

The logo features a red swoosh above the word "Enterprise" in a large, 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 *Starter Guide*

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

Enterprise Threat Protection™

# NOTICES

---

Updates to the SurfControl documentation and software, as well as Support information are available at [www.SurfControl.com/support](http://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](http://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](mailto: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](mailto:eay@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

### **Original SSLeay License**

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

This package is an SSL implementation written by Eric Young ([eay@cryptsoft.com](mailto: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](mailto: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 $
*/
```

These files had forensic matches to various open source projects. It appears that Moez Magfoudh is the original author. The following copyright and usage term text is in the files.

```
/******
**
** FILE_NAME
**
** This file is part of the ABYSS Web server project.
**
** Copyright (C) 2000 by Moez Mahfoudh <mmoez@bigfoot.com>.
** 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. 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 and usage term text is in the file.

#////////////////////////////////////

#

# Copyright (c) 2000-2001 ConnectTel, Inc. All Rights Reserved.

#

# 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 . . . . .	1
ABOUT THIS GUIDE . . . . .	1
TECHNICAL SUPPORT . . . . .	2
OVERVIEW . . . . .	3
HOW IT WORKS . . . . .	4
BASIC ARCHITECTURE . . . . .	5
Server . . . . .	5
Client . . . . .	5
NETWORK CONSIDERATIONS. . . . .	6
Network Placement . . . . .	6
Protocols and Ports . . . . .	7
DATABASE OPTIONS . . . . .	8
BEFORE YOU START . . . . .	9
Threat Shield and 64-bit OS Support . . . . .	10
Threat Shield and Windows Vista . . . . .	10
Threat Shield and virus checkers . . . . .	11
SETTING UP ENTERPRISE THREAT SHIELD . . . . .	12
Stage 1 - Install Threat Shield on the server . . . . .	12
Stage 2 - Launch Threat Shield Manager . . . . .	17
Stage 3 - Deploy the Agents . . . . .	17
Remote deployment . . . . .	18
Stand Alone Remote Deployment . . . . .	19
Installing using a Logon script . . . . .	19
Stand Alone Independent Installation . . . . .	20
Registering Enterprise Threat Shield . . . . .	22
FURTHER CONFIGURATION . . . . .	23
Implementation Strategies . . . . .	23



## ABOUT THIS GUIDE

---

This Starter Guide will help you to install Enterprise Threat Shield with the default settings, so that you can start filtering as quickly as possible. The **Enterprise Threat Shield Administrator's Guide** contains more detailed information on how to optimize and fine-tune Enterprise Threat Shield. You can also access the SurfControl Knowledge Base, visit <http://kb.surfcontrol.com/>.

You can download updated documentation from [www.surfcontrol.com](http://www.surfcontrol.com). Select **Downloads > User Guides** from the main menu, then select the documents you want to download.

# TECHNICAL SUPPORT

---

Visit [www.surfcontrol.com/support](http://www.surfcontrol.com/support). To speak to a technical support representative, call SurfControl Technical Support:

**Table 1** Contact Details

Region	Hours of Operation	Number
USA	8:00 AM - 8:00 PM (EST) Monday - Friday	(831) 440-2700
Europe	9:00 AM - 5:30 PM (GMT) Monday - Friday	+44 1260 296 259
Asia	9:00 AM - 5:30 PM (Beijing, Hong Kong, Taiwan, Singapore, GMT +8) Monday - Friday	+65 6823 1313
Australia	7:30 AM - 6:00 PM (Australia Eastern) Monday - Friday	+61 2941 40033

# OVERVIEW

---

The following are key concepts used by Enterprise Threat Shield and implemented using Threat Shield Manager and Threat Shield Reporter:

- Enterprise Threat Shield controls the use of applications and files at all points in the use cycle – introduction, launch and after being stored – with detection technology specific to each point:
  - FileWatch detects and responds to stored files.
  - WriteWatch detects and responds to files at introduction, as soon as downloading or copying begins.
  - .exeWatch detects and responds to the launch of applications, as soon as execution starts.
  - BrowseWatch detects and monitors Web browsing in real-time. Web browsing can be a point of entry for unauthorized files and applications, so monitoring this activity can show potential problem areas.
- Enterprise Threat Shield enforces policies that range from denying use, to allowing use but managing it. For example, .exeWatch enables you to specify when an application should be restricted, and when it should be allowed. For instance, you could stop users playing games, apart from during lunch-time, or before and after work.
- Enterprise Threat Shield implements policies via rules. These can be created to suit specific end users, workstations, departments or the entire company. For example, a rule that is relevant only to Marketing users will list these users.
- Rules are created with objects that specify different combinations of entities to which a rule may apply. For example, a Who object can be defined that lists the company's Marketing users, and then be attached to a rule that is relevant only to these users.
- Rules have priorities assigned to them. The Threat Shield Agents, which run on the users machines, download rules from the server that are relevant to their particular user. If a file is detected that is included in a rule they check the Rules table, starting from the highest-priority rule. If a rule is triggered, the corresponding action/s are taken and any remaining rules associated with this user or group are skipped (since they are lower priority than the rule being enforced).
- SurfControl provides databases of application signatures that Enterprise Threat Shield uses to identify the programs it is "watching".
- Enterprise Threat Shield provides a database editor that enables you to create your own databases of files not included in a SurfControl database.
- Enterprise Threat Shield uses 'server-agent' architecture to ensure the processing is located in the optimum place, to ensure the greatest efficiency.

# How it works

---

Enterprise Threat Shield works on a centralized server and on users workstations:

- **Threat Shield server** - This is the real-time control center of the application. Rules relating to how users should be monitored are stored on the server, as well as the facility to run reports on these users. This enhances performance as well as simplifying installation and maintenance.
- **Threat Shield Agent** - This uses the workstation's own resources to monitor the desktop. Running as a background process when the workstation is connected to the network, the Agent communicates with the server to establish whether a detected file is present within a rule. If it is, the Agent carries out the action specified in the rule. New rule configuration is obtained from Threat Shield Manager and the Agent can check the users PC either by a scheduled scan or force a scan on a real-time basis.

The Threat Shield Agent is completely invisible to the user and can be deployed in Stand Alone mode. It is then capable of working even if the connection to the Threat Shield server is lost.

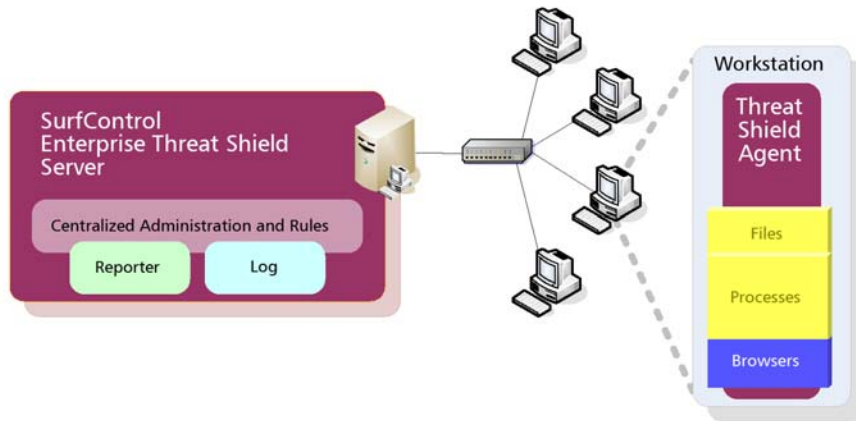
- **Threat Shield Manager** - This is the policy creation module that is used to define, edit and deploy the rules enforced by Enterprise Threat Shield. Rules are created within the Threat Shield Manager then sent to workstations when they poll the server, or when a user logs in.
- **Threat Shield Reporter** - This is the report creation and viewing mechanism. SurfControl-supplied signature databases can be updated periodically via the Internet through the SurfControl Web site. You can also create your own custom databases.

