- Delete old rules.
- Change rule priorities.

NEW

Enables you to add a new rule.

DELETE

Enables you to delete a rule.

RAISE RULE PRIORITY

Enables you to raise the priority of a rule by moving it up in the Rules table. This is disabled when the first rule in the table is selected.

LOWER RULE PRIORITY

Enables you to lower the priority of a rule by moving it down in the Rules table. This is disabled when the last rule in the table is selected.

For information on creating and managing rules see [Chapter 3 'Creating and using rules' on page 61](#)

TOOLS MENU

The Tools menu gives you the means to:

- Check workstation activity.
- Manage the status of workstations.
- Edit databases.
- Set passwords for the Administrative user.
- Set up the Threat Shield system.

WORKSTATION ACTIVITY

The Workstation Activity window shows messages from the client in real time. It enables you to see details of the rule being triggered, including the workstation triggering the rule, the date this happened and the reason.


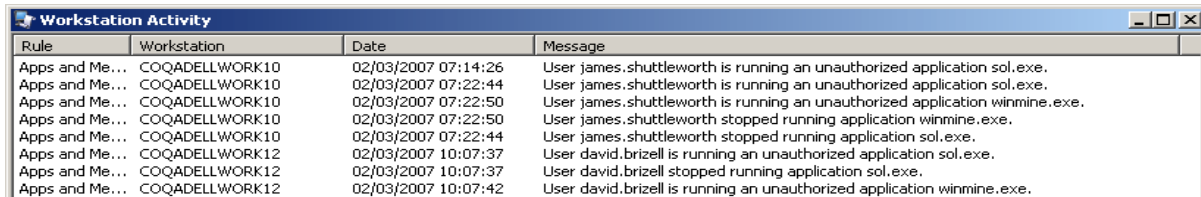
To display the Workstation Activity window, click the  toolbar icon. Alternatively, select **Workstation Activity** from the **Tools** menu. The Workstation Activity window is displayed:

Figure 1 - 3 The Workstation Activity window




Rule	Workstation	Date	Message
Apps and Me...	COQADELLWORK10	02/03/2007 07:14:26	User james.shuttleworth is running an unauthorized application sol.exe.
Apps and Me...	COQADELLWORK10	02/03/2007 07:22:44	User james.shuttleworth is running an unauthorized application sol.exe.
Apps and Me...	COQADELLWORK10	02/03/2007 07:22:50	User james.shuttleworth is running an unauthorized application winmine.exe.
Apps and Me...	COQADELLWORK10	02/03/2007 07:22:50	User james.shuttleworth stopped running application winmine.exe.
Apps and Me...	COQADELLWORK10	02/03/2007 07:22:44	User james.shuttleworth stopped running application sol.exe.
Apps and Me...	COQADELLWORK12	02/03/2007 10:07:37	User david.brizell is running an unauthorized application sol.exe.
Apps and Me...	COQADELLWORK12	02/03/2007 10:07:37	User david.brizell stopped running application sol.exe.
Apps and Me...	COQADELLWORK12	02/03/2007 10:07:42	User david.brizell is running an unauthorized application winmine.exe.

Click the **Clear** button in the bottom left of the window to erase the window's contents.

WORKSTATION DEPLOYMENT AND STATUS

The Workstation Deployment and Status window shows all the workstations in the Network Directory and their current status. This window is used to launch and monitor agents.

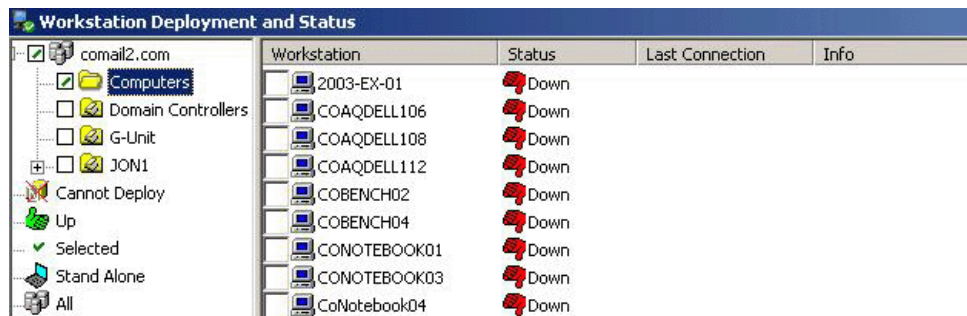
To display the Workstation Deployment and Status window, click the  toolbar icon. Alternatively, select **Workstation Deployment and Status** from the **Tools** menu. The Workstation Deployment and Status window is displayed.








Note: When you add a new workstation to a group within the tree, it will immediately inherit the security of the parent group.

Window Organization. The Workstation Deployment and Status window, shown below, displays a hierarchical tree structure depicting the Active Directory/ Windows NT Directory Service/Novell Directory Service (NDS) structure in its left pane. This tree structure provides a convenient way to deploy Threat Shield Agent on some or all workstations simultaneously.


Figure 1 - 4 The Workstation Deployment and Status window



The bottom part of the left pane displays a series of buttons, which can be used to filter (by status) the information displayed in the right pane of the window. Options include:

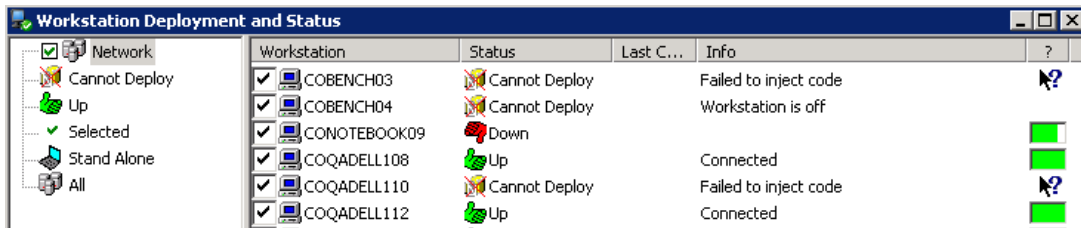
-  - Click to display only those workstations that cannot be deployed.
-  - Click to display only those workstations that have connected successfully.
-  - Click to display only those workstations whose deployment check box has been selected.
-  - Click to display only those workstations which have been set to Stand Alone mode.
-  - Click to display all workstations.

When you click a node in the tree, its objects are displayed in the right pane of the window. The following information is displayed for each entry in the window's right pane:

- **Deploy Check box** - When selected, designates that the Threat Shield Agent is to be launched remotely on the workstation. When not selected, the agent is not launched on the workstation. The deployment process starts automatically once you select the check box.
- **Workstation** - Specifies the name of the workstation.
- **Status** - Indicates the deployment status of the workstation, which can be **Up**, **Down** or **Cannot Deploy**. The default is **Down**.
- **Last Connection** - Indicates the date and time of the last connection.
- **Info** - Provides additional details about the workstation's status.
- **?** - Shows a progress bar indicating the progress of the deployment process on the workstation. By clicking , you can also see additional details about problems in the deployment process.

ACTIVATING THE DEPLOYMENT PROCESS

The deployment process can be initiated on one or more workstations simultaneously. Selecting a check box for an item in the tree (left pane) or in the right pane of the window automatically starts the deployment process for the selected item(s). Once the process begins, you can watch its progress in the progress bar on the far right of the right pane:



- When a workstation has been successfully deployed, the progress bar is green, its status shows **Up** and the comment in the Info column shows **Connected**.
- If a workstation cannot be successfully deployed remotely, a warning message is displayed and its status shows **Cannot Deploy**. The Info column also provides additional information about the reason for unsuccessful deployment.

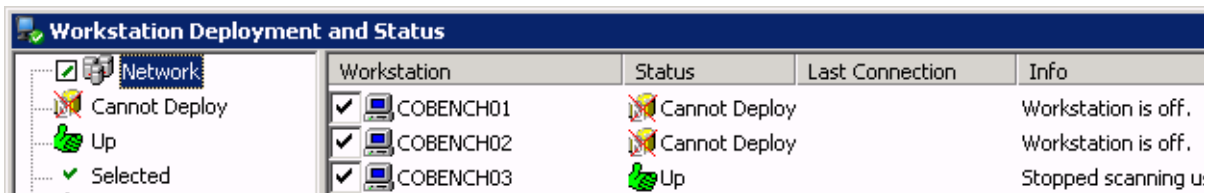


Note: In order to use the Remote Loading feature, the Threat Shield Server must have Administrator rights on the domain.

Deploying on a workstation

To deploy the Threat Shield Agent on a workstation:

- 1 Select the check box in the right-hand pane of the window, adjacent to the workstation(s) you want to deploy
OR
Select a node in the left-hand pane to select all workstations beneath that node.



- 2 The Status will change to a to show that the Agent on that workstation is deployed

Deploying an entire tree node simultaneously

To deploy the Threat Shield Agent on an entire tree node simultaneously:

- 1 Select the check box adjacent to the node name you want to deploy. A message is displayed prompting you to confirm deployment of all the workstations under this node simultaneously.
- 2 Click **OK** to proceed.



Note: When you deselect the node check box in the tree, it stops all Agents on workstations under this node.

STAND ALONE MODE

The Threat Shield Agent has the capability of protecting a workstation when it is not connected to the Threat Shield server or does not have file-sharing set up (or both). It does this by downloading the files that it requires by HTTP then storing them locally. The benefits of Stand Alone are:

- The agent can download its files without having a file sharing connection to the Threat Shield server. These files are protected by security so they cannot be tampered with.
- Because the files are stored locally, the Agent can start up independently without the Threat Shield server having to initiate it. A local connection keeps the Agent active. In this way, policies that the Agent is enforcing will stay in place even if the client becomes disconnected from the Threat Shield server.
- Since data is stored locally, the Agent does not need to use network resources in order to receive data. This is extremely useful in cases where, for example, network resources are scarce due to low bandwidth.
- Firewall issues are avoided when the Agent would normally check a database on the Threat Shield server. The client already contains copies of the rules and databases that it needs, so there is no need to access the network for this information.

During updates the Agent checks an .ini file containing versions of its databases against the one it is about to download. To gather this information the client does not have to be physically connected to the network, though it does need a VPN connection. This information cannot be gathered via the Internet alone, the VPN connection must be in place.

If the Agent is set up in Stand Alone mode and is connected to the Threat Shield Server it will download the latest updates as they become available, then use them locally. The Agent does not download the whole file, only any recent changes. When installing the Agent on workstations, an installation option is provided that enables you to install in Stand Alone mode. This is useful in cases where the bandwidth is too low for initiating the whole deployment.


Using Stand Alone mode

To use Stand Alone mode:

- 1 Open the Workstation Deployment and Status window from the Tools menu.
- 2 You can select workstations for Stand Alone mode in the following ways:
 - Select individual workstations from the right-hand pane.
 - Select a domain or Organizational Unit from the left-hand pane. This will apply to all workstations beneath this node.
- 3 Right-click the node you wish to apply Stand Alone to.
- 4 Choose **Stand Alone** from the pop-up menu. The workstation icon(s) will change to that of a laptop to show that these workstations are now switched to Stand Alone mode.
- 5 Select the Deploy check box corresponding to these workstations to deploy them in Stand Alone mode.

Setting a workstation back to normal mode

To switch Stand Alone mode off and set a workstation back to normal mode:

- 1 Deselect the check box alongside the selected workstations to stop the Agents.
- 2 Once you can see the red Down icon  , which indicates that the Agent is stopped, select the workstation or group of workstations that you wish to change back to normal mode.
- 3 Right-click and select **Switch Stand Alone off** from the pop-up menu. The laptop icon will change to that of a workstation.
- 4 Select one or more check boxes to deploy the agents in normal mode.

CHANGE ACCOUNT INFORMATION

During application installation, you are prompted to supply network administrator user name and password account information. The Threat Shield Server must run under this administrative account to be able to deploy Threat Shield Agents remotely within the network. See The Starter Guide for more details. Network administrator account information can be changed, as required, after application installation.

To change account information:

- 1 Select **Change Account Information** from the Tools menu. The Change Account Information window is displayed.
- 2 Enter the administrator's details.
 - **User name** - Enter the administrator's user name.
 - **Password** - Enter the administrator's password.
 - **Domain** - Enter the domain that the Threat Shield server is a part of.
- 3 Click **OK**.

SETTINGS

Implementation of system settings is carried out in the Settings dialog and include:

- **General Settings tab** - Enables you to specify the minimum size of media files that should be monitored for triggering rules by detection mechanisms, as well as the Directory Service data Who and Exclusion objects to be displayed.
- **Report File Settings tab** - Enables you to specify the parameters for log files, which can be used for monitoring and reporting purposes.
- **Database Settings tab** - Enables you to specify database settings used by Threat Shield Reporter for storing violations data.
- **Reporter Settings tab** - Enables you to specify the user name and password details to be used for accessing Threat Shield Reporter using a browser.
- **E-mail Settings tab** - Enables you to specify the parameters of the e-mail notification that may be sent to the administrator when a rule is triggered.
- **Directory Service tab** - Enables you to specify the parameters of the directory server, which allows you to see the users, groups and workstations of the organization.

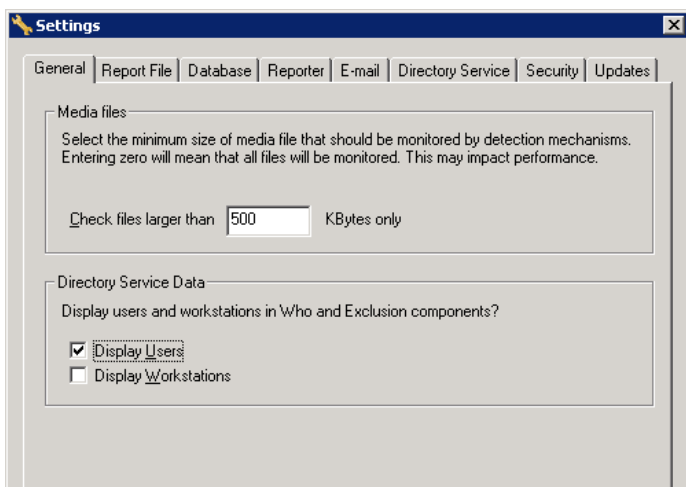
To display the Settings dialog, click the **Settings** toolbar icon  or select **Settings** from the Tools menu.

The General Tab

The General tab enables you to set the minimum size of media files that should be monitored for triggering rules. You can also specify whether to display users, workstations, or both, in Who and Exclusion objects for Directory Service data. If you choose to display both users and workstations, Threat Shield Manager's performance is slower than if you select only a single option.

Setting up the General tab:

- 1 Select the **General** tab in the Settings dialog.



- 2 Specify the size of files that you want to be monitored.
 - **Check files larger than ...K Bytes only** - Enter the required file size into the text box. Only files of a size greater than this, in kilobytes, will be monitored.
- 3 Select how you want details to be shown in Who and Exclusion objects.
 - **Display Users** - Select the check box to display all users.
 - **Display Workstations** - Select the check box to display all workstations.
- 4 Click **OK**.

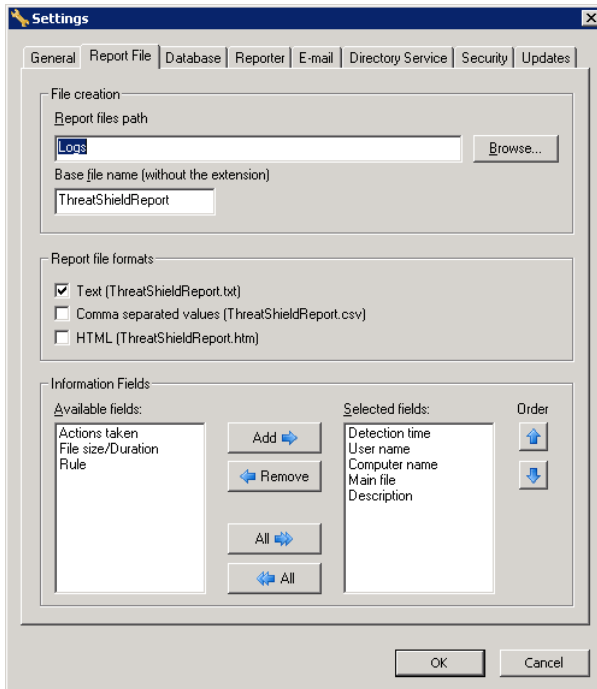
The Report File tab



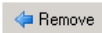

The Report File tab enables you to specify the parameters for log files, which can be used for monitoring and reporting purposes. It enables you to configure the location, format and information (such as description and actions taken) in the log file. First you define the log file report path and format, then select the information fields for the log file report along with their order of appearance.



Note: For the report to be generated, the Generate report check box must be selected in the relevant FileWatch, WriteWatch or .exeWatch detection object Actions tab.

- 1 Select the **Report File** tab in the Settings dialog:



- 2 Specify a location and name for the Report file:
 - **Report File path** - Enter a path to the Report file or click **Browse** to select the folder where the log files will be created.
 - **Base file name (without the extension)** - Enter the log file name.
- 3 Choose the format of the Report File by selecting one or more of the Report file formats check boxes:
 - **Text (<Base file name>.txt)** - Select this check box to save the log file in plain text format.
 - **Comma separated values (<Base file name>.csv)** - Select this option to save the log file in *.csv format. This format can be imported into Microsoft Excel and most database applications.
 - **HTML (<Base file name>.htm)** - Select this option to save the log file in *.htm format. This format can be used with your Internet Explorer or Netscape.
- 4 The Report File tab Information Fields panel is comprised of an Available (left-side) panel and a Selected (right-side) panel. Only the fields that are listed in the Selected panel will apply to the report:
 - Select the required field in the Available fields panel and click the **Add** button .
 - Select all fields by clicking the **Add** button .
- 5 To remove fields:
 - Select the required field in the Available fields panel and click the **Remove** button .
 - Select all fields by clicking the **All** button .

- To change the order of information fields in the report select a required field in the Selected panel and click:



- To move it one field up, toward the top of the report.



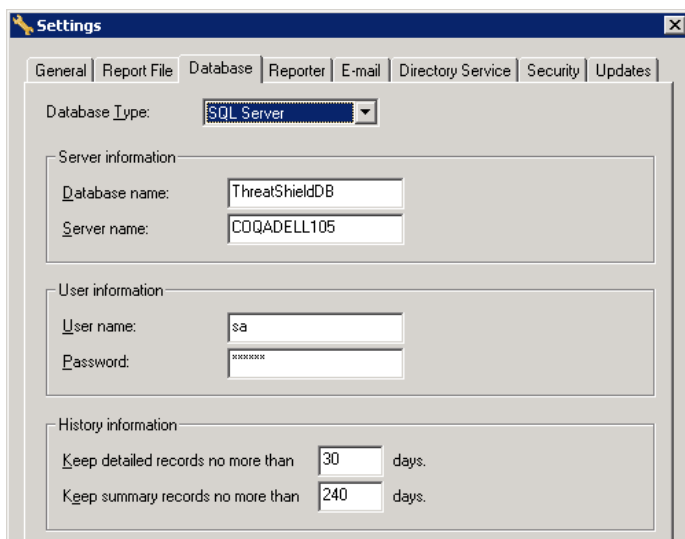
- To move it one field down, toward the bottom.

- Click **OK**.

The Database Tab

Database settings specify the database server on which the data used by Threat Shield Reporter is stored. A database must be defined in this tab for Threat Shield Reporter to be able to create reports.

- Select the **Database** tab in the Settings dialog:



- Select the type of database that you wish to use.
 - Database type** - Select the SQL server to be used from the Database type drop-down list.
- Enter the name of the database and the server.
 - Database name** - Enter a name for the database. The default name is ThreatShieldDB.
 - Server name** - Enter the name or IP address of the server name where this database is created.
- Specify the credentials for the user that will be authenticated by the database server. If these fields are blank, Windows authentication is performed instead of SQL authentication. In this case, users who want to view reports over the Web may not be permitted to do so.
 - User name** - Enter the user name that is authorized to create new databases and objects within the database.
 - Password** - Enter the password for this user.
- When log files are written to the database, they include data about the date and time the rule was triggered. Database log files also contain more detailed information, such as the path for this file and summary data, like the number of files found during a specific scan.

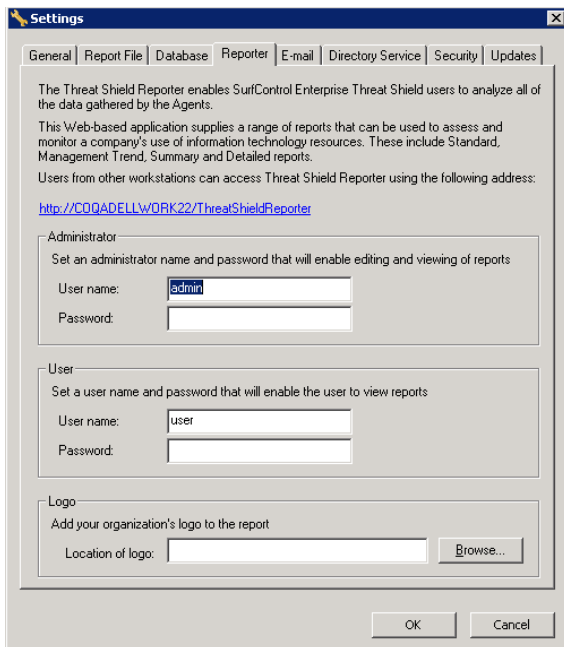
- **Keep detailed records no more than ... days** - Enter a value for the number of days these records should be kept in the database.
 - **Keep summary records no more than ... days** - Enter a value for the number of days records should be retained in the database
- 6 Click the **Test Connection** button to check that the details you have entered are valid.
 - 7 Click **OK**.