Once you have configured Enterprise Threat Shield the Agent will pick up the new configuration when it polls the server. This will also happen when the Agent starts up as the user logs in. No software installation is required on the workstations being monitored.

# BASIC ARCHITECTURE

---

Enterprise Threat Shield provides centralized workstation policy management using a client-server model. Figure 1 outlines the overall architecture of Enterprise Threat Shield. Reporting, logging, and administration are all managed from the server or an administrative workstation. A thin-client is deployed to each workstation which can moderate file access, program execution, and browser activity.



**Figure 1** Enterprise Threat Shield Overview

## SERVER

The Threat Shield server is responsible for maintaining workstation rules, monitoring client deployments, and managing threat databases for spyware, P2P, instant messaging, and games. Log information is gathered and published to a relational database for auditing and reporting.



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

## CLIENT

The Threat Shield client acts as a thin-client policy enforcement tool on each workstation. By examining the contents of the filesystem, as well as attempts by the user to execute programs and write data to the drives, the Threat Shield client effectively manages and reports on activity on the workstation.

# NETWORK CONSIDERATIONS

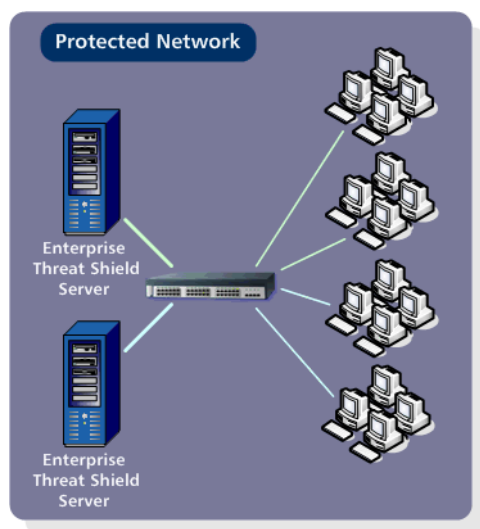
---

You should review the following network considerations before deploying SurfControl Enterprise Threat Shield on your network. You should also become familiar with the three test implementation plans covered in “Implementation Strategies” on page 23 of this guide.

## NETWORK PLACEMENT

Threat Shield servers should be installed in your organization’s protected network. The Threat Shield server requires a static IP address on a TCP/IP network. It does not, however, impose any limitations on the network switching and routing configuration, so long as the workstations can communicate with the Threat Shield server(s). There must also be sufficient network bandwidth and low latency.

Figure 2 shows an Threat Shield protected network installation with multiple servers. You should install at least one Threat Shield server for every 5,000 monitored workstations in your network. There is no limitation on the number of Threat Shield servers you can deploy, but each workstation must be managed by one server only. This helps avoid unnecessary bandwidth consumption and processing contention.



**Figure 2** Threat Shield Protected Network Deployment

## PROTOCOLS AND PORTS

Figure 3 shows an overview of the network architecture for Enterprise Threat Shield. Threat Shield network considerations include Windows file sharing connections, client-server communication through keep-alives, and SQL database communication including authentication.

You must allow access to these ports between the server and the workstations for Threat Shield to function properly. These access allowances must include both router configuration as well as firewall software installed on Windows workstations.

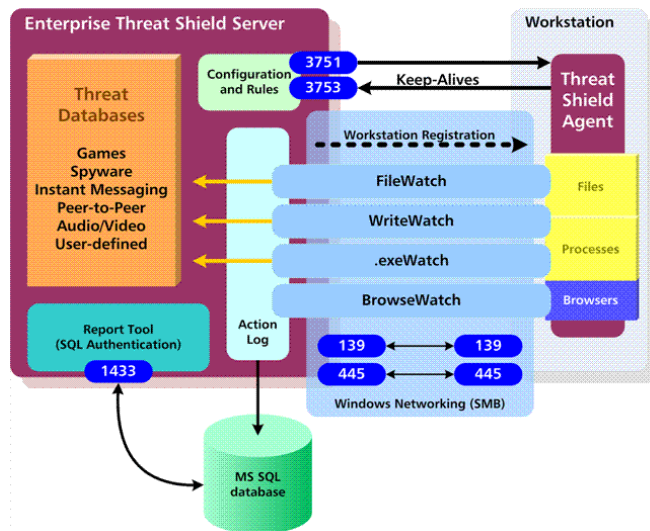


Figure 3 Enterprise Threat Shield Network Overview

### Windows File Sharing

The Threat Shield server installation program creates a network file share on the Enterprise Threat Shield server. In addition, servers distribute files to workstations during deployment. Windows file sharing consists of SMB session creation and data transfer on TCP/IP ports 139 and 445.

Enterprise Threat Shield can be installed on any type of server, as long as it does not contain either of the SurfControl Web Filter or E-mail Filter products. This server must have file & printer sharing enabled.

### Enterprise Threat Shield Client Keep-Alive

The Threat Shield client deployed on workstations periodically sends a keep-alive notification to the Threat Shield server on TCP/IP port 3753.

### Threat Shield Reporter

The Threat Shield Reporter installs on top of Microsoft IIS, uses HTTP port 80 for its interface, and uses SQL authentication for database access.

### SQL Authentication

SQL database communication is performed either using trusted Windows authentication or SQL authentication over TCP/IP port 1433. However, Threat Shield Reporter requires SQL authentication.

# DATABASE OPTIONS

---

Enterprise Threat Shield ships with MSDE 2000, but can also create the required data structure in a fully-licensed version of MS SQL Server 7.0 or MS SQL Server 2000.

Using a fully-licensed version of SQL server (rather than MSDE) allows more flexibility and the ability to fine-tune database performance. If you plan to use a fully-licensed version of SQL, make sure the SQL server is installed and running before attempting to install Enterprise Threat Shield.

The deployed Threat Shield client does not interact directly with the SQL database; therefore no database engine needs to be installed on Threat Shield clients.

## BEFORE YOU START

---

Before you start, ensure that your client and server machines meet the minimum requirements as listed below. .Net framework and Microsoft IIS MUST be installed BEFORE installing Enterprise Threat Shield:

**Table 2** Threat Shield Server requirements

Component	Requirement	
<b>Threat Shield Server</b>	Processor	Pentium IV or above
	Memory	256 MB
	Operating System	<ul style="list-style-type: none"> <li>Windows 2000</li> <li>Windows Server 2003</li> </ul>
	Applications	.Net Framework v1.1 Internet Information Server v5.0 or higher.
	Threat Shield Reporter (Server Side)	Internet Information Server v5.0 or higher .Net Framework 1.1 MSDE or Microsoft SQL Server 2000 (or higher) Internet Explorer 5.5
	Threat Shield Reporter (Viewer Side)	Internet Explorer 5.5

**Table 3** Threat Shield Agent requirements

Component	Requirement	
<b>Threat Shield Agent</b>	Operating System	<ul style="list-style-type: none"> <li>Windows 2000</li> <li>Windows Server 2003</li> <li>Windows XP</li> <li>Windows Vista</li> </ul>
	Agent Memory	<ul style="list-style-type: none"> <li>20 MB of RAM</li> </ul>
	Agent Disk space (in Stand Alone Mode)	<ul style="list-style-type: none"> <li>30 MB free on hard drive</li> </ul>

## BEFORE YOU START

**Table 4** Network requirements

Component	Requirement
Network Operating System	<ul style="list-style-type: none"><li>• Microsoft NT Network</li><li>• Microsoft Active Directory</li><li>• Novell NDS V4 or above</li></ul>

If your environment does not meet these recommendations you could use an alternative method of deployment such as a logon script. You can also install the Stand Alone feature (selected during the installation of the product) to download all of the Threat Databases onto the client machines. This enables the Threat Shield Agent to run without a connection to the Threat Shield server, keeping network traffic to a minimum.