The Reporter Tab

Threat Shield Reporter is the mechanism used to create and view reports on data of rules triggered. In the Reporter tab, you specify the user name and password required to view Threat Shield Reporter reports within the Intranet using a browser, as well as the user name and password for Administrator-level access to the application.

To define Reporter settings:

- 1 Select the **Reporter** tab in the Settings dialog:



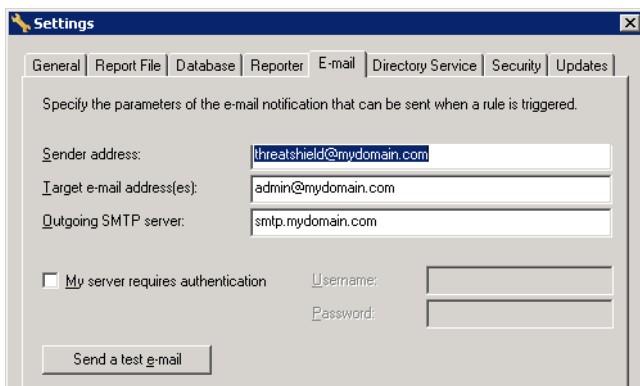
- 2 Enter the authentication details to be assigned to users with Administrator access rights.
 - **User name** - Enter a user name for the Administrator.
 - **Password** - Enter a password.
- 3 Enter the authentication details for viewing Threat Shield Reporter reports. No saving or editing will be allowed with these credentials.
 - **User name** - Enter a user name for someone with User (read-only) rights.
 - **Password** - Enter a password.
- 4 An image file can be displayed at the top of all Threat Shield Reporter reports.
 - **Location of logo** - Enter the path to the image or click **Browse** to navigate to the required file.
- 5 Click **OK**.

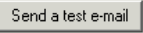
The E-mail Tab

Enterprise Threat Shield enables you to monitor the user's actions through e-mail reporting when a rule is triggered. The E-mail tab enables you to specify the parameters of the e-mail notification.

To define E-mail Settings

- 1 Select the **E-mail** tab in the Settings dialog.



- 2 Enter details for the e-mail notification.
 - **Sender address** - Enter the URL from which the e-mail will be sent.
 - **Target e-mail addresses** - Enter one or more separated by semicolons. For example, admin@mydomain.com; user@company.com
 - **Outgoing SMTP server** - Enter the name or IP address of the default outgoing e-mail server.
 - **My server requires authentication** - Select the check box to enter the username and password .
- 3 Click the **Send a test e-mail** button  if you want to send a message to check that your settings will work. You can edit this message within the Threat Shield Manager, using the **E-mail format** button. This can be found in the Actions tab of the object you are configuring.
- 4 Click **OK**.



Note: For e-mail notification to be enabled, the 'Send an e-mail report' check box must be selected within the relevant FileWatch, WriteWatch or .exeWatch Actions tab.

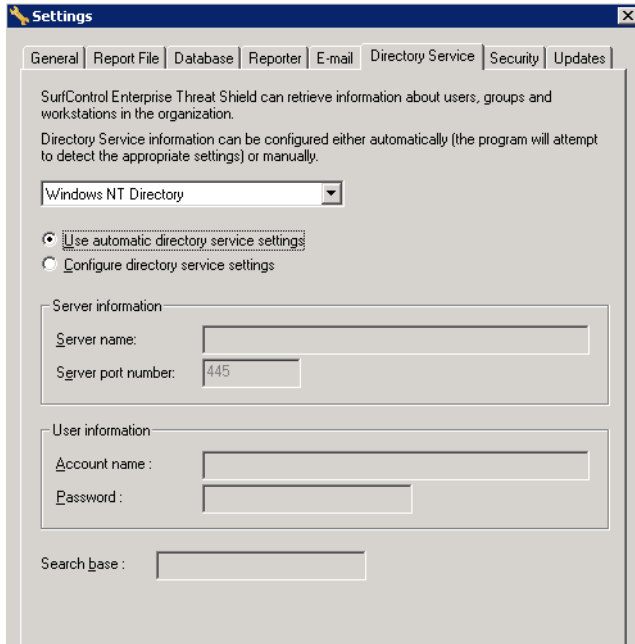
The Directory Service tab

Enterprise Threat Shield can retrieve directory data from a variety of directory servers. These servers include the entire Windows family, as well as the Novell network starting from version 4. The directory servers supply Enterprise Threat Shield with information about users, groups and workstations in the organization. The Directory Service can be configured either automatically (Enterprise Threat Shield will attempt to detect the appropriate settings) or manually, using the Directory Service tab. Enterprise Threat Shield supports three types of directory services:

- Windows NT Directory (this is also the default option).
- Active Directory for Win2000 directory server and up.
- NDS for Novell network OS. Enterprise Threat Shield supports Novell version 4 and up.

To configure directory service settings manually:

- 1 Select the Directory Service tab:



- 2 Specify how you want directory service information to be retrieved, by choosing the operating system from the drop-down list. The default is Windows NT Directory.
- 3 Select one of the following options:
 - **Use automatic directory service settings** - The server will automatically detect the settings.
 - **Configure directory service settings** - Enter the relevant information for your selected operating system:
 - **For Windows NT Directory** - Enter the Server name with double back slashes before the name (for example, \\server1).
 - **For Active Directory (Windows 2000 and up)** - Enter the following:
 - Directory server name (or the domain name).
 - Port number (the default is 3268, which is the Active Directory port).
 - Network user name and password (not necessary if the administrator runs Enterprise Threat Shield).
 - Root for search in DNS format (for example, dc=microsoft or dc=com).
 - **For NDS (Novell 4 and up)** - Enter the following:
 - Network user name and password.
 - Root for search in DNS format (for example, o=Microsoft).
- 4 Click **OK**. This will automatically transmit the configuration to the client machines.

The Security Tab

The Security tab enables you to change the Enterprise Threat Shield entry password in order to prevent unauthorized access to the system and its rules change features.



Note: When the system is first installed, the Administrator password is " " (no password required) and should be changed at the first opportunity.

To change the Enterprise Threat Shield entry password:

- 1 Select the Security tab:

Settings

General | Report File | Database | Reporter | E-mail | Directory Service | Security | Updates

Entry password

Change the SurfControl Enterprise Threat Shield entry password to prevent unauthorized access to Threat Shield Manager.

Enter current password:

Enter new password:

Verify new password:

- 2 Enter a new password to enhance security for the Threat Shield Manager.
 - **Enter current password** - Enter the current Enterprise Threat Shield password.
 - **Enter new password** - Enter the new password.
 - **Verify new password** - Enter the new password again.
- 3 Click **OK**. If the user name or password details that you enter are invalid, a warning message is displayed. The change is effective the next time you access the system.



Note: Only one instance of Enterprise Threat Shield is allowed to run at one time. If you attempt to log in while the application is open to another user, a warning message is displayed.

The Updates tab

See [Chapter 2 'Updating SurfControl-supplied Databases'](#) on page 34

HELP

The Help menu gives you access to tools to help you solve problems with Enterprise Threat Shield.

- **Contents** - Launches the Help system with the Contents pane uppermost.
- **Index** - Launches the Help system with the Index pane uppermost.
- **Search** - Launches the Help system with the Search pane uppermost.
- **Register** - Launches a dialog box where you can enter your serial number and activation key:



Figure 1 - 5 The Enterprise Threat Shield Registration dialog

- **Tech Support** - Sends an e-mail message to Technical Support. This message contains a copy of relevant configuration files in order that Technical Support can use them to discover what the problem is.
- **About SurfControl Enterprise Threat Shield** - Launches a message box which contains the version number of the product:

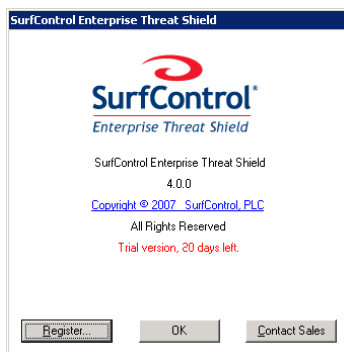


Figure 1 - 6 The Enterprise Threat Shield About box

This dialog box gives you three options:

- **Register** - Launches the Registration dialog (see above) where you can enter your serialization codes after purchasing the product.
- **OK** - Closes the dialog box.
- **Contact Sales** - Launches the SurfControl Contact information site where you can locate a SurfControl Sales office or Reseller.

A version of this dialog also appears when you first launch the Threat Shield Manager, except that the **OK** button is replaced by a **Try** button. Clicking this button enables you to evaluate Enterprise Threat Shield without registering.

DETECTION TECHNOLOGIES

The FileWatch, WriteWatch, .exeWatch and BrowseWatch detection methods use the same main detection engine, characterized by three detection technologies (see note below):

- Application detection, which controls the use, downloading and storing of all applications listed in the SurfControl signature databases (such as Spyware, games, MP3 peer-to-peer applications and instant messages). Users can also create a signature database using the DB Editor to detect user specified applications.
- Media file detection (music and movie content), which looks within the files for the specific protocols and formats typical of files, such as MP3 or MPEG. Databases are not used for this purpose.
- Actual use time tracking for web sites and pages, which detects active surfing time instead of just noting whether a browser is open or closed. The actual amount of time spent using a particular web site or page is recorded.

The first two detection methods above identify a file independently of its name or extension, monitoring and identifying the application by its content or "signature". Files are still detected even if they are renamed, hidden or compressed.

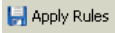










Note: The FileWatch and WriteWatch features detect both application and media files. The .exeWatch feature only detects applications.

THE THREAT SHIELD TOOLBAR

The toolbar buttons provide quick access to the most commonly used functions in the Threat Shield Manager main window. The following table contains a brief description of each toolbar option:

Table 1 - 1 Toolbar buttons

Button	Name	Description
	Apply Rules	Enables you to save the configuration data to the server, so that it can be transferred to the clients as and when they contact it.
	New rule	Enables you to add a new rule.
	Delete selected rule	Enables you to delete a rule.
	Raise rule priority	Enables you to raise the priority of a rule by moving it up in the Rules table. This is disabled when the first rule in the table is selected.
	Lower rule priority	Enables you to reduce the priority of a rule by moving it down in the Rules table. This is disabled when the last rule in the table is selected.
	Workstation Activity	Displays the Workstation Activity window, which shows current system messages.
	Workstation Deployment and Status	Displays the Workstation Deployment and Status window, which shows all the workstations on the domain and their current status. This option remotely launches the clients that are selected in the window. It then sends the latest configuration and monitors the client.
	Open Threat Shield Reporter	Enables you to open the Threat Shield Reporter module to create and view reports.
	Settings	Displays the Settings dialog, which enables you to implement various system settings.

KEY POINTS

The following list is a summary of the main points covered in this Chapter. Use this list as a quick reminder of what you can do within the Threat Shield Manager:

- The Threat Shield Manager is an interface which enables you to communicate with the Threat Shield server.
- Threat Shield Manager enables you to set the rule configurations that are used to manage the content databases, and monitor clients.
- With the Threat Shield Manager you can define the objects of rules, then use these objects to build rules.
- You can enable and disable rules.
- Windows in the Threat Shield Manager enable you to see what rules are being triggered and why, as this occurs.
- Deploy or stop Agents from running, or switch them to Stand Alone mode.
- Gives you access to the Reporter and configuration settings.

Threat Shield Objects

Overview.....	page 26
Creating a policy.....	page 27
Who.....	page 28
Content.....	page 30
FileWatch.....	page 39
WriteWatch.....	page 44
.exeWatch.....	page 48
Defining Message Formats.....	page 51
BrowseWatch.....	page 54
Exclusions.....	page 56
Key Points.....	page 59

OVERVIEW

This chapter explains how to create and use objects in the rules that you will apply to clients. The bottom half of the Threat Shield Manager contains two panes where these objects are created and managed.

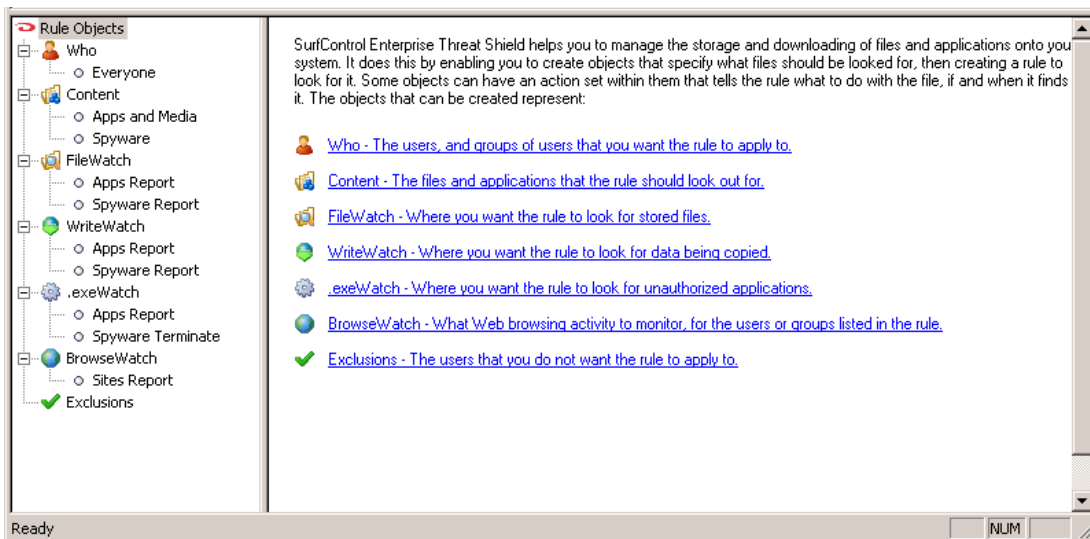
TERMINOLOGY USED

The following terminology is used in this chapter:

- **Object** - A collection of settings that are combined into a single unit, which can then be added to a rule. This makes rule creation simpler, as it enables you add single entities that do multiple jobs to a rule.

WHAT CAN BE CONFIGURED IN THESE PANES?

The bottom two panes of the Threat Shield Manager are used to configure the objects that you can add to rules and create your own policies:



With these panes you can:

- Create any of the following objects: Who, Content, FileWatch, WriteWatch, .exeWatch, BrowseWatch and Exclusion objects.
- Change the settings in existing objects.
- Create and edit User-defined databases.

CREATING A POLICY

There are three steps to creating a policy to apply to a rule:

Step 1 - Define who the rule will apply to, using Who - The Who object defines who a rule should apply to. It can contain single users or a group of users. It can also be set up to apply to a set of workstations. See [‘Who’ on page 28](#).



Note: Selecting a Who object does not deploy the agents on those elements within the Who object.

Step 2 - Define what to look for, using Content - The Content object enables you to define what files and applications a rule should look out. When a Content object is added to a rule that rule will trigger when it finds one of these files in the locations it is asked to check. See [‘Content’ on page 30](#).

Step 3 - Define the object to be used - The next objects you need to add specify the conditions that should trigger a rule, and the actions to be performed if a rule is triggered:

- **FileWatch** - The FileWatch object controls stored unauthorized files or applications. It searches for applications, such as games, P2P (Peer-to-peer), IM (Instant Messaging) and spyware, as well as music and video file types, including MP3 and Mpeg. See [‘FileWatch’ on page 39](#).
- **WriteWatch** - The WriteWatch object controls the introduction (downloading or copying) of unauthorized files or applications into file system folders. It monitors and protects areas of the network or local drives from infection by recreational or malicious files or applications. WriteWatch also detects, terminates and cleans existing spyware and stops new installations. See [‘WriteWatch’ on page 44](#).
- **.exeWatch** - The .exeWatch object controls the unauthorized use of applications. It monitors the running of applications like Spyware, and the loading of modules, such as dlls. It also monitors MP3 file swapping, messengers or any other applications operating on your network. Enterprise Threat Shield automatically monitors individual workstations and network servers to detect the use of these applications. See [‘.exeWatch’ on page 48](#).
- **BrowseWatch** - The BrowseWatch object identifies web browsing activity and monitors actual use time spent at visited web sites and web pages. BrowseWatch detects the duration of active web browsing, providing information about real interaction time as well as how long a browser is open, thus providing enhanced understanding of Internet use. See [‘BrowseWatch’ on page 54](#).
- **Exclusions** - The Exclusions object identifies should be excluded from a rule. If a user is included in a user group which has a few rules applied to it, you can ask a rule not to apply to this one user by adding them to the Exclusions object. See [‘Exclusions’ on page 56](#).

WHO


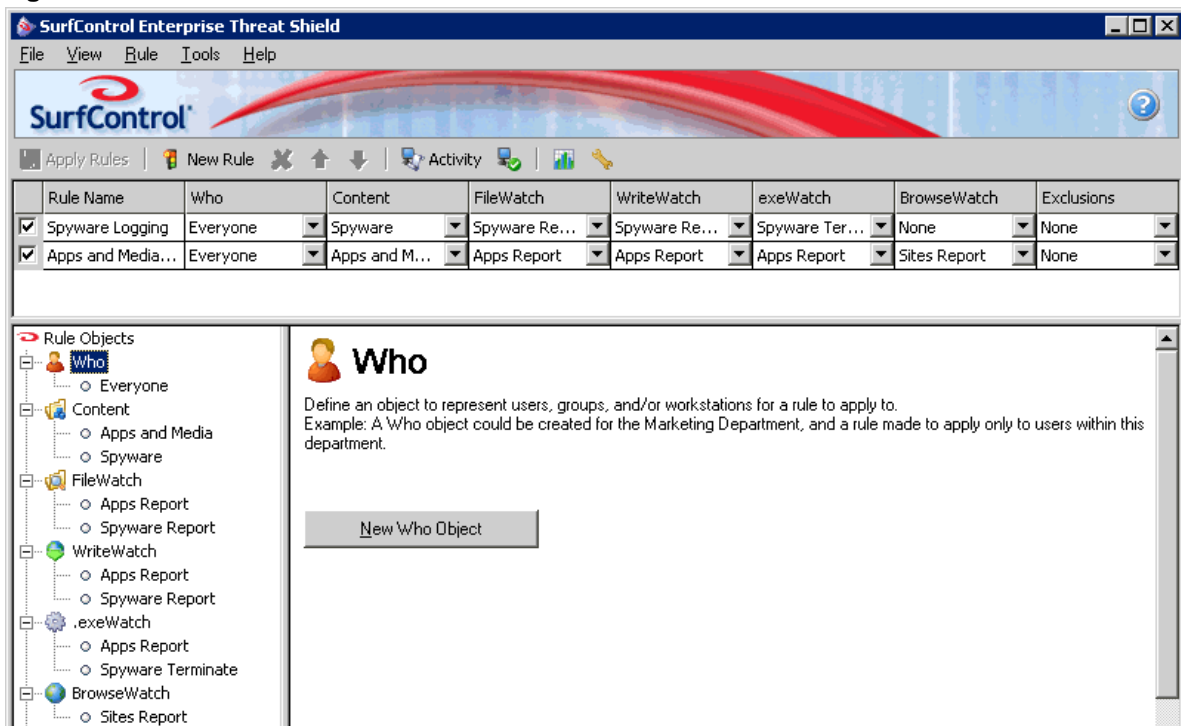
The Who panel enables you to define an object that specifies a set of workstations, users and groups to which a rule may apply. For example, a Who object can list the company's Marketing users, for use with a rule that manages these users. By default, only groups and operational units are displayed for this object. To be able to select individual users or workstations, you must make the relevant change in the General tab of the Settings dialog box. Access this by clicking  or selecting Settings from the Tools menu.

Figure 2 - 1 The Who screen



ADDING WHO OBJECTS

Before you can configure an object, you need to add it.

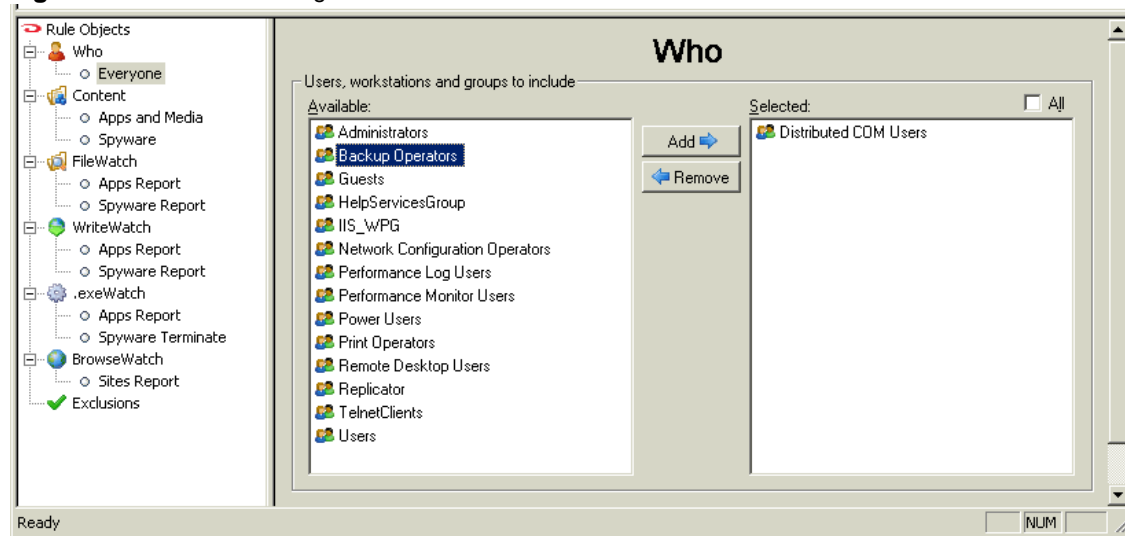
To add a Who object:

- 1 Select Who in the Threat Shield objects tree.
- 2 Click **New Who Object** in the **Who** pane. The new object will appear in the Rule Objects tree beneath the **Who** node.
- 3 Enter a name for the object.
- 4 You will now see the **Who** configuration screen. This screen appears when:
 - You select an existing Who object from the Rule Objects tree.
 - You add a new Who object.
- 5 You now need to configure this object. See the following section for information on how to do this. To edit an existing object, select it from the Rule Objects tree to see its corresponding configuration pane.

CONFIGURING WHO OBJECTS

The Who configuration pane enables you to configure an object that specifies which users and groups rules should apply to:

Figure 2 - 2 The Who configuration screen



To define a Who object:

- 1 Click the Who object in the Rule Objects tree.
- 2 Expand the branch beneath Who and select the object you wish to configure. You will now see the object's configuration pane.
- 3 Use the arrows to select the users or groups that you want to add or remove from the Selected pane. Only workstations, users and groups listed in the Selected pane will be considered by the rule which applies to this object.

 Move the selected user or group into the Selected pane. Rules will now apply to this user/group.

 Move the selected user or group into the Available pane. Rules will not apply to this user/group.

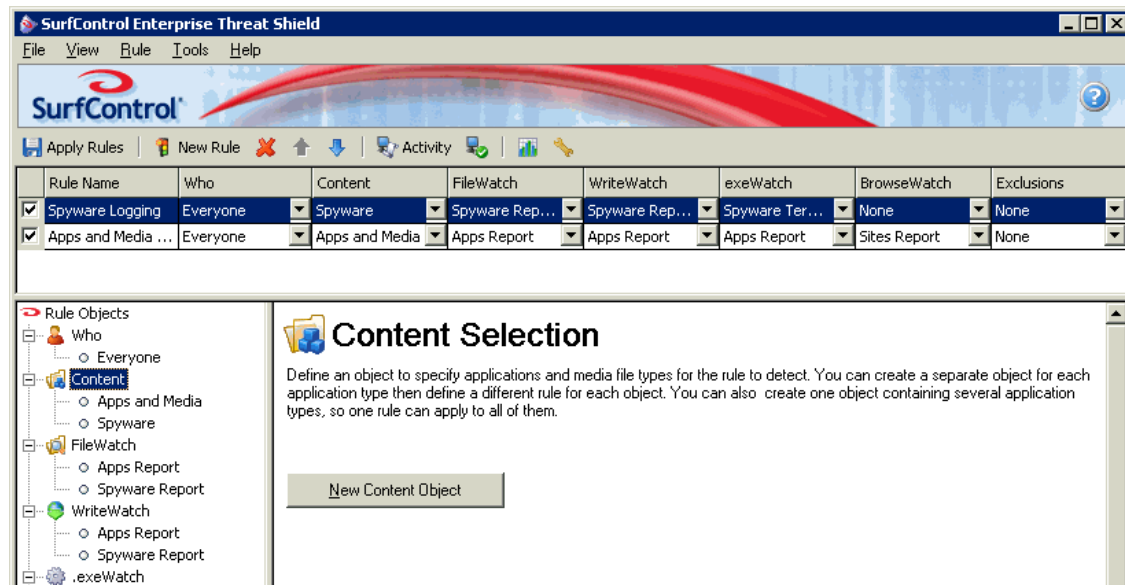
 Select to move all users or groups into the Selected pane. Deselect to move them out of this pane.

- 4 Selecting workstations, users and groups will not immediately start the Threat Shield Agent running on the workstations. You will need to deploy the Threat Shield Agent. See Chapter 1 'Activating the Deployment Process' on page 11. You can now add this object to a rule to have the rule applied to everything within the object.

CONTENT

The Content panel enables you to specify a set of signature databases (SurfControl-provided or User-defined) and media file types that a rule will detect:

Figure 2 - 3 The Content Selection screen



SIGNATURE DATABASES

The Application detection technology references applications listed in SurfControl-supplied and User-defined signature databases.

SurfControl Signature Databases

Enterprise Threat Shield provides a comprehensive set of signature databases that specify the applications whose use can be monitored and surveyed according to the rule that you set. These databases are kept current by SurfControl's Web site, which provides database updates periodically via the Internet.

User-defined Signature Databases

In addition, you can create and update your own customized signature databases using the Enterprise Threat Shield DB Editor. If you are creating custom databases, SurfControl recommends creating a different database for each application type, for example, a database for MP3 file swapping programs, and so on. In this way, the system needs to reference only a single database to enforce the rule.

The Content Selection panel is used to define Content objects. For example, by creating a different object for each application type (for example, MP3 File Swapping and Instant Messaging), you can then define different rules for each.

To create and edit your own databases you need to use the DB Editor. See [Chapter 2 'The Threat Shield DB Editor' on page 33](#) for more information.

ADDING A CONTENT OBJECT

Before you can configure an object, you need to add it:

To add a new Content object:

- 1 Select Content in the Threat Shield objects tree.
- 2 Click **New Content Object** in the **Content** pane. The new object will appear in the Rule Objects tree beneath the **Content** node.
- 3 Enter a name for the object.
- 4 You will now see the **Content** configuration screen. This screen appears when:
 - You select an existing Content object from the Rule Objects tree.
 - You add a new Content object.
- 5 You now need to configure this object. See the following section for information on how to do this. To edit an existing object select it from the Rule Objects tree to see it's corresponding configuration pane.

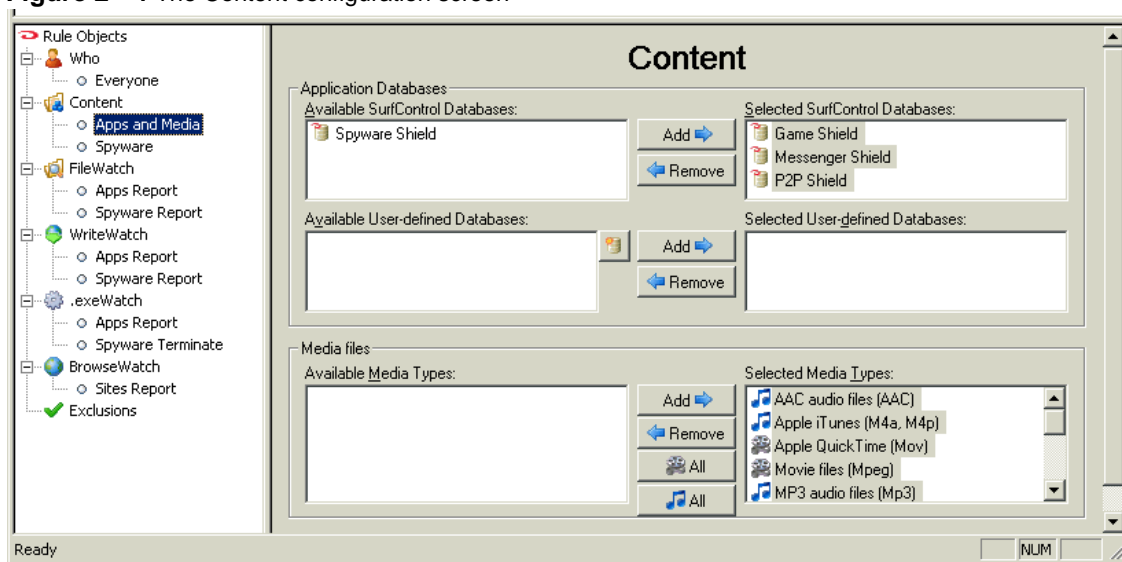
CONFIGURING CONTENT OBJECTS

There are two types of database that can be used: SurfControl supplied databases and User-defined databases. The Content Selection pane enables you to configure an object that specifies what databases a rule should use and what media files this rule should apply to.

To define a Content object:

- 1 Click the Content object in the Rule Objects tree.
- 2 Expand the branch beneath Content and select the object you wish to configure. You will now see the object's configuration pane:

Figure 2 - 4 The Content configuration screen

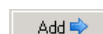



- 3 Use the arrows to select the database that you want to add or remove from the Selected pane.


 Move the selected database into the Selected pane. Rules will now apply to this database.


 Move the selected database into the Available pane. Rules will not apply to this database.

- 4 Only databases listed in the Selected pane will be used by the rule which applies to this object. To be seen by Enterprise Threat Shield, the databases should be in the Data folder.
- 5 Use the arrows to select the media type(s) that you want to add or remove from the Selected pane. Only media types listed in the Selected pane will be used by the rule which applies to this object.

 Move the media into the Selected pane. Rules will now apply to this media type.

 Move the selected media into the Available pane. Rules will not apply to this media type.

 Ensures only movie files are listed in the Selected Media format pane.

 Ensures only audio files are listed in the Selected Media format pane.



Note: Media files that are smaller than the minimum size set in the General tab of the Settings dialog box will not be checked. If media files are being allowed that should be stopped, check that the setting in this tab is not too large. The Settings dialog box can be accessed from the Tools menu.

Managing Media Files

Enterprise Threat Shield provides a set of Media file formats that specify the media file types whose use can be monitored and surveyed according to the rule that you set. Threat Shield Agent is able to search for these types of files by recognizing their special characteristics. The following is a list of supported media file types:

- AAC audio files (.AAC)
- Apple iTunes (.M4a, .M4p)
- Apple QuickTime (.Mov)
- Movie files (.Mpeg)
- MP3 audio files (.Mp3)
- Ogg Vorbis (.Ogg)
- Windows Audio files (.Wav)
- Windows Media Audio (.Wma)
- Windows media files (.Asf)
- Windows Media Video (.Wmv)
- Windows video file (.Avi)

Bit Torrent Detection


The bulk of all P2P traffic on the web is Bit Torrent files and Enterprise Threat Shield can detect these. To detect Bit Torrent files, select the P2P database and add it to your Content object. Bit torrent files will automatically be detected. Once this is done:

- WriteWatch will delete any torrent files, if it this is set in the Actions tab.
- The threshold setting for the minimum size of Media files that must be checked, will not affect torrent detection.
- The Threat Shield Reporter log files will show all details of torrent files that are detected.
- The Threat Shield Reporter will show records of torrent detection, and you can choose to filter by torrent in the Content tab of the Reporter.
- Torrent files will be shown in the Workstation Deployment and Status window.

THE THREAT SHIELD DB EDITOR

The DB Editor application enables you to create and edit your own databases, which can then be selected when defining Content objects. These databases appear in the User-defined Databases area of the Content Selection object panel. There are two types of database that can be used with Enterprise Threat Shield:

- **SurfControl supplied databases** - Enterprise Threat Shield includes a set of pre-defined databases with files and applications whose use is managed according to policy rules. SurfControl supplied databases cannot be modified in any way, they can only be updated.
- **User-defined databases** - The DB Editor application enables you to create and edit user-defined databases. There are no default User-defined databases supplied, you must create your own. Once you have created your own database you can edit it using the DB Editor.

To access the DB Editor click the DB Editor button  in the Application Databases section

OR

Right-click in one of the User-defined Databases panes and select **New**. You can also see the DB Editor when you right-click an existing User-defined Database and select **Edit**.

Menus in the DB Editor

The menu bar contains the following menus:

- **File Menu** - contains the following options:
 - **Save** - Enables you to save the database under the same name.
 - **Properties** - Opens the Database Properties window to display details about the database.
 - **Password Protection** - Displays the Password Protection window, enabling you to enter a password for your database.
 - **Exit** - Enables you to exit the Threat Shield DB Editor application. If the database was not saved, a message will remind you to save it.
- **Edit Menu** - contains the following options:
 - **Add Item** - Enables you to add a new application to the database.
 - **Add Item list** - Enables you to add a group of applications to the database.
 - **Rename Item** - Displays the Edit Item Description window, enabling you to change the name of the item.
 - **Delete Item** - Enables you to delete the currently selected item from the database.
 - **Find Again** - Enables you to search for the search item again.

- **View Menu** - contains the following option:
 - **Item Info** - Displays the Item Information window that displays the item's description, the main .exe file name, the number of files in the item, and so on.
- **Tools Menu** - contains the following options:
 - **Generate Item List** - Generates a list of database items in an HTML format, which can be viewed by any browser.
 - **Send Item to SurfControl** - see '[Sending an item to SurfControl](#)' on page 34.

SENDING AN ITEM TO SURFCONTROL

You can e-mail an item to SurfControl to be added to the SurfControl databases.

To send items to SurfControl:

- 1 Select the database item to send in the Items pane of the DB Editor.
- 2 Select **Send an item to SurfControl** from the **Tools** menu or right-click and choose this option. Your default e-mail client window is displayed showing the default message. If you have no e-mail client profile configured you will see a warning and the message will not be sent.
- 3 Send the message and the attached item to SurfControl.

UPDATING SURFCONTROL-SUPPLIED DATABASES

SurfControl-supplied databases include the following:

- Games Shield
- Messengers Shield
- P2P Shield
- Spyware Shield

If you are a registered user you can update SurfControl-supplied databases by manually connecting to SurfControl's Web site. In addition, you can set Threat Shield Manager to update a database automatically.



Caution: You must update your databases as often as possible to ensure that Enterprise Threat Shield is filtering as efficiently as possible. Failure to do so may compromise your system's protection.

Database and Software Update Service

The Enterprise Threat Shield Web site contains the latest version of SurfControl signature databases and your databases can be updated automatically to the latest version via the Internet. Enterprise Threat Shield can automatically check for the latest databases and software versions every day and when it starts up. It can then update your software automatically, if required. In this way, you can ensure that Enterprise Threat Shield will work with the latest SurfControl databases without your intervention. For details, refer to the next section 'Updating databases automatically'.

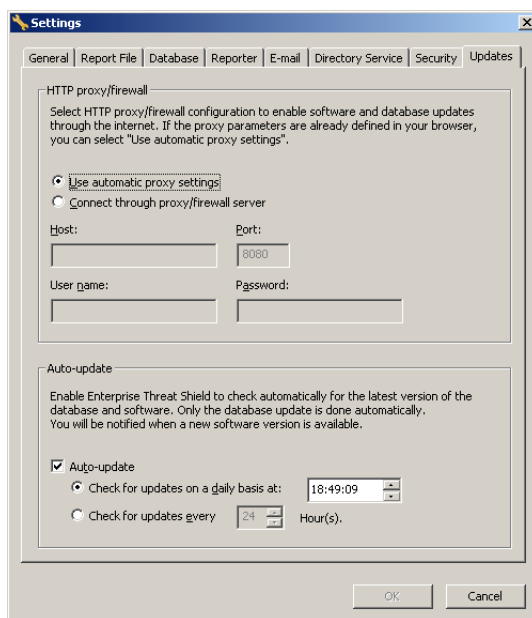
Updating databases automatically

To update databases automatically:

- 1 Choose **Settings** from the **Tools** menu in the Enterprise Threat Shield Manager.

- 2 Select the Update tab.
- 3 Define how you want the Threat Shield server to access the internet.
 - **Use automatic proxy settings** - Select this to use the automatic proxy settings for updating your databases (recommended for most users).
 - **Connect through Proxy/Firewall server** - Enter your proxy details into the relevant fields:
 - The Host name or IP address of the server
 - The port number of the server.
 - The username and password of your proxy/firewall server to enable the Threat Shield Manager to connect through this server.

Figure 2 - 5 HTTP proxy/firewall settings



- 4 If you want Threat Shield to automatically download updates of the latest SurfControl database and software versions select the 'Auto-update' check box.
- 5 Select one of the update options and specify a time:
 - **Check for updates on a daily basis at <date>** - Click the arrows to set a time. Updates will occur at this time every day if they are available.
 - **Check for updates every <hour> Hour(s)** - Click the arrows to set the time span in hours of when a check will be made. For example, inserting 6 will run an update check every six hours. If an update is available then this will be downloaded. Deselect this option if you don't want an update to occur automatically.
- 6 Click **OK**.

Updating databases manually

To update databases manually:

- 1 Right-click the SurfControl database that you want to update and select **Update**.

- 2 The update will start immediately. Enterprise Threat Shield updates the SurfControl defined databases by connecting to the Threat Shield Server via the Internet and replacing the existing database with an up to date one.

Viewing Database Properties

To view information regarding a selected SurfControl supplied database.

- 1 Right-click a SurfControl database and select Properties. A Database Properties message is displayed. The information contained in this message is as follows:
 - **Description** - The name of the database.
 - **Location** - The path to the database location.
 - **Type** - SurfControl supplied or User-defined.
 - **Items number** - This number reflects the number of applications, in all versions, in the database.
 - **Version** - The version number of the database.
- 2 Click **OK**.

Managing User-defined Databases

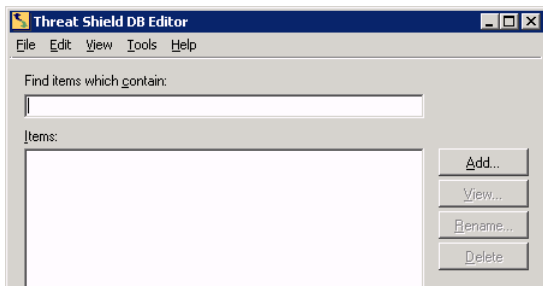
The DB Editor enables you to create and edit your own signature databases, so that you can add applications to the detection process and manage their use. SurfControl recommends creating a different database for each application type.

You can edit customized databases using the DB Editor. This includes adding new items to your database, changing the database description and so on. Only databases that you have created can be edited, SurfControl-supplied databases cannot be edited.

Creating a database

To create your own databases using the Threat Shield DB Editor:

- 1 Right-click in a User-defined Databases pane and select **New**. You will see the Threat Shield DB Editor.

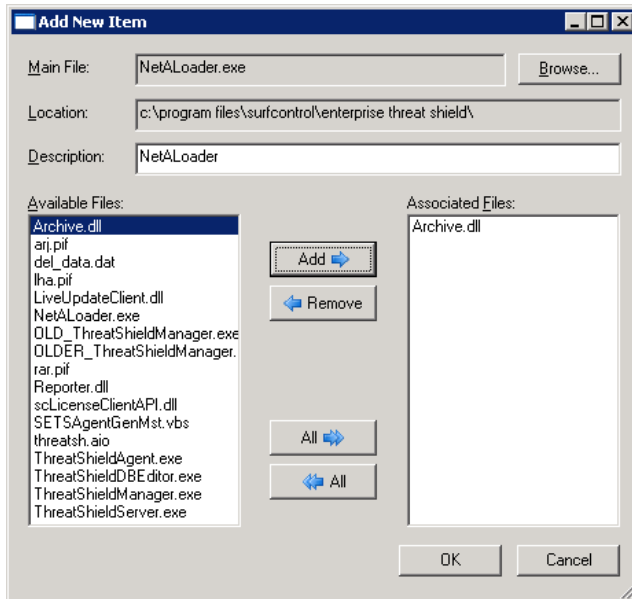


- 2 Click the **Add** button or select **Add Item** from the Edit menu.
- 3 Click **Browse** in the Add New Item dialog box that follows.
- 4 Use the Explorer dialog box to navigate to the file that contains the applications that you want to add to the database.



Note: A User-defined database must be stored in the Data folder if it is to be seen by the Enterprise Threat Shield Manager.

- This will add the path to the Location field:



- Enter a name for the application into the **Description** field.
- Select the main executable file of the application (*.exe, *.com, *.dll, *.ocx, *.sys or *.vxd). This file will be used to detect the application.



Note: The detection mechanism is not file name sensitive. Instead it reviews the content of the executable file and stores it in the database.

- Click **Add** (You can click **Remove** if you want to move the selected item back to the Available Files pane). Use CTRL+click or Shift+click to select multiple files.



Note: You can also add items by dragging and dropping the main executable application file from Explorer into the Items area. The Add New Item window is then displayed automatically.

- Click **OK**.

Editing databases

Before you start to edit a database, the following must be true:

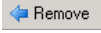
- The database must be one that you have created (not a SurfControl supplied database).
- The database must not be selected. If it is in the 'Selected User-defined databases' pane select the database then click **Add** to move it into the 'Available User-defined databases pane'.

To edit a database:

- Right-click the database and choose **Edit** from the drop-down menu.
- You will see the DB Editor with the name of the selected database displayed on the title bar. Modify your database, by adding or removing items as described in [See 'Creating a database' on page 36](#).

Deleting databases

Before you can delete a database, the following must be true:

- The database must be one that you have created (not a SurfControl supplied database).
- The database must not be selected. If it is in the 'Selected User-defined Databases' pane select the database then click  to move it into the 'Available User-defined Databases' pane.

To delete a database:

- 1 Right-click the database and choose **Delete** from the drop-down menu.
- 2 Click **OK** in the message that follows to remove the database from your system.