### THREAT SHIELD AND 64-BIT OS SUPPORT

The Threat Shield server can be installed on Windows 64-bit OS machines. The Threat Shield Agent will be able to run on Windows 64-bit OS clients with the following constraints:

- FileWatch, WriteWatch and .exeWatch will be unable to monitor network file paths.
- If you define a rule that contains a BrowseWatch object, the BrowseWatch part of the rule will not work on a 64-bit client machine.
- The .exeWatch driver is not supported.
- You will be unable to run the Threat Shield Agent in hidden mode.

### THREAT SHIELD AND WINDOWS VISTA

The Threat Shield Agent will be able to run on Windows Vista clients with the following constraints:

- FileWatch, WriteWatch and .exeWatch will be unable to monitor network file paths.
- If you define a rule that contains a BrowseWatch object, the BrowseWatch part of the rule will not work on a Vista client machine.
- The .exeWatch driver is not supported on a Windows Vista 64-bit OS. It is, however, supported on the Windows 32 version.
- Warning Message boxes will not appear on clients that are running Windows Vista.
- You will be unable to deploy the agents using a login script.
- You will be unable to run the Threat Shield Agent in hidden mode.

## THREAT SHIELD AND VIRUS CHECKERS

The virus checkers in Table 5 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 5** 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

# SETTING UP ENTERPRISE THREAT SHIELD

---

Before you install Enterprise Threat Shield you need to ensure that your network settings will allow it to work. This is particularly important with the deploying of the Threat Shield Agent which can be stopped by certain applications such as firewalls.

Setting up SurfControl Enterprise Threat Shield is a three stage process:

Stage	Page
Stage 1: Download and Install Enterprise Threat Shield	12
Stage 2: Launch Threat Shield Manager	17
Stage 3: Deploy the Agents	17

## STAGE 1 - INSTALL THREAT SHIELD ON THE SERVER

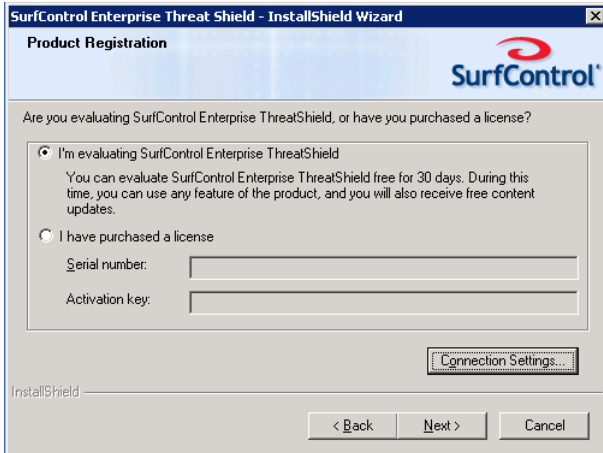
Enterprise Threat Shield can be installed on any type of server, as long as it does not contain either of the SurfControl Web Filter or E-mail Filter products. This server must have file & printer sharing enabled. For most installation options, you do not have to install files on the local drives of client workstations. Instead, Threat Shield Agents are initiated from the Threat Shield Manager which resides on a central Threat Shield Server.