Adding Item Lists

The Threat Shield DB Editor enables you to add a group of applications to the database, by importing a text file containing the paths and descriptions of the items to add.

To add an Item List:

- 1 Create a text file containing the necessary information. For each item enter a different line, containing the item path and description (<Main exe file (full path)>, <Item Description>). For example:
d:\games\quake\quake.exe, Quake III Arena
c:\CrazyGravity\gravity.exe, Crazy Gravity
d:\games\Tetris.exe
- 2 Open the DB Editor and select Add item list from the Edit menu. In the Open window that follows select the text file, containing the items to add to the database. If you don't add a description, SurfControl uses the exe file name as the description.
- 3 Click **Open**. The applications that exist in the text file will be added to the database.



Caution: The ThreatShield DB Editor considers all the files in the item's folder as part of the item, so selecting Delete application files will delete all files in that directory. If an application such as Windows Mines resides in the Windows directory, then using the Add Items List command could result in the entire Windows directory being destroyed. **DO NOT** use Add Items List in such cases.

- 4 Click **OK** in the message that follows to remove the database from your system.

Searching for Items

You can search for an item by entering the item's description (or part of the description) into the Search Item area. The item that matches the entry is automatically selected in the Items area. For example, enter Pin to search for the Pinball item.

FILEWATCH

FileWatch enables you to create an object that controls stored unauthorized files and applications. It is particularly good at tracking Spyware. It can also control music or video files, games, and the P2P applications used to download media files. The files are recognized by their internal stamp (even if they are compressed) rather than their name or extension, so they can still be found if the extension has been changed.

During a scan, stored files are checked against the database of defined applications or file types, so you can 'immunize' workstations and servers from Spyware applications and files. If the 'Send an e-mail report' check box is selected in the Actions tab, an e-mail is sent to the system administrator with a summary of all the unauthorized files that were detected by the scan.

Figure 2 - 6 The FileWatch screen



ADDING A FILEWATCH OBJECT

Before you can configure an object, you need to add it.

To add a FileWatch object:

- 1 Select FileWatch in the Threat Shield objects tree.
- 2 Click **New FileWatch Object** in the FileWatch pane. The new object will appear in the Threat Shield objects tree beneath the FileWatch node.
- 3 Enter a name for the object. You will now see the FileWatch configuration screen. This screen appears when:
 - You select an existing FileWatch object from the Rule Objects tree.
 - You add a new FileWatch object.
- 4 You now need to configure this object. See the following section for information on how to do this. To edit an existing object select it from the Threat Shield objects tree to see it's corresponding object pane.

CONFIGURING FILEWATCH OBJECTS

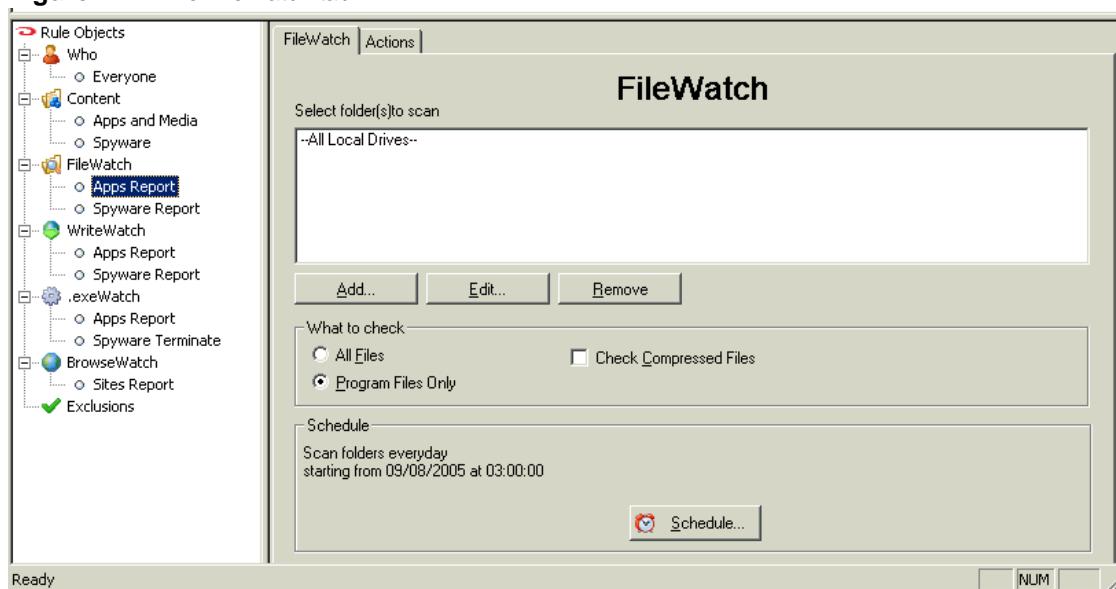
Once you have added a FileWatch object, use the configuration panel to define its behavior. The panel is comprised of two tabs:

- **FileWatch tab** - Enables you to specify the folders that should be scanned, and how frequently scanning should be performed.
- **Actions tab** - Enables you to specify the actions that should be performed when a folder is detected that violates a rule.

FileWatch tab

The FileWatch tab enables you to specify which folders should be monitored, what to check and how often:

Figure 2 - 7 The FileWatch tab



To define the folders to be monitored:

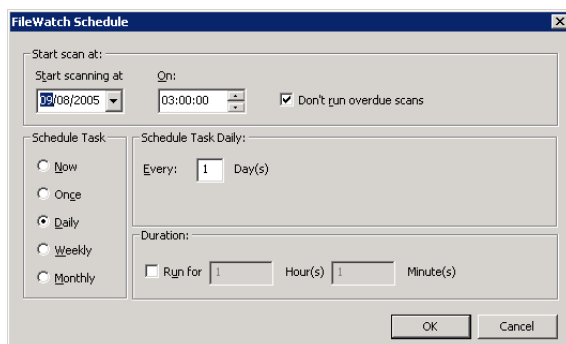
- 1 In the left-hand pane of the Threat Shield Manager double-click FileWatch to see the FileWatch screen.
- 2 Expand the branch beneath FileWatch and select the object you wish to configure. You will now see the object's configuration pane.
- 3 Use the buttons within the FileWatch pane to add, edit or remove the path to the folders that you want to be monitored.
 - **Add** - A dialog box appears that enables you to add a search path to the folder to be monitored. There are two options:
 - **All Local Drives** - All the drives of the local computer will be monitored. This will include any removable drives attached to the machine such as USB and MP3 players. If you set Threat Shield to delete files on 'All Local drives' you must be aware that files on this type of device will also be deleted.
 - **Path** - Select any local path. You can also add a path that includes an environment variable, in case the path is not absolute throughout the organization, for example, %windir%\system32.

- **Edit** - Edit the search path to the selected file.
 - **Remove** - Remove the search path to the selected file.
- 4 Select options to specify the type of files that you want FileWatch to check:
- **All Files** - Scan All files (including program files). This more complete scanning typically increases the scan time.
 - **Program Files only** - Scan files with executable extensions such as .exe, .dll, .com, .ax, .ocx.
 - **Check compressed files** - Select the check box to have FileWatch check files of this type even if they are in compressed format. This will display a window which enables you to report on password protected archive files that are copied to the local disk.
- 5 Set a schedule for the scan. See the following section for more details.

Scheduling a scan

Once you have defined what files to scan you can set a time for a scan to occur automatically:

- 1 Click  **Schedule...** to see the FileWatch Schedule dialog box.



- 2 Select the date and time that the scan should start.
 - **Start scanning at** - Click the arrow to the right of the field to open a calendar from which you can select a date.
 - **On** - Select a segment of the time and use the arrows to adjust it up or down.
 - **Don't run overdue scans** - Select the check box to stop any scans that were not run from running as soon as the Agent detects this. Instead the scan will be started at the next scheduled time.
- 3 Select the frequency of the scan.
 - **Now** - The scan will be started as soon as the new configuration is received by the client.
 - **Once** - The scan will be performed only once, on the date and time that you specified in step 3.
 - **Daily** - Displays an extra section where you can enter how often you want the scan to occur. For example, if you enter 3, the scan will run every third day, starting from the day and time set in the 'Start Scan at <time>' section (the default is 1, which means the scan will be run every day).
 - **Weekly** - Displays an extra section where you can specify the days on which you want the scan to occur. Select the check boxes corresponding to the days of the week on which the scan should be performed, at the specified time. The scan will be performed on those days in each subsequent week, starting from the indicated date.

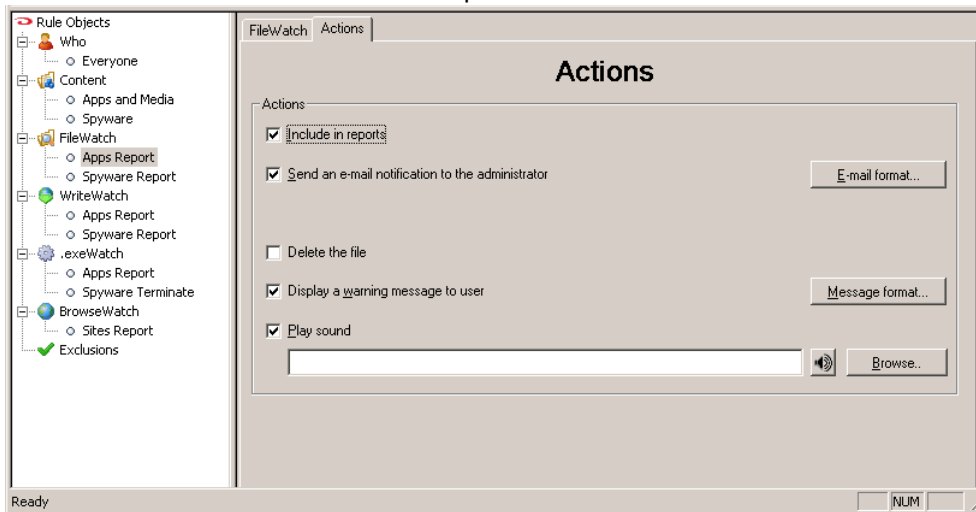
- **Monthly** - Displays an extra section where you can specify the day on which you want the scan to occur on a monthly basis. Enter the day of the month on which you want the scan to occur. The scan will be performed on that day in each subsequent month, starting from the indicated date.
- 4 Specify a maximum duration for the scan by selecting the 'Run for ... Hour(s)' check box. Enter the required hours and/or minutes. If the scan has not completed by the specified time span, it will stop. Nothing will be reported after this point.
 - 5 Click **OK** to save the schedule settings.


Actions tab

The Actions tab enables you to specify the actions that should be performed when a rule is triggered.

To define the actions to be taken when a rule is triggered:

- 1 Select the Actions tab in the FileWatch pane:



- 2 Select the check boxes that correspond to the action to be taken if a FileWatch rule is triggered:
 - **Include in reports** - Writes the details of the rule triggering to a log file and to an external database. This option must be selected to view activity data and is selected by default when a FileWatch object is created.
 - **Send an e-mail notification to the administrator** - Sends an e-mail to the system administrator. Select the check box then click the **E-mail format** button to enter details of your e-mail (see ['E-mail messages' on page 51](#) for more details).
 - **Delete the file** - Delete the file on the workstation that has triggered the rule. In addition, related files that are part of the application, and relevant entries in the registry, are also deleted.
 - **Display a warning message to user** - Issues a warning message to the user who is detected as triggering the rule. Select the check box then click the **Message Format** button to enter details of your message (see for ['Warning Messages' on page 52](#) details)
 - **Play sound** - Issues a sound message to the user who triggers the rule. Select the check box and click **Browse** to navigate to your sound file. You can define a *.wav file (containing a pre-recorded message) that will be played on the users workstation when the rule is triggered. Click  to play the sound.

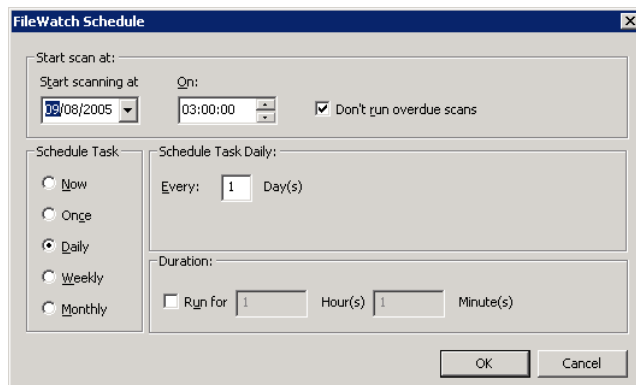
Once you have set up your actions for FileWatch, the selected action(s) will be performed when the rule is triggered.

FILEWATCH AND REMOVABLE DEVICES

FileWatch will include any removable devices attached to the client machine, such as MP3 players and USBs, in its scan. The only evidence of the scanning of these devices will be in the event of a rule being triggered by a file on the device. You will then see evidence of this device in the reports.

Adding devices during a scan

If a scan is in progress when a device is added, the scan will stop and will not restart. The way the scan runs after this point depends on the options that are checked within the Schedule task section of the FileWatch Schedule dialog box.



- **Now** - The reports will show any unauthorized files found up to the point of interruption. A new scan will not be started.
- **Other Schedule task option (Once, Daily, Weekly and Monthly) without 'Don't run overdue scans' checked** - A new scan will be started straight after the interruption.
- **Other Schedule task option (Once, Daily, Weekly and Monthly) with 'Don't run overdue scans' checked** - A new scan will be started at the time dictated by the settings within Schedule task sections. This may not be until a month later if this is what the Schedule task section specifies. This may not be till a month later, if this is what the Schedule task section specifies. For example: If you have scheduled scans to be performed daily at 5.00pm and one of these scans is interrupted, the next scan will not start until 5.00pm the following day.

Removable devices and 'All Local Drives'

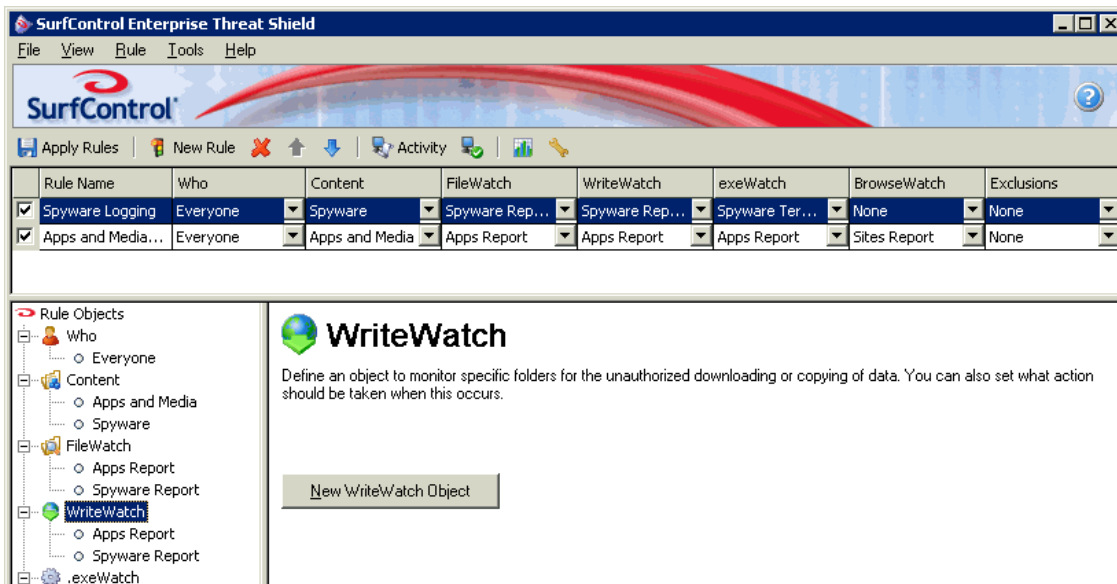
When you select 'All Local Drives' as a search path this will apply to any mobile devices attached to the machine. This means that if you ask FileWatch to delete any files that trigger a rule, files on a mobile device will be included. Before choosing this option, make sure that it is appropriate for FileWatch to delete files off such devices in the event of a rule being triggered.

WRITEWATCH

WriteWatch defines an object that monitors specific file system folders for the downloading or copying of unauthorized files or applications. This enables you to control the loading of applications, music or video files to the computer or a defined disk area. Unauthorized media files and file sharing programs are caught, regardless of how they attempt to enter the network, whether by a P2P application, e-mail, Instant Messenger, or even a CD brought from home.

An action can be triggered so that a report is sent to the system administrator or manager when a user attempts to download an unauthorized file or application. WriteWatch uses signature databases to identify the files and applications that should be controlled, as defined by the Content object used by a rule. See [“Content” on page 30](#).

Figure 2 - 8 The WriteWatch screen



ADDING WRITEWATCH OBJECTS

Before you can configure an object, you need to add it:

To add a new WriteWatch object:

- 1 Select WriteWatch in the Threat Shield objects tree.
- 2 Click **New WriteWatch Object** in the WriteWatch pane. The new object will appear in the Threat Shield objects tree beneath the WriteWatch node.
- 3 Enter a name for the object. You will now see the WriteWatch configuration screen. This screen appears when:
 - You select an existing WriteWatch object from the Rule Objects tree.
 - You add a new WriteWatch object.
- 4 You now need to configure this object. See the following section for information on how to do this. To edit an existing object select it from the Threat Shield objects tree to see it's corresponding object pane.

CONFIGURING WRITEWATCH OBJECTS

Once you have added a WriteWatch object, use the configuration panel to define its behavior. The panel is comprised of two tabs:

- **WriteWatch Tab** - Enables you to specify the folders that should be monitored, and how frequently scanning should occur.
- **Actions Tab** - Enables you to specify the actions that should be performed when a folder is detected that triggers a rule.

WriteWatch tab

The WriteWatch tab enables you to specify which folders should be monitored:

Figure 2 - 9 The WriteWatch tab



To define the folders to be monitored:

- 1 In the left-hand pane of the Threat Shield Manager double-click WriteWatch to see the WriteWatch pane.
- 2 Expand the branch beneath WriteWatch and select the object you wish to configure. You will now see the object's configuration pane.
- 3 Use the buttons within the WriteWatch pane to add, edit or remove the path to the folders that you want to be monitored.
 - **Add** - A dialog box appears that enables you to add a search path to the folder to be monitored. There are two options:
 - **All Local Drives** - All the drives of the local computer will be monitored. This will include any removable drives attached to the machine such as USB and MP3 players. If you set Threat Shield to delete files on 'All Local drives' you must be aware that files on this type of device will also be deleted.
 - **Path** - Select any local path. You can also add a path that includes an environment variable, in case the path is not absolute throughout the organization, for example, %windir%\system32.
 - **Edit** - Edit the search path to the selected file.
 - **Remove** - Remove the search path to the selected file.

- 4 Select a check box if you want WriteWatch to check for compressed files, or stop writing to removable drives:
 - **Check compressed files** - Select the check box to have WriteWatch check files of this type even if they are in compressed format. This will display a window which enables you to report on password protected archive files that are copied to the local disk.
 - **Do not allow writing to removable drives** - Select the check box to stop writing of information to any removable drive that is attached to the client. See the following section for more details

REMOVABLE DRIVE DATA LOSS PROTECTION

Enterprise Threat Shield can prevent the writing of data from the workstation to any removable drives that are attached to it. This helps to prevent the copying of confidential data to a mobile device. Once this option is selected, any write activity to removable drives will be treated in the way specified in the Actions tab, by default this will be a termination of the write activity and the generation of a report.

There are a few things to remember when enabling this feature:

- The rule enforcing this must be the first rule in the list and therefore have top priority.
- Any drives subsequently added, will be recognized and monitored without further configuration.
- Any exclusion set up for files and folders relating to this WriteWatch object will be ignored. Users, workstations and groups can still be excluded.
- If a media file is being copied to the drive, the media threshold size will be ignored.
- You do not need to add a Content object to a rule using this feature.

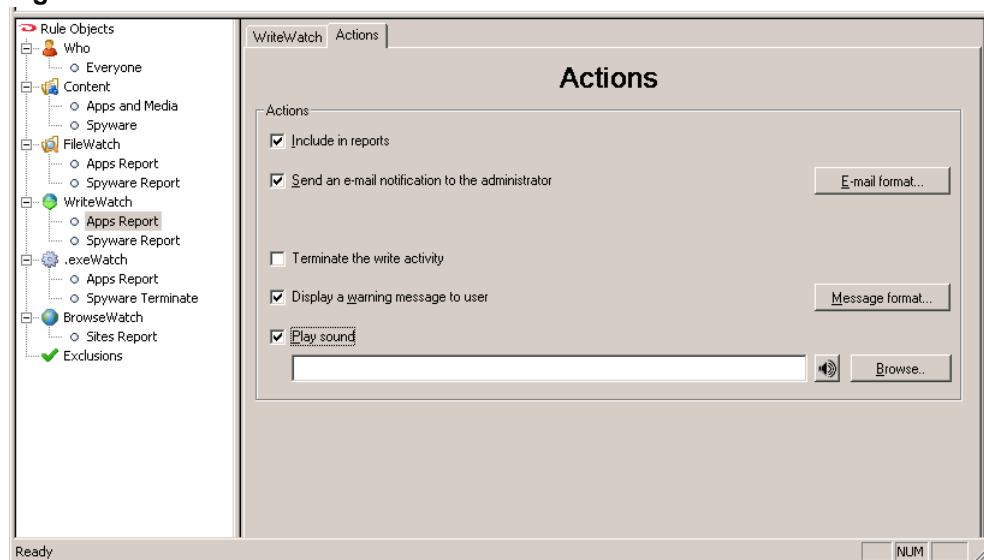
Actions Tab


The Actions tab enables you to specify the actions that should be performed when a rule is triggered.

To define the actions to be taken when a rule is triggered:

- 1 Select the Actions tab in the WriteWatch pane.

Figure 2 - 10 The Actions tab



- 2 Select the check boxes that correspond to the action to be taken if a WriteWatch rule is triggered.
 - **Include in reports** - Writes the details of the rule triggering to a log file and to an external database. This option must be selected to view activity data and is selected by default when a WriteWatch object is created.
 - **Send an e-mail notification to the administrator** - Sends an e-mail to the system administrator. Select the check box then click the **E-mail format** button to enter details of your e-mail (see [‘E-mail messages’ on page 51](#) for more details).
 - **Terminate the write activity** - Stops the downloading or copying of the file.
 - **Display a warning message to user** - Issues a warning message to the user who is detected as triggering the rule. Select the check box then click the **Message format** button to enter details of your message (see below for more details)
 - **Play sound** - Issues a sound message to the user who triggers the rule. Select the check box and click **Browse** to navigate to your sound file. You can define a *.wav file (containing a pre-recorded message) that will be played on the users workstation when the rule is triggered. Click  to play the sound.
- 3 Once you have set up your actions for WriteWatch, the selected action(s) will be performed when the rule is triggered.

.EXEWATCH

.exeWatch manages the use of any application that you specify. It enables you to create access policies and procedures for games, MP3 file swapping applications, instant message applications, spyware or any other applications operating on your network. Access to these applications can be permitted but managed by time or data limits.

Enterprise Threat Shield automatically monitors individual workstations and network servers to detect the applications that are currently running on the workstations. Threat Shield Agent compares them with the applications in its databases. When unapproved use is detected, the agent can block the application, delete its files, display a warning message, and/or report to the server.

.exeWatch uses the same signature databases as FileWatch and WriteWatch to identify the applications that should be controlled, as defined by the Content object used by a rule.

Figure 2 - 11 The .exeWatch screen



ADDING .EXEWATCH OBJECTS

Before you can configure an object, you need to add it:

To add a new .exeWatch object:

- 1 Select .exeWatch in the Threat Shield objects tree.
- 2 Click **New .exeWatch Object** in the .exeWatch pane. The new object will appear in the Rule Objects tree beneath the .exeWatch node.
- 3 Enter a name for the object. You will now see the .exeWatch configuration screen. This screen appears when:
 - You select an existing .exeWatch object from the Rule Objects tree.
 - You add a new .exeWatch object
- 4 You now need to configure this object. See the following section for information on how to do this. To edit an existing object select it from the Rule Objects tree to see it's corresponding object pane.

CONFIGURING .EXEWATCH OBJECTS

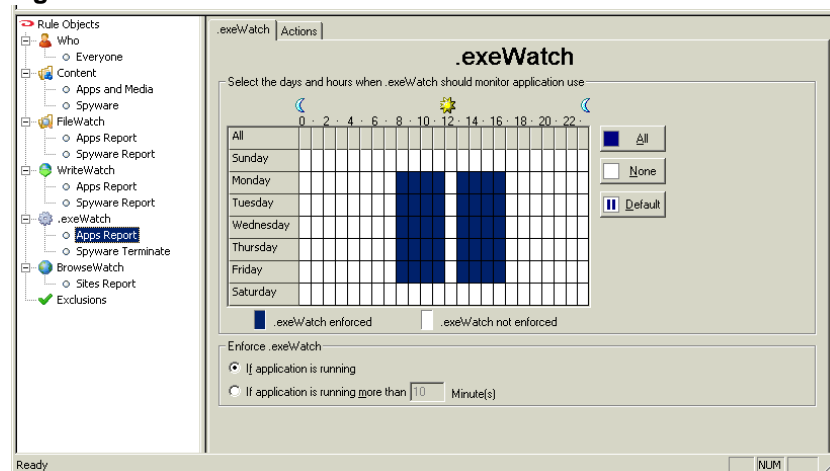
Once you have added an .exeWatch object you can use the configuration panel to define its behavior. The panel is comprised of two tabs:

- **.exeWatch Tab** - enables you to specify at what times the rule should be enforced, and to what extent application use may be allowed during that time.
- **Actions Tab** - enables you to specify the actions that should be performed when application use that triggers a rule is detected.

.exeWatch tab




The .exeWatch tab enables you to restrict the use of applications:

Figure 2 - 12 The .exeWatch tab



The .exeWatch grid area represents all the days and hours of the week. A shaded cell indicates a specific day or hour during which the rule is enforced. An unshaded cell indicates that the rule is not enforced during that specific day and/or hour.

To define specific hours and/or days that the rule should be enforced:

- 1 Click .exeWatch to see the .exeWatch screen.
 - 2 Expand the branch beneath .exeWatch and select the object you wish to configure. You will now see the object's configuration pane.
 - 3 You will now see the .exeWatch time grid. Click the buttons to shade the time grid or click inside a cell:
 - Click inside a cell to shade or unshade that cell. This will enforce or disable the rule for that particular hour or day.
 - Click a cell in the All row to shade or unshade all cells representing that particular hour of each day of the week
-  Shades the entire grid area. This will apply the rule during every hour of every day.
 -  Clears the entire grid area. The rule will not apply at any time.
 -  Shades the cells representing default business hours. This will apply the rule during business hours only.

- **If application is running** - The rule will be triggered as soon as the application starts up.
- **If application is running more than <minutes> Minute(s)** - The rule will be triggered when the application has been running for longer than the time set.

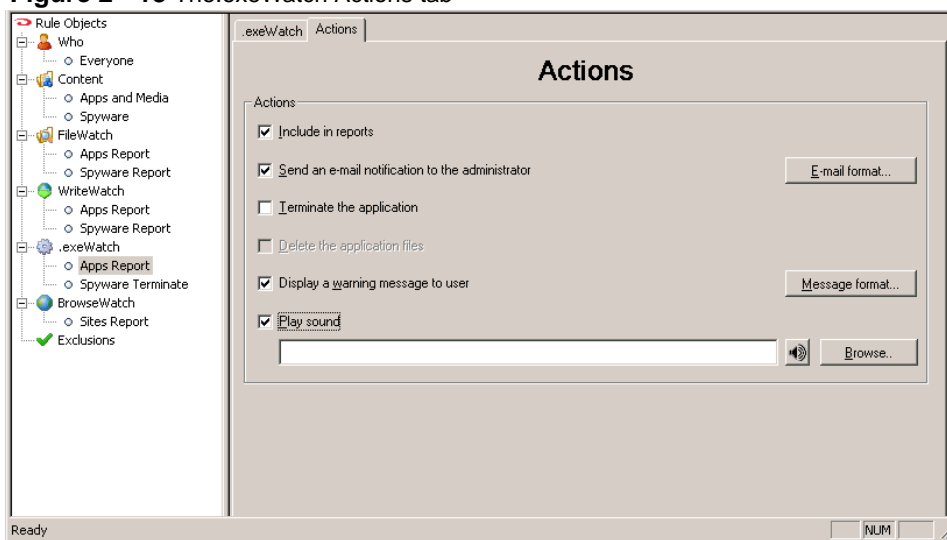
Actions Tab

The Actions tab enables you to specify the actions that should be performed when application file use triggers a rule.

To define actions to be taken when a rule is triggered:

- 1 Click the **.exeWatch** object in the Threat Shield objects tree to see the Actions tab.

Figure 2 - 13 The.exeWatch Actions tab



- 2 Select the check boxes that correspond to the action to be taken if an .exeWatch rule is triggered:
 - **Include in reports** - Writes the details of the rule triggering to a log file and to an external database. This option must be selected to view activity data and is selected by default when a FileWatch object is created.
 - **Send an e-mail notification to the administrator** - Sends an e-mail to the system administrator. Select the check box then click the **E-mail format** button to enter details of your e-mail (see [‘Defining Message Formats’ on page 51](#) for more details).
 - **Terminate the application** - Blocks the application, stopping it from launching.
 - **Delete the application files** - Deletes the unauthorized application files on the workstation that has triggered the rule. In addition, related files that are part of the application and relevant registry entries are also deleted. Select the ‘Terminate the application’ check box to enable this option.
 - **Display a warning message to user** - A warning message is issued to the user who is detected as triggering the rule. Select the check box then click the **Message format** button to enter details of your message (see [‘Defining Message Formats’ on page 51](#) for more details)
 - **Play sound** - A sound message is issued to the user who triggers the rule. Select the check box and click **Browse** to navigate to your sound file. Click to play the sound.
- 3 Once you have set up your actions for .exeWatch, the selected action(s) will be performed within the time scale specified in the Enforce .exeWatch section of the.exeWatch tab.

DEFINING MESSAGE FORMATS

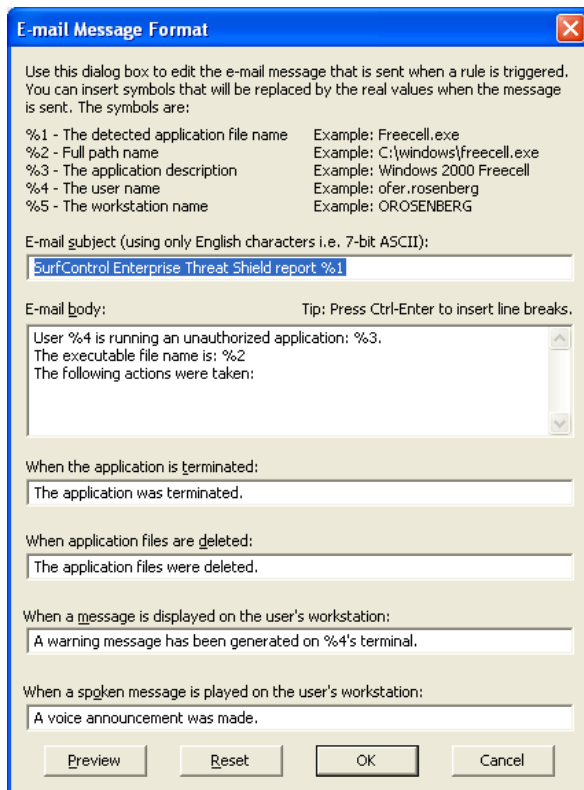
You can set up e-mail and warning messages to either notify the administrator that a user has triggered a rule or to warn the user that they have contravened the organization's Acceptable Usage Policy.

E-mail messages

Enterprise Threat Shield enables you to send an e-mail notification to the system administrator when a rule is triggered. The E-mail Message Format dialog box enables you to edit the e-mail message that will be sent to the administrator to reflect your own organization's policies (in tone and content) and preferred language.

To define E-mail Message format:

- 1 In the Threat Shield Manager objects tree, double-click the object that you want to add a message to. You should now see the object's configuration screen.
- 2 Select the Action tab and click the **E-mail format** button. This will display the E-mail Message Format dialog box:



- 3 Specify the text that will appear in the e-mail message.
 - **E-mail subject** - Enter a subject line for the e-mail. Do not enter anything other than English characters. Any other characters (such as Japanese characters or Unicode) will not be displayed in the E-mail client.
 - **E-mail body** - Enter a message to the administrator, in the format defined in the E-mail body pane. Press <Ctrl><Enter> to introduce a line break.

- **When the application is terminated** - Enter text informing the administrator of this action.
 - **When application files are deleted** - Enter text informing the administrator of this action.
 - **When a message is displayed on the user's workstation** - Enter text informing the administrator of this action.
 - **When a spoken message is played on the user's workstation** - Enter text informing the administrator of this action.
- 4 Enter the required details into the dialog box. You can introduce dynamic content into your e-mail by inserting the symbols shown in the window header. These will be replaced by real values in the e-mail. For example, when you enter %1, the name of a detected file will be reported.
 - 5 Click the **Preview** button to view the e-mail message or click **Reset** to return all settings to their default values.
 - 6 Click **OK**.



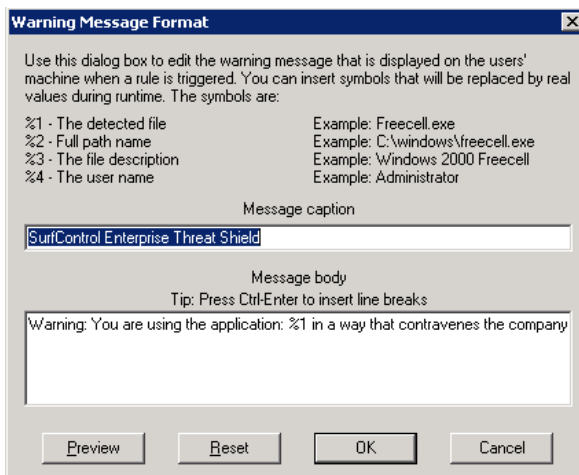
Note: Other e-mail specifications can be set via the Settings dialog box E mail tab. See Chapter 1 "Settings" on page 13.

Warning Messages

Enterprise Threat Shield enables you to generate a warning message that is displayed on the end user's workstation when a rule is triggered. The Warning Message Format window enables you to edit the warning that will be sent to reflect your own organization's policies (in tone and content) and your preferred language.

To define a Warning Message format:

- 1 Click the **Message format** button in the Actions tab to display the Warning Message Format dialog box.



- 2 Specify the text that will appear in the e-mail message.
 - **Message caption** - This appears in the title bar of the message, the default is SurfControl Enterprise Threat Shield.

- **Message body** - Enter a message to inform the user of the fact that they have contravened your organization's Acceptable Usage Policy. Press <Ctrl><Enter> to introduce a line break.
- 3 Enter your required details into the dialog box. You can introduce dynamic content into your message by inserting the symbols shown above the Message caption text field. These will be replaced by real values in the e-mail. For example, when you enter %1, the name of a detected file will be reported.
- 4 Click the **Preview** button to view the e-mail message or click **Reset** to return all settings to their default values.
- 5 Click **OK**.

BROWSEWATCH

BrowseWatch detects the Web sites and Web pages visited during web browsing, then sends this information to the Threat Shield Server. Enterprise Threat Shield's ability to detect surfing activity helps to preserve company productivity, by ensuring that employees do not waste company time and bandwidth with excessive recreational surfing.

BrowseWatch identifies visited sites and how much time was spent at each. Web browsing is detectable when the browser is the foreground window on a workstation.

Unlike other Enterprise Threat Shield detection methods that report activity in real time, Web-browsing activity is logged and reported to the Threat Shield Server at regular intervals, the frequency of which you define.

The BrowseWatch screen is used to specify reporting details for detected Web browsing activity.

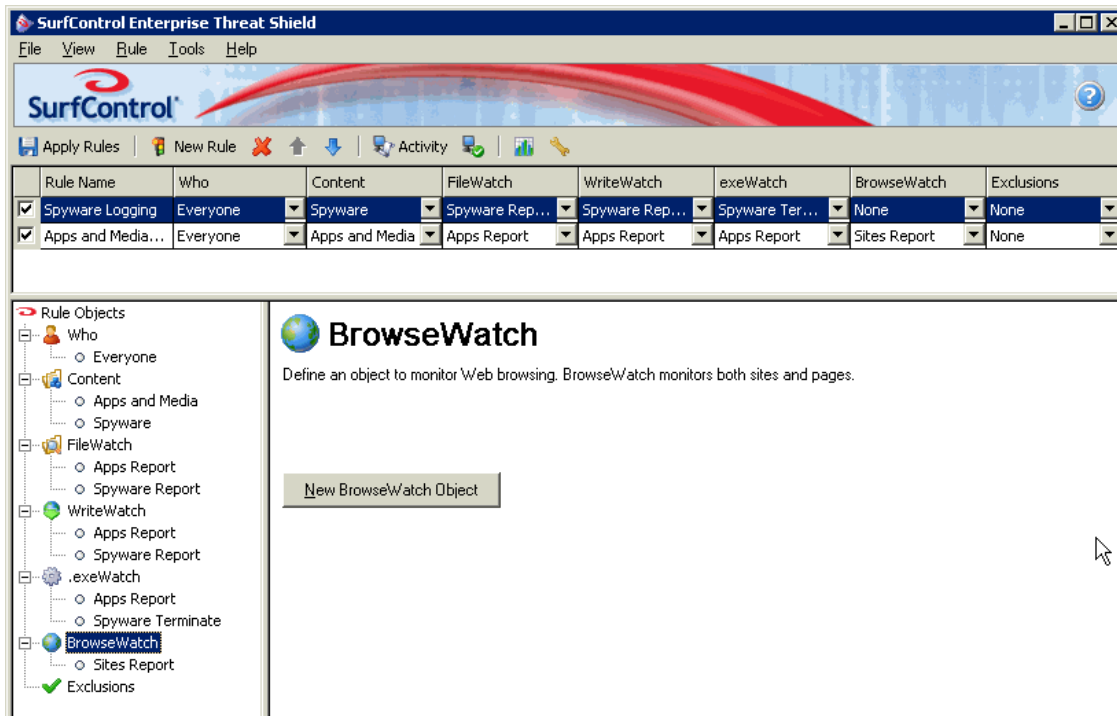


Figure 2 - 14 The BrowseWatch screen

BrowseWatch can monitor most standard browsers. These include:

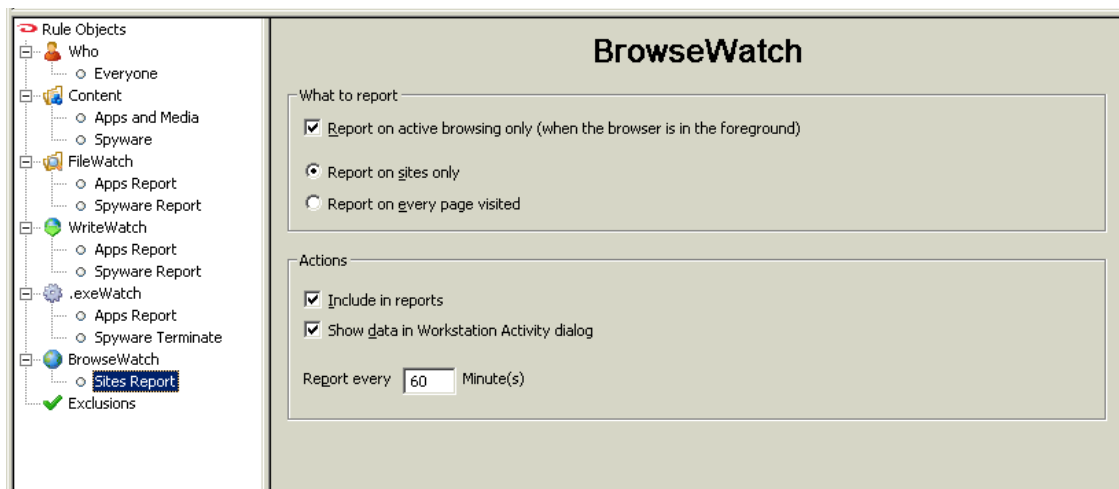
- Internet Explorer
- Netscape (pre Version 8 only)
- MyIE2
- Opera
- Mozilla
- Avant Browser
- FireFox

ADDING BROWSEWATCH OBJECTS

Before you can configure an object, you need to add it.

To add a new BrowseWatch object:

- 1 Select **BrowseWatch** in the Threat Shield objects tree.
- 2 Click **New BrowseWatch Object** in the **BrowseWatch** pane. The new object will appear in the Rule Objects tree beneath the **BrowseWatch** node.
- 3 Enter a name for the object.
- 4 You will now see the BrowseWatch configuration screen:



- 5 This screen appears when:
 - You select an existing BrowseWatch object from the Rule Objects tree.
 - You add a new BrowseWatch object.
- 6 You now need to configure this object. See the following section for information on how to do this. To edit an existing object select it from the Threat Shield objects tree to see it's corresponding object pane.

CONFIGURING BROWSEWATCH OBJECTS

The BrowseWatch pane enables you to specify the actions that should be performed when web browsing triggers a rule.

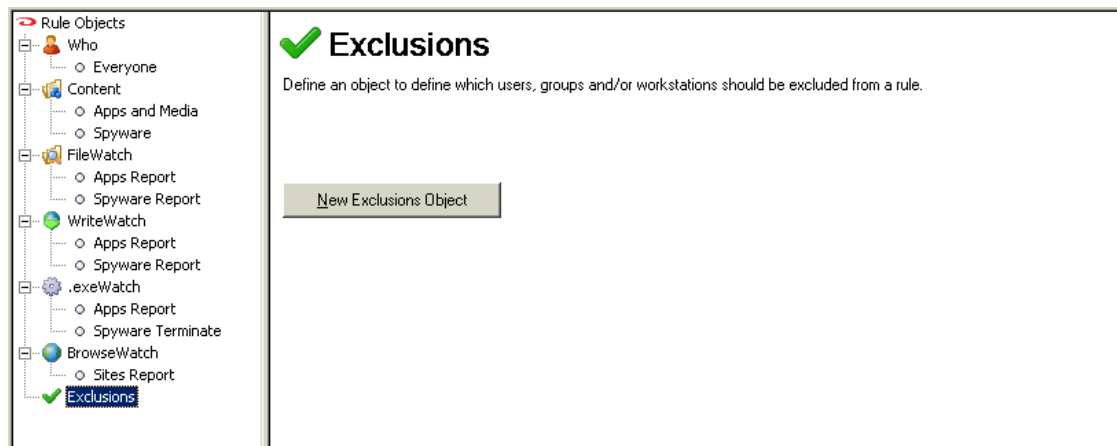
To define a BrowseWatch object:

- 1 Click the BrowseWatch object in the Rule Objects tree.
- 2 Expand the branch beneath BrowseWatch and select the object you wish to configure. You will now see the object's configuration pane.
- 3 Select the 'Report only on active browsing (when the browser is in the foreground)' check box to activate BrowseWatch for the object. This is the default. When selected, web-browsing activity is logged only when the browser is the foreground window. When not selected, all activity is logged while any browser is running.

EXCLUSIONS

The Exclusions screen is used to define objects that specify the workstations, users and groups, as well as files and folders that are to be exempted from a rule's application. By default, only groups and operational units are displayed for this object. To be able to select individual users or workstations, you must make the relevant change in the General tab of the Settings dialog box.

Figure 2 - 15 The Exclusions screen



ADDING EXCLUSIONS OBJECTS

Before you can configure an object you need to add it.

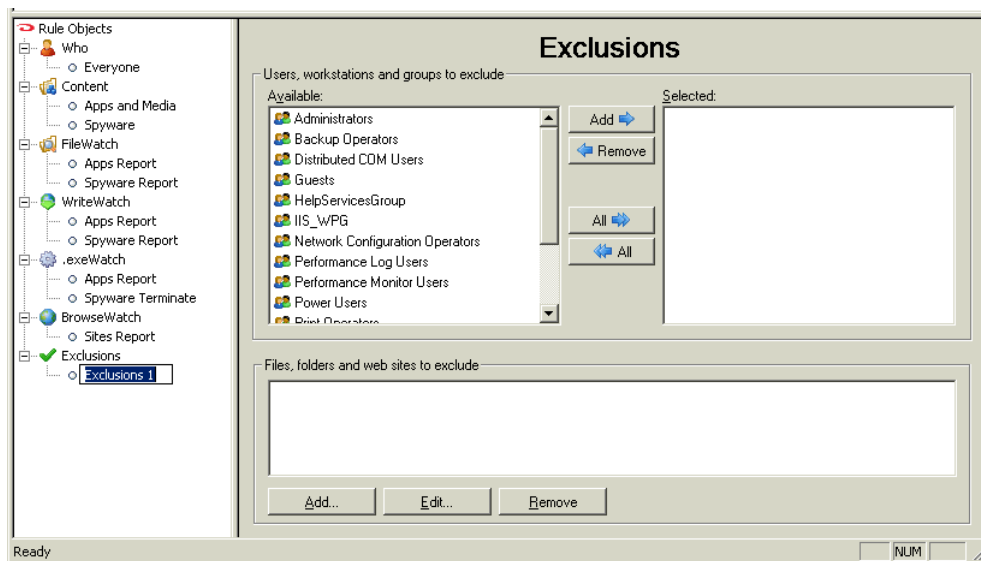
To add a new Exclusions object:

- 1 Select **Exclusions** in the Rule Objects tree.
- 2 Click **New Exclusions Object** in the **Exclusions** pane. The new object will appear in the Rule Objects tree beneath the **Exclusions** node.
- 3 Enter a name for the object.
- 4 You will now see the Exclusions configuration screen. This screen appears when:
 - You select an existing Exclusions object from the Rule Objects tree.
 - You add a new Exclusions object.
- 5 You now need to configure this object. See the following section for information on how to do this. To edit an existing object select it from the Threat Shield objects tree to see it's corresponding object pane.

CONFIGURING EXCLUSIONS OBJECTS





The Exclusions pane enables you to specify the users and groups to which the current policy shouldn't be applied:

Figure 2 - 16 The Exclusions pane



To define an Exclusions object:

- 1 Click the **Exclusions** object in the Rule Objects tree.
- 2 Expand the branch beneath Exclusions and select the object you wish to configure. You will now see the object's configuration pane.
- 3 Select the users or group(s) in the 'Available' pane that you want this Exclusion to apply to then click the corresponding button to add or remove them.

- | | |
|---|---|
|  | Move the selected user or group into the Selected pane. Rules will now apply to this user/group. |
|  | Move the selected user or group into the Available pane. Rules will not apply to this user/group. |
|  | Add all of the Available users or groups to the Selected pane. |
|  | Remove all of the Available users or groups from the Selected pane. |

EXCLUDING FILES, DIRECTORIES AND WEB SITES

The 'Files, Folders and Web sites to exclude' section of the Exclusions panel is used to select the files, directories or Web sites to which any rule containing this object will not apply. For example:

- Select the winmine.exe file to exclude all instances of the winmine.exe file.
- Select the c:\windows\winmine.exe directory path, to exclude only the winmine.exe file that located on your computer under this directory.

2

THREAT SHIELD OBJECTS

Exclusions

- Select c:\windows (without selecting the specific file to ignore), to exclude the entire c:\windows directory from the policy.
- Specify a name using a wildcard to exclude all files containing the designated name. For example, when you specify "Beatles", any file containing the word Beatles is excluded.
- Specify an environment variable, such as %windir%\system 32, to exclude paths that are not absolute throughout the organization.
- Specify a Web site to exclude all browsing to the designated site. For example, specifying *yahoo* excludes all Web pages in which the word yahoo exists. You can also exclude a site by specifying the URL. For example: http://www.yahoo.com, or even a specific page.



Note: Wildcard characters can be included in the file or URL specification (this will not work for directories). For example, winmin*.exe.

To select files and directories to be excluded from the rule:

- 1 In the Exclusions panel 'Files and folders to exclude' area, click **Add**. The Add Item dialog box is displayed.
- 2 In the Enter a new item field, enter the item to exclude or select the item from the displayed navigation windows using the Browse for file or Browse for folder buttons.
- 3 Click **OK**. The selected item is displayed in the Files and Folders to Exclude area.



Note: You can modify or cancel excluded files or directories by clicking the Files and Folder to Exclude area **Edit** or **Remove** buttons.

KEY POINTS

The following list is a summary of the main points covered in this Chapter. Use this list as a quick reminder of what you can do within the Threat Shield Objects section:

- Objects are the building blocks of rules.
- The same object can be applied to multiple rules.
- The Who object must be added to all rules.
- The Content object must be added to all rules unless they are simply a BrowseWatch rule or a WriteWatch rule that is there just to stop writing to removable drives.
- The BrowseWatch object is simply a monitoring object. It does not perform any actions.
- You can create an Exclusions object that enables you to list users you do not want a rule to apply to.

2 THREAT SHIELD OBJECTS

Key Points

Creating and using rules

Overview.....	page 62
The Rules Section.....	page 63
Creating Custom Rules.....	page 66
Managing rules.....	page 68
Key Points.....	page 70

OVERVIEW

This chapter explains how to use the Rules section of the Threat Shield Manager. Once you set up your rules, you no longer need to monitor users individually. As soon as a user triggers a rule, the Threat Shield Agent will take action, and notify you of its actions, if desired.

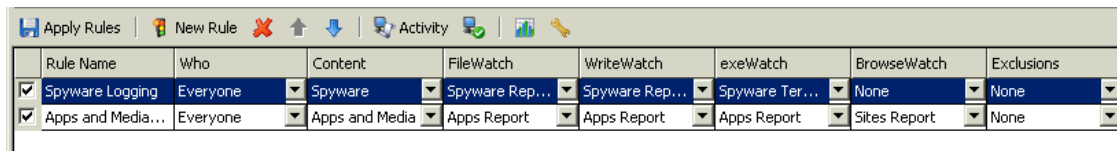
TERMINOLOGY USED

The following terminology is used in this chapter:

- **Threat Shield Agent** - The Threat Shield Agent runs as a stealth application on each workstation and is initiated from the Threat Shield server. The Threat Shield Agent runs as a stealth application on each workstation and is initiated from the Threat Shield server. Users see no evidence of it unless a rule is triggered. This depends on the action set up as a response to this event such as a message being displayed. Threat Shield Agent gathers rule configuration from Threat Shield Manager then uses this to enforce rules when they are triggered. This also happens when an initiated or scheduled scan of the client is performed.” on page 3.
- **Object** - Objects are the building blocks of rules. They are created using the Rule Objects tree and its corresponding panels and define who the rule is to apply to, what it is supposed to look for and where, and what to do if it is triggered.

What can be configured in the Rules Table?

In the Rules Table you can create and configure rules:



	Rule Name	Who	Content	FileWatch	WriteWatch	exeWatch	BrowseWatch	Exclusions
<input checked="" type="checkbox"/>	Spyware Logging	Everyone	Spyware	Spyware Rep...	Spyware Rep...	Spyware Ter...	None	None
<input checked="" type="checkbox"/>	Apps and Media...	Everyone	Apps and Media	Apps Report	Apps Report	Apps Report	Sites Report	None

The Rules Table enables you to:

- Create new rules.
- Configure existing rules by making changes to its objects.
- Add new objects to rules.
- Raise or lower the priority of a rule.
- Enable or disable rules.
- Delete rules that are no longer necessary.

THE RULES SECTION

The Rules Table section of the Threat Shield Manager is where you set up your rules. It lists all of the currently defined rules:

Figure 3 - 17 The Rules section

Rule Name	Who	Content	FileWatch	WriteWatch	exeWatch	BrowseWatch	Exclusions
<input checked="" type="checkbox"/> Spyware Logging	Everyone	Spyware	Spyware Rep...	Spyware Rep...	Spyware Ter...	None	None
<input checked="" type="checkbox"/> Apps and Media...	Everyone	Apps and Media	Apps Report	Apps Report	Apps Report	Sites Report	None

DEFAULT RULES

Enterprise Threat Shield is supplied with two rules by default. These two rules deal with the two aspects of filtering that are the most important to your organization: core and productivity:

- **Core rules** - Prevent activity that puts the company at risk, from breaches in security and confidentiality.
- **Productivity rules** - Prevent users from wasting time with excessive surfing. They also prevent users from taking up valuable network space by downloading and running applications such as MP3, messenger programs and P2P applications.

You will see these two rules in place when you first open the Threat Shield Manager:

Spyware Logging rule

This is a core rule. It is supplied so that Enterprise Threat Shield can monitor spyware and malicious applications as soon as it is installed and the Agents deployed, with no configuration necessary. The Spyware Logging rule contains five objects which work together to provide protection as follows:

- **Who** - The Who object specifies 'Everyone'. The rule will apply to everyone on the network who has the Threat Shield Agent running on their machine.
- **Content** - The Content object is set to use the Spyware Shield database. This database is continuously updated and contains thousands of signatures of spy ware components. It is based on a unique, unalterable stamp which ensures that spy ware can be detected even if it has been disguised using renaming, or compression. For detailed information about what this database contains, visit <http://www.surfcontrol.com/> where you will find a link to a list for SpyWare Shield in the Dynamic Threat Database pages.
- **FileWatch** - The FileWatch object is set to search for Spyware files that have been stored on any of the drives on the users workstation. It will look for all files, including those that have been compressed, and log any that are found. This scan will be run every day automatically.
- **WriteWatch** - The WriteWatch object is set to search for Spyware files being written to any of the drives on the workstation. It will look for all files, including those that have been compressed. If it discovers a Spyware file being written to one of these drives, it will stop the writing activity and log that this activity has taken place.
- **.exeWatch** - The .exeWatch object is set to monitor the workstation all of the time so the Spyware Logging rule will be enforced no matter what time of day or night Spyware is run, or saved to the workstation.

Because the objects are set to report if the rule is triggered, you can see what they have detected and the action that was taken by running a report using the Threat Shield Reporter. See [Chapter 4 'Threat Shield Reporter' on page 71](#) for details on how to use the Reporter.

How the Anti-Spyware Logging rule protects your system. As soon as the user logs into their workstation the Agent initiates then contacts the Threat Shield Server. It will then:

- 1 Download all of the rules relating to this user, including any containing groups that this user is a member of.
- 2 The FileWatch object will scan all of the specified drives and report on any Spyware files it finds.
- 3 If a Spyware file is found, the .exeWatch object will block it before it starts to run.
- 4 The rule will remain active and will trigger if and when the user attempts one of the following:
 - They try to run one of the Spyware files that FileWatch found - .exeWatch will block the application (it will not be able to start) and log the action.
 - They try to download a file containing an item that is included in the Spyware database - the objects will work in the following way:
 - FileWatch will detect that the file contains this item and report on it.
 - WriteWatch will stop the data from being copied to the workstation and log the action.
 - .exeWatch will block any Spyware files attached to the data, so they cannot initiate.

This rule will be active at all times while this user is logged in.

Apps and Media Logging rule

This is a productivity rule. It is supplied so that Enterprise Threat Shield can help you manage how users use the Internet and the space they take up with inessentials, such as music and audio files. It will work as soon as Threat Shield is installed and the Agents deployed, with no configuration necessary. The Apps and Media Logging rule also reports on the user's web browsing activity, so you can ensure they are not wasting time with excessive surfing. It contains six objects which work together to provide protection as follows:

- **Who** - The Who object specifies 'Everyone'. The rule will apply to everyone on the network who has the Threat Shield Agent running on their machine.
- **Content** - The Content object is set to use three databases: Game Shield, Messenger Shield and P2P Shield. These databases are continuously updated, and between them protect against over-use of messenger, file-sharing and gaming applications. For detailed information about what these databases contain, visit <http://www.surfcontrol.com/>. Follow the Adaptive Threat Intelligence link to navigate to lists for the three Shields in the Dynamic Threat Database pages.
- **FileWatch** - The FileWatch object is set to search for any files that are listed in the three databases and stored on any of the drives on the users workstation. It will look for all files, including those that have been compressed, and log any that are found. This scan will be run every day automatically.
- **WriteWatch** - The WriteWatch object is set to detect any Application files that are included in the three databases and being written to any of the drives on the workstation. If it discovers any of these files being written to one of these drives, it will log that this activity has taken place so you can see it in the Workstation Activity window.
- **.exeWatch** - The .exeWatch object is set to monitor the workstation during work hours so the Apps and Media Logging rule will be enforced during the times that your users are supposed to be working. The default time is from 8.00am till 12.00pm then 1.00pm to 4.00pm. Outside this time the applications

in these three databases will be allowed to run without the rule being triggered. This allows users to use these applications during non-working hours. Any attempt to run these applications at other times will be logged.

- **BrowseWatch** - To ensure you have full protection, a BrowseWatch object has been added to the Apps and Media Logging rule. This object is set to monitor your users' Web browsing at all times. It reports on any Web sites they visit, although only when the Browser is active (i.e. they are actively surfing). This information is recorded to the database and log files and you can see this data in the Workstation Activity window and in any reports you decide to run.

Because the objects are set to report if the rule is triggered, you can see what they have detected and the action that was taken by running a report using the Threat Shield Reporter. See [Chapter 4 "Threat Shield Reporter" on page 71](#) for details on how to use the Reporter.

How the Apps and Media Logging rule protects your system. As soon as the user logs into their workstation the Agent initiates and contacts the Threat Shield Server. It will then:

- 1 Download all of the rules relating to this user including any rules containing groups that this user is a member of.
- 2 The FileWatch object will scan all of the specified drives and report on any Apps and Media files it finds.
- 3 The rule will remain active from 8.00am to 12.00pm and 1.00pm to 4.00pm. Within this time frame, it will trigger if, and when, the user attempts one of the following:
 - They try to run one of the Apps and Media files that FileWatch has found.
 - They try to download a file containing an application that is included in the one of the three Apps and Media databases.

This rule will be active within the time limits set by .exeWatch. while this user is logged in.



Note: You can edit both of the default rules to suit your own circumstances. For example, you may want to change the working times in the .exeWatch object, because it doesn't reflect your working hours, or ask FileWatch to look at different drives than those specified. See [Chapter 2 "Threat Shield Objects" on page 25](#) for details on editing these objects.

SurfControl recommends that you do not remove the default rules and try to leave them in their original state as far as is practical. This ensures you will always have protection from Spyware and unwanted application/media files at all times.

CREATING CUSTOM RULES

Custom rules enable you to fine-tune protection so that every eventuality is covered, in a way that best suits your company. Rules can be created to suit specific end users, workstations, departments or the entire company.


Before you start to create a rule, spend some time thinking about what you want the rule to achieve. Is it going to be something that will apply to the whole company, or is it going to be set up to solve a particular problem, such as a user downloading an excessive amount of mp3 files onto their computer.

All of the objects that you can create relate to a specific point in the search for unauthorized files by specifying who to look for, what files are being downloaded or run and when this is happening. Using these building blocks you can create a rule that is very precise in its action.

THE RULES TABLE

Rules are created using the Rules Table at the top of the Threat Shield Manager:

Figure 3 - 18 The Rules section



Rule Name	Who	Content	FileWatch	WriteWatch	exeWatch	BrowseWatch	Exclusions
<input checked="" type="checkbox"/> Spyware Logging	Everyone	Spyware	Spyware Rep...	Spyware Rep...	Spyware Ter...	None	None
<input checked="" type="checkbox"/> Apps and Media...	Everyone	Apps and Media	Apps Report	Apps Report	Apps Report	Sites Report	None

Each line in the table is a rule. Each rule contains the following elements:

- **Activation check box** - When you create a new rule this is automatically checked. This means that the rule is active and will run within the parameters that you have set for it. If you uncheck this check box the rule will be disabled and will not run.
- **Rule Name** - The name of the rule, which should be a name that easily identifies it in the Workstation Activity window and reports. See [‘Rename a rule’ on page 68](#).
- **Object selection drop down lists** - Each column represents an object from the Rule Objects tree. As you create new objects they are automatically added to their respective list. One object can be added to multiple rules, you do not have to create a new object for each rule. See [Chapter 2 ‘Threat Shield Objects’ on page 25](#) for detailed information on how to create objects.

DESIGNING A RULE


Think about the rule logically. This is made easier by the way the rules are set out in the Rules Table. Ask yourself:

- 1 Who do I want this rule to apply to? Set up your Who object to list these users/groups.
- 2 What files or applications do I want the rule to look for? Set up a Content object to define these files.
- 3 What should this rule do when it finds files of this type on the workstations of the users in the Who object? Define the objects relating to what you want the rule to do:
 - Do I want the rule to scan for the files that are included in the Content? If yes, set up a FileWatch object to define the level of search, where to look for these files and what to do if they are found.
 - Do I want to stop the downloading and copying of the files that I added to the Content object? If yes, set up a WriteWatch object to define where to check for this activity and what to do if it is discovered.

- Do I want to stop the applications in the Content object from running, or at least monitor them. Or do I want to allow them to run, but only at certain times? If yes, set up an .exeWatch object that defines when they can be run and what to do if they are run outside the specified time.
- Do I want to monitor the browsing activity of the users listed in the Who object? If yes, set up a BrowseWatch object to define the level of monitoring and reporting.
- Are there any users belonging to groups that are included in the Who object who I do not want this rule to apply to? If so, set up an Exclusions object that lists these users.

PUTTING THE RULE TOGETHER

Once you have created all of the objects that you need, you can start to build your rule:

- 1 Select New Rule from the File menu or click the **New Rule** toolbar button .
- 2 The rule will appear at the bottom of the rule list, and will be called 'Rule...' then a number. Double-click its name and enter a more descriptive name. This is important, as you need to be able to recognize the rule in the Workstation Activity window, and in any reports you subsequently run.
- 3 The Who column in this rule will be set to 'Everyone' as this is the default. Click the arrow to open up the Who list and choose the Who object you created earlier.
- 4 The Content column in this rule will be set to 'None'. Click the arrow to open up the Content list and choose the Content object you have just created.
- 5 Continue to choose objects from each of the columns until you have included all of the objects you need.
- 6 Once you are satisfied that your rule contains all of the information it needs, click **Apply Rules** to transmit this new rule to the Threat Shield Agents.

RULE PRIORITY

When the Agent identifies a file or application, it checks the rules list and works from top to bottom. If the file does not trigger the first rule, it will check the next, and so on until it has completed the list, or a rule is triggered. Once this happens, the Agent will stop the process and no more rules will be checked until another file is detected.

EXAMPLE

The Agent only downloads the rules that apply to the user or machine that it is running on. A user might have four rules that apply to him, on his machine. If Rule 1 triggers then rules 2, 3 and 4 will not be checked. The Agent will simply carry out the action defined in the objects attached to this rule, then stop.

If this user then downloads a file that is included in Rule 3 and not in 1 and 2, then 1 and 2 will run before the Agent triggers Rule 3. Rule 4 will not be checked because Rule 3 has been triggered.

This means that the arrangement of rules in the list is quite important. For example, if you are asking for a report on a user downloading a particular type of file, you need to make sure that this rule is at the top of the list. This ensures that the first rule to trigger will be the rule attached to this file and the other rules will only be actioned if this file is not found.



Note: If you set up a rule with the 'Prevent data being copied to removable drives (Removable Drive Data Loss Protection)' option set within a WriteWatch object, you must make sure that this rule is the first within the Rules grid. This will give it priority over other rules and enable it to work correctly.

MANAGING RULES

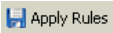
Once you have created your rules you can manage them in the following ways:

- Enable or disable a rule
- Rename a rule
- Change a rule's priority
- Delete a rule

ENABLE OR DISABLE A RULE

You can switch rules on or off by selecting or deselecting the Activation check box alongside the rule. Once a rule is disabled it will not be downloaded by the Agents. If you activate a disabled rule, you must apply the rules to transmit this new configuration to the Agents. The Agents on the workstations of the users that this rule applies to will then download this rule and apply it to their users. By default all rules are checked and therefore enabled.

To disable a rule:

- 1 Deselect the check box alongside the rule.
- 2 Click the **Apply Rules** button  or choose Apply Rules from the File menu. The rule will no longer be triggered when the Agent detects a file that it is set to search for.

To switch this rule back on, select the check box and apply the rules.

RENAME A RULE

When a new rule is added, it is assigned a default name comprising "Rule" plus a digit. For example, the first rule is assigned the default name Rule #3, because it appears after the two default rules. This default name should be changed to a name that is more informative.



To rename a rule:

- 1 In the Threat Shield Manager Rules section, double-click in the Rule Name field that you want to change.
- 2 A cursor will appear in the field. Change the rule name to the one required.
- 3 Click anywhere else in the window to save the change

CHANGE A RULE'S PRIORITY

Each new rule that is added is automatically placed at the bottom of the Rules table, implying the lowest priority. If required, you can change any rule's priority by moving it up or down in the Rules table, as described below. See ['Rule priority' on page 67](#) for more information on how rule priority works.

To change a rule's priority:

- 1 Open the Threat Shield Manager and select the rule you want to move.
- 2 Click one of the Rule Priority buttons to move the rule up or down:
 - Click  or select **Rule > Raise rule priority** to move the rule up the table.
 - Click  or select **Rule > Lower rule priority** to move the rule down the table.

CHANGE A RULES CONFIGURATION

To change the action of an existing rule:

- 1 Identify which rule you need to make changes to.
- 2 Use the table below to help you decide which of the objects, in this rule, you need to make changes to:

Table 3 - 1 Tasks and which objects they apply to


Task	Object	Tab
Change the users or groups that the rule will apply to.	Who	NA
Change the types of file and application that will be looked for.	Content	NA
Change the paths that will be scanned for stored unauthorized files.	FileWatch	FileWatch tab
Change the time that these scans will take place.	FileWatch	FileWatch tab > Schedule... button
Change the paths that will be scanned for the downloading or unauthorized files.	WriteWatch	WriteWatch tab
Prevent data being copied to removable drives	WriteWatch	WriteWatch tab
Change the time that an application is allowed to run.	.exeWatch	.exeWatch tab
Stop an application from running.	.exeWatch	.exeWatch tab
Change the level of monitoring of users surfing behavior.	BrowseWatch	NA
Change the action taken when a rule is triggered.	The Action tab of the corresponding object.	

- 3 Once you know which object you need to change and the name of this object, select it in the Rule Objects tree.
- 4 Make the required changes to the object. For more information on how to make changes to objects see [Chapter 2 "Threat Shield Objects" on page 25](#).

DELETE A RULE

If you no longer need a rule, you can delete it from the Rules section of the Threat Shield Manager.

To delete a rule:

- 1 Open the Threat Shield Manager and select the rule you want to delete.
- 2 You can use any of the following methods to delete the rule:
 - Click the **Delete selected rule** toolbar icon .
 - Select Delete from the Rule menu.
 - Place the cursor on the rule in the Rules table and press the <Delete> keyboard key.



Note: If you don't want to use the rule but think you might need it later, you can just uncheck the check box by the rule to deactivate it.

KEY POINTS

The following list is a summary of the main points covered in this Chapter. Use this list as a quick reminder of what you can do within the Rules Section:

- When a user logs into their machine the Agent initializes, contacts the Threat Shield server and downloads any rules that relate to that user or machine (depending on how you have set up your Who object).
- Always create the objects that you need for your rule before you create the rule itself.
- When you add a new rule it is important to change the default rule name to something that identifies the rule clearly. This is so that you can understand which rule has been triggered and therefore what triggered it
- The arrangement of rules in the list is important. For example, if you are asking for a report on a user downloading a particular type of file you need to make sure that this rule is at the top of the list. This ensures that the first rule to trigger will be the rule attached to this file and the other rules will only be actioned if this file is not found.
- You can change rule priority so that greater emphasis is placed on finding files and applications of a certain type.
- You can delete any rule that is no longer necessary. Alternatively, if you don't want to use the rule but think you might need it later, you can uncheck the check box by the rule to deactivate it.
- You must always have a Who object in a rule plus one of the Watch objects. These include FileWatch, WriteWatch, .exeWatch and BrowseWatch. You also need a Content object, unless this is a BrowseWatch rule which just monitors users' Web browsing.
- If you set up a rule with the 'Prevent data being copied to removable drives (Removable Drive Data Loss Protection)' option set within a WriteWatch object, you must make sure that this rule is the first within the Rules grid. This will give it priority over other rules and enable it to work correctly.

Threat Shield Reporter

Overview	page 72
Launching the Threat Shield Reporter	page 73
Using Threat Shield Reporter	page 74
Key points	page 82

OVERVIEW

This chapter explains how to use the Threat Shield Reporter to run reports and show how your users are using company IT resources. These reports can give you an insight into the types of file they are downloading, running and storing and enables you to manage this activity.

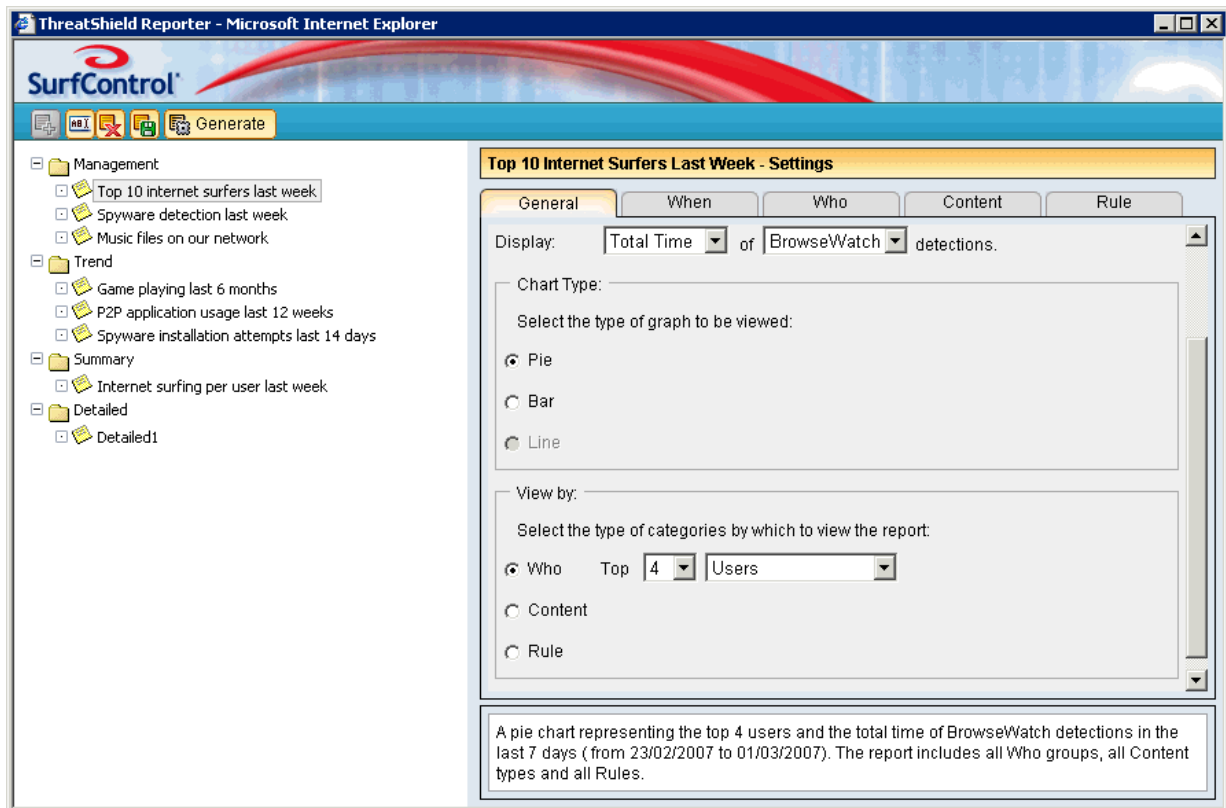
TERMINOLOGY USED

The following terminology is used in this chapter:

- **Parameters** - The specification of what information the report should contain.

WHAT CAN THE REPORTER BE USED FOR?

The Threat Shield Reporter is used to create reports on different aspects of the way your users use the network and internet:



The Threat Shield Reporter enables you to:


- Make decisions about how rules should be set up to control the use of your network.
- See trends in browsing activity.
- See who is triggering the most rules and with what.

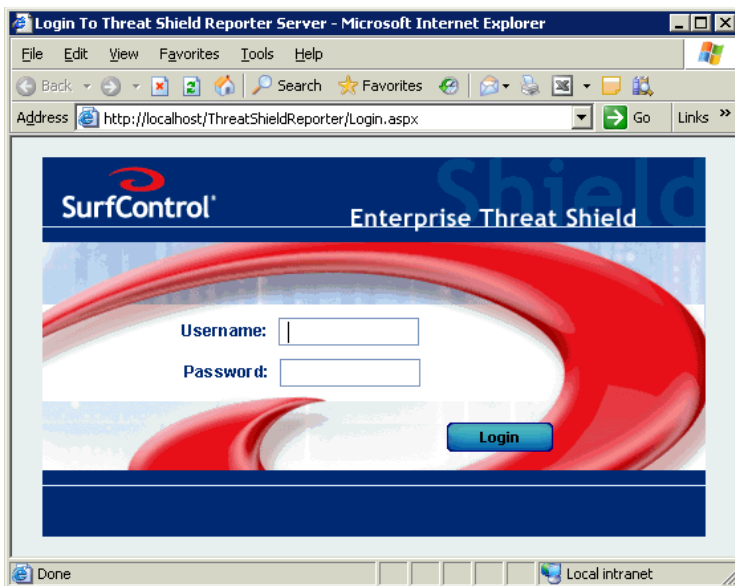
LAUNCHING THE THREAT SHIELD REPORTER

Threat Shield Reporter analyzes the data collected by Threat Shield. It enables you to create a variety of reports that can be displayed in graphical and tabular format. The application is SQL-based, thereby enabling its information to be easily accessed by and integrated with other SQL-based applications.

Threat Shield Reporter is accessed remotely using an Internet browser. Only users that have the correct authorization can log in to the application. This authorization is determined in advance using the Reporter tab in the Threat Shield Manager Settings dialog. All users accessing Threat Shield Reporter can view and configure the same reports. Remote access is available using Internet Explorer V5.5 or higher and permits reports to be viewed by any computer in the Intranet.

To access the Threat Shield Reporter:

- 1 Open a Web browser and enter the following URL:
<http://<hostname / <IP address of machine Threat Shield is installed on>/ThreatShieldReporter>
- 2 You can see the full path in the Reporter tab of the Settings dialog. If you have administrative privileges you can also open the Threat Shield Reporter by clicking  in the Threat Shield Manager. You will now see a Threat Shield login screen:



- 3 Enter your authentication details:
 - **Username** - Enter your user name. The default username is 'admin'.
 - **Password** - Enter the password for this user. The default password is '' (leave the text field blank).
- 4 Click the **Login** button. The Threat Shield Reporter screen will open.

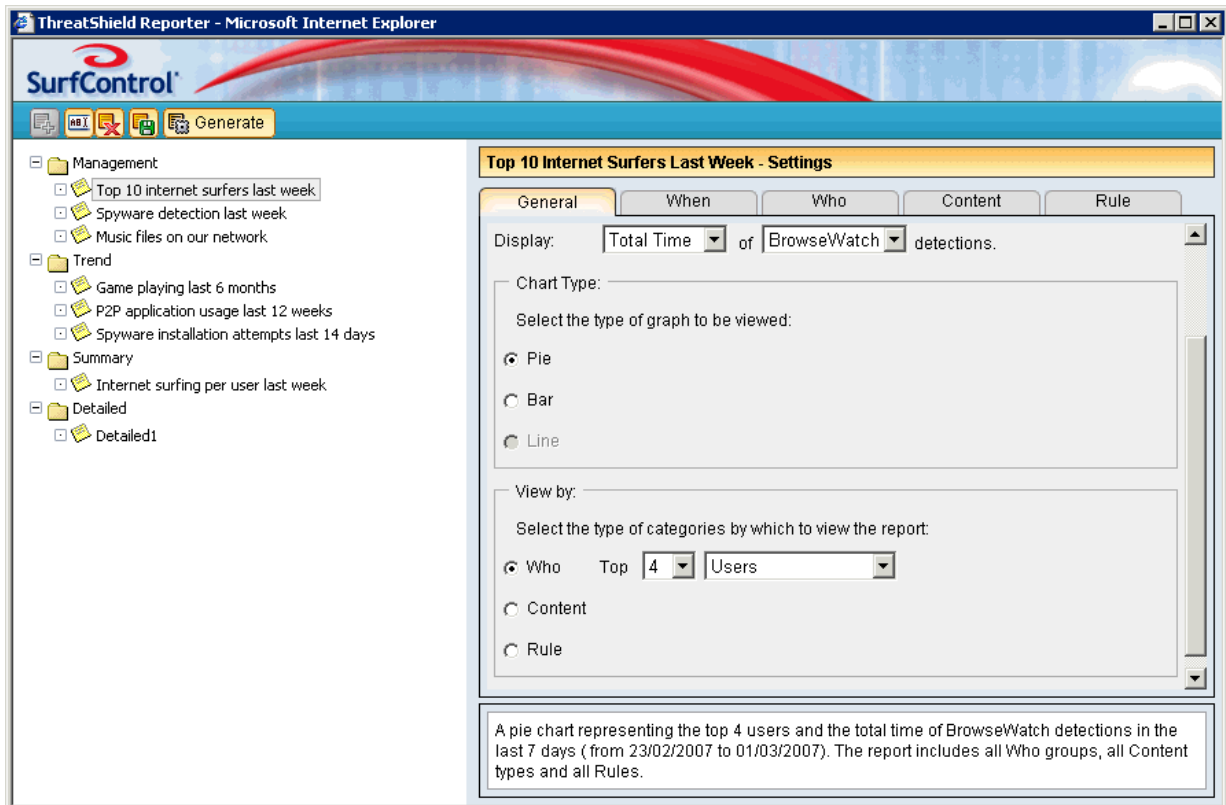


Note: If you start an admin session using the Administrator credentials then close the logon and Reporter windows, the connection will not be dropped until the Active Server Page (ASP) has timed out. This means that if you subsequently log in from a remote machine before the ASP has timed out, you will see a dialog warning that you can view, but not edit, data. Subsequent logins on the same machine will not be affected.

USING THREAT SHIELD REPORTER

After launching Threat Shield Reporter, the application's main window is displayed, enabling you to access all of the Threat Shield Reporter functions.

Figure 4 - 19 Threat Shield Reporter Main Window



The Threat Shield Reporter consists of the following:

- **Report Tree** - Lists the four report types that can be created using Threat Shield Reporter. Clicking a report type branch (for example, the Management Reports branch) lists the reports available for that report type. When a report sub branch is selected, its report definition details are displayed in the Report Definition area.
- **Report Definition Area** - Defines the parameters for the report. This area consists of five tabs, which are used to configure the parameters for the report output.

CREATING A QUICK REPORT






Threat Shield Reporter provides a variety of pre-defined reports with preset default settings. These reports can be run at the click of a button. You can also change a predefined report's settings for a one-time run. All predefined report settings return to their defaults after execution so you can create custom reports specific to your needs. Custom reports are configured just like predefined reports but they can be used only once and are not saved. For more details see [“Configuring Report Parameters” on page 78](#).

Running a quick report

Select the predefined report you want in the Report tree and click the **Generate** button to instantly produce the report. The generated report is displayed in a separate window.

Threat Shield Reporter Toolbars





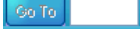




Threat Shield Reporter provides two toolbars for quick access to commonly used operations. The main window toolbar, shown below, contains the following options:

	Adds a new report of the selected type
	Renames a report
	Deletes a report
	Saves the report settings
	Generates the results of the report



Note: All of the toolbar operations are also accessible from the right-click menu when you click on a node in the Report Tree. For users with User access rights, all of the toolbar buttons above are disabled except for the **Generate** button. For more details see [“Access Rights” on page 76](#)

A toolbar is available for quick navigation within a generated report. You can also print a generated report or export it to other external applications, such as Microsoft Word or Excel. The following table contains a brief description of each toolbar option:

	Moves to the first page of the report.
	Moves to the previous page of the report.
	Moves to the next page of the report.
	Moves to the last page of the report.
	Jumps to the page specified in the text box.
	Prints the report.
	Exports the report to PDF format.
	Exports the report to Microsoft Word format.
	Exports the report to Microsoft Excel format.

ACCESS RIGHTS

Threat Shield Reporter has two levels of access right to the application:

- **User** - Users with User access rights can generate and view reports only. This access level cannot save reports for re-use.
- **Administrator** - Users with Administrator access rights can perform the same tasks that a User can, plus additional ones. This access level can create, rename, delete and save reports in the system. Reports created by the Administrator are available to all other users accessing Threat Shield Reporter (those with User access rights). Credentials for this access level are defined in the Reporter tab of the Settings dialog. In addition, the Administrator can select the organizational logo to be displayed at the top of all reports (also defined in the Reporter tab).



Note: Only one Administrator can be logged in at any one time. If more than one user with Administrator access rights attempts to log in to Threat Shield Reporter, only the first user will be able to log in. A warning message is displayed for subsequent users, and they will be denied the connection until the first user logs out.

REPORT TYPES

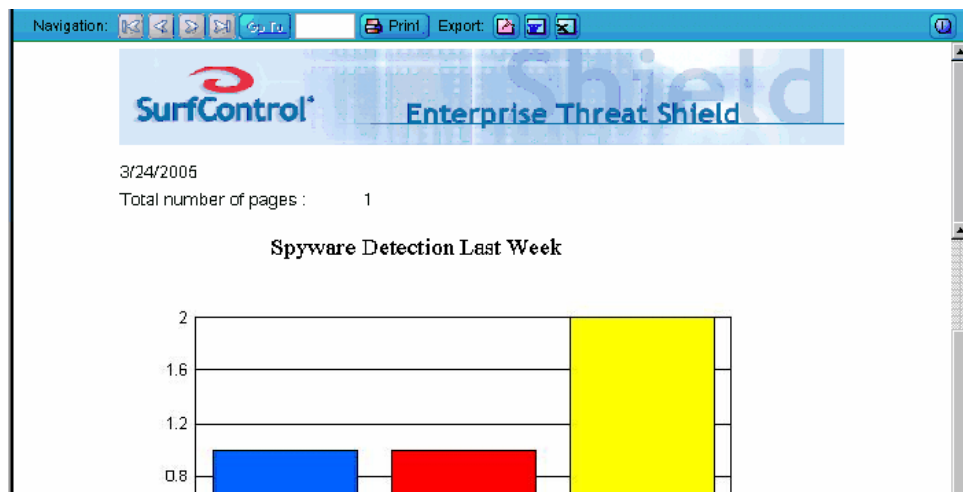
Threat Shield Reporter can produce four different types of reports: Management reports, Trend reports, Summary reports and Detailed reports.

Management Reports

Management reports provide both a graphical and tabular display of data for violations that occur under specific conditions, which you define using available filtering options. Reports of this type are useful for comparing the number of rules triggered by organizational unit. Several predefined Management reports are provided with default settings. In addition, you can create customized reports to meet your specific needs. The following figure shows a sample Management report.

This report shows a bar graph of the top 10 workstations and their total count of .exeWatch detections of spyware during March 11, 2005 up to March 24, 2005. The report includes all Who groups, specific Content types and all rules.

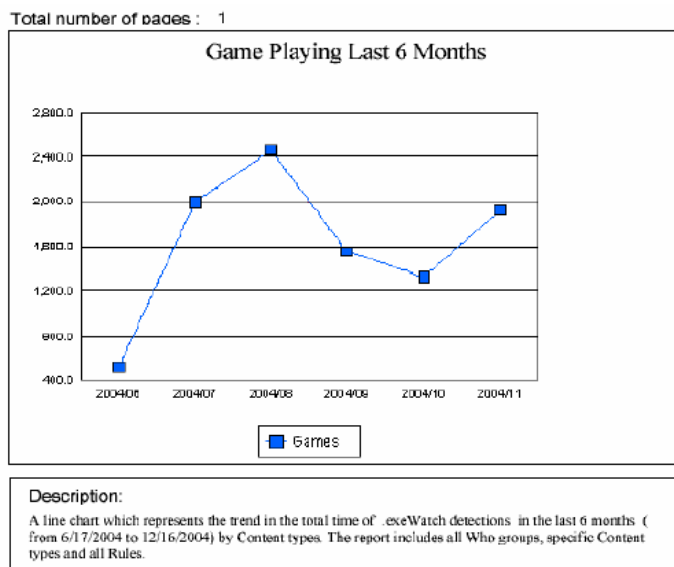
Figure 4 - 20 A Management report



Trend Reports

Trend reports display summary information both graphically, and in table format for rules triggered over time. Several predefined reports are available and you can create customized reports. The figure below shows a sample Trend report. This report presents a line graph showing the total time, in minutes, of .exeWatch detections of games during the six-month period between June 17, 2004 and December 16, 2004. The report includes all Who groups, specific Content types and all rules.

Figure 4 - 21 A Trend report



Summary Reports

Summary reports display aggregate data in tabular format only. A number of predefined reports are available, plus you can create custom reports. The figure below shows a sample Summary report. This report shows the total time, in minutes, for BrowseWatch detections for the top 100 users during the seven day period between January 4, 2005 and January 10, 2005. The report includes all Who groups, all Content types and all rules.

Figure 4 - 22 A Summary reports

1/10/2005

Total number of pages : 1

Description:
A table which summarizes the total time of BrowseWatch detections, per the top 100 users in the last 7 days (from 1/4/2005 to 1/10/2005). The report includes all Who groups, all Content types and all Rules.

Name	Total Time (minutes)
Administrator	13,106
Barbara	8,794
Dan	8,338
David	5,988
Diane	5,581
Donna	5,919

Detailed Reports

Detailed reports show the raw data as it appears in the database, with all relevant technical information, such as the workstation, file name, detection time, and so on. Data for this report type can be filtered, and you can also choose how you want to sort the report's output. No predefined reports are available for this report type. The figure below shows a sample Detailed report. This report presents data for all detected .exeWatch violations in the two week period between December 3, 2004 and December 16, 2004. The report includes all Who groups, specific Content types and all rules.

Figure 4 - 23 A Detailed report

Detailed Report

Description:
 A list of all the record detections by .exeWatch in the last 2 weeks (from 12/3/2004 to 12/16/2004). The report includes all Who groups, specific Content types and all Rules.

Name	Workstation	DetectionTime	FileName	Duration
Diane	diane-pc	12/6/2004 12:46:34P	alexa45.exe	97
Diane	diane-pc	12/5/2004 11:15:34P	alexa16.exe	116
Michal	guest-pc	12/6/2004 9:47:34P	alexa44.exe	37
Michal	guest-pc	12/7/2004 4:10:34A	alexa21.exe	19

Defining Reports

When defining reports in Threat Shield Reporter, you specify how to view report results, how to filter the raw data, and how to sort tabular results. Report parameters are defined in the Report Definition area.


Navigating in a Report

Threat Shield Reporter enables you to quickly and easily navigate within a generated report. For more details about navigation and export options, see [“Threat Shield Reporter Toolbars” on page 75](#).

CONFIGURING REPORT PARAMETERS

When setting up predefined and custom reports, you define the parameters to be used to create these reports. Report parameters are organized within five tabs, as follows:

- General tab
- When tab
- Who tab
- Content tab
- Rule tab

After defining a report's parameters, click the **Generate** button  to run the report. The generated report opens in a separate window. The first page of the report contains descriptive information about the report, such as its run date and number of pages. Reports containing both a chart and text (Management and Trend reports) show the chart first, followed by a description of the report and a data table. The description is generated automatically, based on the parameters specified for the report.

Summary and Detailed reports display a report description followed by a data table. They do not include charts. You can select multiple entities at once using standard Microsoft multi select options.

Defining General Tab Parameters

General tab report parameters specify the detection type to be included in the report and how this data will appear. The following report parameters are defined in this tab:

- **Title** - The title of the report.
- **Display** - The type of data to be displayed. You can choose to display either the Total Count of rules triggered or the Total Time of detected rules triggered. Total Time is relevant only for .exeWatch and BrowseWatch violations, and is shown in minutes. When choosing FileWatch or WriteWatch, the drop down list changes to show Total Size, which is shown in kilobytes.

You also select the type information to be contained in the report in the drop down list (either FileWatch, WriteWatch, .exeWatch or BrowseWatch).

- **Chart Type** - Indicates the type of chart to be displayed. You can select Pie, Bar or Line charts. The graphical display of report data is only available for Management and Trend reports.
- **View By** - Determines how data is compared within the report. For example, if you select to view data by Who object, data is compared among various Who objects, such as workstations, users and groups. For graphical display, the View by criterion forms the graph's X axis, and the detection type (see the Display field above) is the graph's Y axis. You can view data by Who object, content type or rule.
- **Sort By** - Determines how report data is to be sorted. You can sort by Name or by Total. This option is only available for Summary and Detailed reports.


Defining When Tab Parameters

When tab parameters determine the time frame to be covered by the report. You can select from among the following options:

- **From / Until** - Designates the specific date range for the report. Click the From radio button and then click the respective From and Until calendars (see below) to choose a specific start and stop date for the report, respectively.
- **Last N days** - Specifies a reporting period covering the last N days, where N is a number between 1 and 15. This value is calculated by counting backwards N days from the current day, inclusive. For Trend reports, this value must be greater than 1.
- **Last N weeks** - Specifies a reporting period covering the last N weeks, where N is a number between 1 and 15. This value is calculated by counting backwards N weeks from the current week, inclusive. For Trend reports, this value must be greater than 1.
- **Last N months** - Specifies a reporting period covering the last N months, where N is a number between 1 and 15. This value is calculated by counting backwards N months from the current month, inclusive. For Trend reports, this value must be greater than 1.

Defining Who Tab Parameters

Who tab parameters define the Who objects to be displayed in the report, such as workstations, users and groups. The following options define Who entities in this tab:

- **All** - All Enterprise Threat Shield Who objects are contained in the report. This is the default setting.
- **Specify** - Enables you to specify those Who objects to be included in the report. To specify a Who object, select it in the **Available** pane and then click  to move it to the **Selected** pane. Multiple entries can be selected.

Defining Content Tab Parameters

Content tab parameters specify which content types (What Content objects) to include in the report. The following options define content types in this tab:


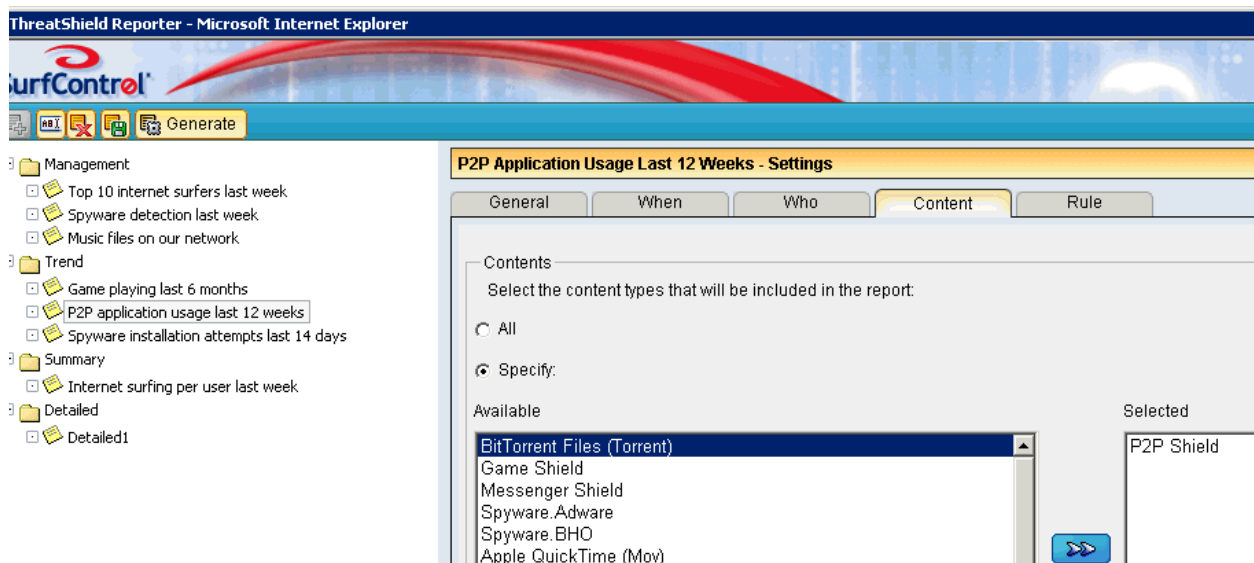

- **All** - All Enterprise Threat Shield content types are contained in the report. This is the default setting.
- **Specify** - Enables you to specify those content types to be included in the report. To specify a Content object, select it in the **Available** pane and then click  to move it to the **Selected** pane. Multiple entries can be selected:

Figure 4 - 24 Adding Bit Torrent Files to a report



Defining Rule Tab Parameters

Rule tab parameters enable you to specify the rule(s) to be contained in the report. The following options define applicable rules in this tab:

- **All** - All Enterprise Threat Shield rules are contained in the report. This is the default setting.
- **Specify** - Enables you to specify those rules to be included in the report. To specify a rule, select it in the **Available** pane and then click  to move it to the **Selected** pane. Multiple rules can be selected.

CREATING A NEW REPORT


You can create new reports for any of the four available report types. After a report is created and its parameters are saved, the report is accessible to all users in the system.



Note: This operation is not available to users with User access rights.

Only one user with Administrator access rights can be logged in at a time. If a user with Administrator access rights is logged in, additional users with these access rights cannot log in.

To create a report:

- 1 In the report tree, click the node for the report type you want to add.
- 2 Click  in the toolbar OR Right-click and select **Add Report**.
- 3 Enter a name for the report in the text box. The report is added to the report tree under the node for the report type you selected. The report contains default settings (as determined by the report type you selected) but you can change these by modifying the report's parameters.
- 4 Click **OK**.


MODIFYING REPORT PARAMETERS

You can modify a report's parameters then save the report with its new settings for future use, providing that the following is true:

- You have administrative rights. Users with User access cannot modify reports.
- You are the only one logged into the Threat Shield Reporter. Only one user with Administrator access rights can be logged in at a time. If a user with Administrator access rights is logged in, additional users with these access rights cannot log in.

After a report is defined and its parameters saved, the report is accessible to all users in the system.


To modify report parameters:

- 1 In the report tree, click the report you want to modify.
- 2 Change the parameters for the report as described in [“Defining Reports” on page 78](#).
- 3 Click  to save the report's settings.

Renaming a Report

You can change the name of any report in the system.


To rename a report:

- 1 In the report tree, click the report you want to modify.
- 2 Click  in the toolbar OR right-click and select **Rename**.
- 3 Enter the new name for the report. The report is displayed in the report tree showing the name you specified.

Deleting a Report

You can delete any report in the system, including predefined reports.

To delete a report:

- 1 In the report tree, click the report you want to modify.
- 2 Click  in the toolbar OR right-click and select **Delete**. The report will be removed from the report tree.

KEY POINTS

The following list is a summary of the main points covered in this chapter. Use this list as a quick reminder of what you can do within the Reporter:

- You can create reports then enable colleagues such as managers to view them via a Web browser from any location.
- You can export reports to applications such as PDF, Word and Excel so that you can save them as hard copies.
- Only one user with Administrator access rights can be logged in at a time. If a user with Administrator access rights is logged in, additional users with these access rights cannot log in.
- You can change the name of any report in the system.
- You can delete any report in the system, including predefined reports.
- Only users that have the correct authorization can log in to the application.

Troubleshooting

Existing AV and AS products blocking the Agent	page 84
Client based firewalls	page 85
MS File and Printer Sharing	page 86

EXISTING AV AND AS PRODUCTS BLOCKING THE AGENT

If you already have Anti-Virus and Anti-Spam programs on your clients they may see the Agent as a program that must be blocked. To prevent this from happening, you will need to add the listed files to the Exclusion/Trusts lists:

Table 1 Anti-virus products that could block the Agent

Anti-virus product	File(s) to add to Exclusion/Trust lists
F-Secure	NetAloader.exe
Trend	fcl.exe
Kaspersky	NetAloader.exe and fcl.exe

CLIENT BASED FIREWALLS

If you have Windows XP SP2 or Windows Vista installed on your clients, and you are either deploying the Threat Shield Agent from the server, or using the logon script (when the user is the administrator of this machine), the Threat Shield Agent should not be stopped from deploying. Enterprise Threat Shield can open its required ports, 3751 and 3753 in the windows firewall on the workstation.

If you are using other firewalls, either client-based or between the server and the Agent, you will need to open inbound ports and outbound ports on the client.

On the client:

- Open inbound ports 445, 139, 3751.
- Open outbound port 3753.



Note: Other anti-spyware products may prevent installation of the Threat Shield client. Disable other anti-spyware utilities before deploying the Threat Shield client.

MS FILE AND PRINTER SHARING

In order to use MS File and Print sharing you need to install the MS File and Printer Sharing protocol on to clients. Use the Network Connections utility within Control Panel to do this. MS File and Printer Sharing should be set up as follows:

- Regular Remote Deployment of Threat Shield Agents requires MS File and Printer Sharing on the Agent machines and the server machine.
- Stand Alone Remote Deployment of the Threat Shield Agent requires MS File and Printer Sharing on the Agent machines only.
- Logon scripts require MS File and Printer Sharing on the server machine only.
- The Stand Alone Independent installation does not require MS File and Printer Sharing.



Appendix

A - Using Group Policy page 88
B - Ports page 91

A - USING GROUP POLICY

You can install the clients of SurfControl Enterprise Threat Shield remotely without the user's interaction via Active Directory and Group Policy. In order to do this you must have installed the product so that it supports Stand Alone, enabling the Agents to run in Stand Alone mode see [Chapter 1 'Stand Alone mode'](#) on page 12 for more information.

After you deploy the software, it is available for installation the next time the client computer restarts. To configure group policies you must have a domain running Active Directory. Any computers that you intend to manage must be members of this domain, and be seen within Active Directory Users and Computers. To use Remote Install you need to:

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

The following instructions assume that you are familiar with Active Directory and using the Microsoft Group Policy Manager to apply policies to machines or groups of machines.

BEFORE YOU START

If you wish to install clients onto Windows XP you will need to apply a policy setting that turns off fast network startup. If you don't do this each client will need to restart twice before software installation policy changes will be applied to it. To turn off Fast Logon Optimization, enable the following policy setting:

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

For more information on the issues of Fast Logon Optimization see the Microsoft KB article:

<http://support.microsoft.com/kb/q305293/>



Note: If you are installing clients onto any operating system other than Windows XP, you do not need to do this.

STEP 1 - CREATE AN MST FILE

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

To create an MST file:

- 1 Place the Enterprise Threat Shield Client install files in a directory that is shared with all computers in Active Directory. This folder must allow read access for all domain computers.
- 2 Navigate to the Enterprise Threat Shield installation directory on your Threat Shield server and locate the SETSAgentGenMst.vbs file.
- 3 Copy and run this script either from the domain server itself, or from a server that has access to the domain server (the domain server can be either Active Directory or Novell) where you are hosting the Threat Shield .msi.

The following are parameters that can be entered:

```
cscript SETSAgentGenMst.vbs SETSAgent.msi customer.mst /server:<the name of the server  
where Threat Shield is located> /passwd:<uninstall protection password> /continue:<whether the  
installation should continue if the connection to the Threat Shield server fails>
```

```
EXAMPLE: cscript SETSAgentGenMst.vbs SETSAgent.msi customer.mst /server:ETS server  
/passwd:abc123 /continue:1
```

See the Windows group policy documentation for more details.

STEP 2 - CREATE A GROUP POLICY

Download and install the Group Policy Management console from: <http://www.microsoft.com/downloads>.

Then create a group policy:

- 1 Select **Administrative Tools > Active Directory Users and Computers** from the Start menu.
- 2 If you wish to add devices to an existing organizational unit go straight to step 7. If you need to create a new one then follow steps 3-6.
- 3 In the **Active Directory Users and Computers** window, right-click your Active Directory and select **New > Organizational Unit**.
- 4 Enter a name into the **New Object - Organizational Unit** dialog and click **OK**.
- 5 The new object will appear in the domain tree. Select the **Computers** node to see all available computers (devices) in the right-hand pane.
- 6 Drag the devices that you want to install the Threat Shield client on, into the new organizational unit that you have just created.
- 7 Right-click the new organizational unit and select **Properties**.
- 8 Select the **Group Policy** tab, then click **Open**. This opens your organizational structure within the Group Policy Management console.



Note: If you did not download and install this software you will not see the option to open this program. You will need to close the Active Directory Users and Computers window and re-open it after you have installed the program.

- 9 In the Group Policy Management window right-click the organizational unit that you have just created and select **Create and link a GPO from here**.
- 10 In the dialog that follows enter a name for the Group Policy Object. This name is then shown beneath both the organizational unit and the group policy object.
- 11 Right-click the new group policy object and select **Edit**.
- 12 The policy for Threat Shield must always be applied to computers, not users. Expand **Computer Configuration** (NOT User Configuration) then expand **Software Settings**.
- 13 Right-click Software Installation and select **New > Package**.
- 14 In the Explorer dialog, enter a UNC path to the .MSI installer file that you created in STEP 1 - Create an MST file. Click **Open**.



Note: If you want to browse to the file rather than enter a UNC path, you must navigate via My Network Neighbourhood, otherwise the computers in your domain will not be able to access the .MSI installer file.

APPENDIX

A - Using Group Policy

- 15 In the **Deploy Software** dialog box select the **Advanced** option, then click **OK**.
- 16 You will now see the SurfControl Threat Shield Properties dialog. Select the Deployment tab.
- 17 In the Deployment options section, select 'Uninstall this application when it falls out of scope of management'. This will enable the Agents to be removed from client machines automatically if you uninstall Threat Shield.
- 18 Next, select the Modifications tab, then click **Add**.
- 19 Navigate to the transform file (MST) using a UNC path then click **Open**.
- 20 Click **OK**. The software package is listed under Software Installations ready for deployment. You can double-click the package to edit it at any time.
- 21 Apply the GPO by dragging it onto the OU that you created earlier.

USING REMOTE INSTALL ON CLIENTS RUNNING WINDOWS VISTA

If you want to use remote install to install agents on clients running Windows Vista, you will need to complete the following steps:

- 1 Perform all of the steps in the **STEP 2 - Create a Group Policy** section (see above).
- 2 Next select **Administrative template > Windows Components > Windows Installer > Always install with elevated privileges**.
- 3 Select the Enable option.
- 4 Click **OK**.

UNINSTALLING THREAT SHIELD AGENTS

You can uninstall Threat Shield Agents that have been installed via a GPO.

To do this:

- 1 Open the Group Policy Management application.
- 2 Select the GPO that you want to remove (this will be in the Organizational Unit).
- 3 Right-click and select **Delete**.
- 4 Click **OK**.
- 5 Reboot the workstations. Once this has happened the Agents will be removed.

B - PORTS

SurfControl Enterprise Threat Shield uses the ports listed in Table 1.

Table 1 Ports used by SurfControl

Port	Use
25	E-mail Notifications
53	Resolving IP address to workstation ID
80	Necessary for Live updates, Threat Shield Reporter and Stand alone functionality
137, 138, 139	NetBIOS queries
389, 445	Network Group updates
1433	Writing data to SQL
3751, 3753	Used for client/server communication

APPENDIX
B - Ports

INDEX

Symbols

? 10

A

activation check box 66
adaptive threat intelligence 64
administrator access rights 76
apply rules 6

B

benefits of stand alone 12

C

cannot deploy 10, 11
check workstation activity 9
connected 11

D

database tab
 database name 16
 database type 16
 keep detailed records no more than ... days 17
 keep summary records no more than ... days 17
 password 16
 server name 16
 test connection button 17
 user name 16
delete selected rule 69
deploy check box 10
deploying an entire tree node 11
deployment process 11
directory service tab
 configure directory service settings 19
 for active directory 19
 for nds (novell 4 and up) 19
 for windows nt directory 19
 use automatic directory service settings 19
display the workstation activity window 9
down 10, 13

E

edit databases 9

e-mail tab

my server requires authentication 18
outgoing smtp server 18
send a test e-mail button 18
sender address 18
target e-mail addresses 18

exporting

G

general tab

check files larger than ...k bytes only 14
display users 14
display workstations 14

I

info 10

L

laptop icon 12, 13
last connection 10

M

manage the status of workstations 9
menu bar 5

N

network directory 9
normal mode 13

O

object 62
object selection drop down lists 66

P

parameters 72
progress bar 11

R

remote loading feature 11
removable drive data loss protection 67
report definition area 74

- report file tab
 - base file name (without the extension) 15
 - comma separated values (.csv) 15
 - html (.htm) 15
 - report file path 15
 - text (.txt) 15
- report tree 74
- reporter tab
 - location of logo 17
 - password 17
 - user name 17
- rule name 66
- rule objects tree 5
- rule priority buttons 68
- rule section 5

workstation deployment and status 9

S

- security tab
 - enter current password 20
 - enter new password 20
 - verify new password 20
- set passwords 9
- status 10

T

- the e-mail tab
 - e-mail format button 18
- threat shield agent 62
- threat shield agent. 3
- threat shield objects pane 5
- threat shield server 3
- toolbar 5
- transmitting rules 67

U

- up 10
- updates tab
 - check for updates every hour(s) 35
 - check for updates on a daily basis at 35
 - connect through proxy/firewall server 35
 - use automatic proxy settings 35
- user access rights 76
- using logical operators 59

V

- vpn connection 12

W

- workstation 10