The software should be installed on a shareable local drive folder of a file server with writable access for the administrator (read only access for users)

To install Threat Shield on the server:

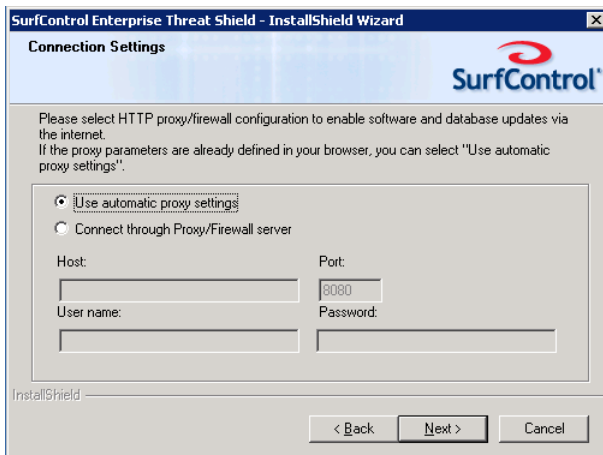
- 1 Download Enterprise Threat Shield from SurfControl's Web site.
- 2 Double-click the Enterprise Threat Shield executable file to start the Enterprise Threat Shield wizard.
- 3 When you see the Welcome screen click **Next>**.
- 4 In the License Agreement screen select the 'I accept the terms of the license agreement' option and click **Next>** if you wish to proceed with the installation.

- The next dialog box enables you to evaluate the product or purchase it. The evaluation period is 30 days. After this period you will be unable to launch the Threat Shield Manager without purchasing a license first. If you have already purchased a licence, select the 'I have purchased a license' option to enable the Serial number and Activation key fields. Enter the Serial number and Activation key that SurfControl sent you when you licensed the product:



If you do not use a proxy server to access the Internet click **Next>**, and go to step 8. If you do access the Internet via a proxy server, click the **Connection Settings** button.

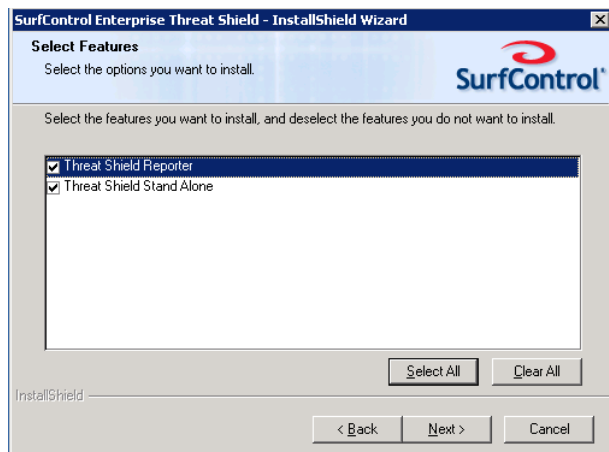
- You will see a dialog that enables you to specify how you want this access to take place. Enterprise Threat Shield needs these settings in order to connect to the Internet for updates:



- Click **Next>**.

## SETTING UP ENTERPRISE THREAT SHIELD

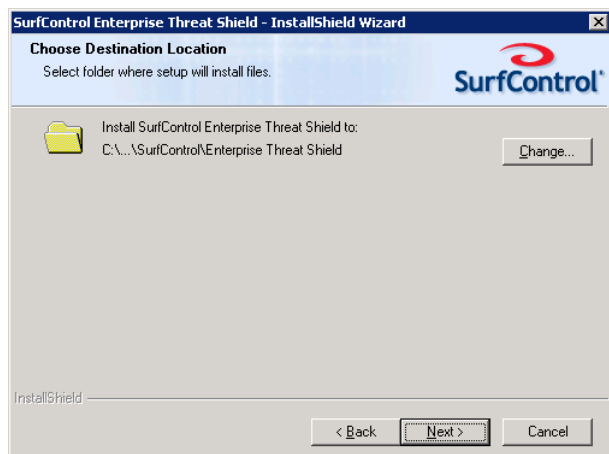
- 8 The next dialog box enables you to specify the features that you want to include with this installation of Enterprise Threat Shield:



- **Threat Shield Reporter** - Enables you to run reports on how your network and Internet are being used. Select this to install the Reporter.
- **Threat Shield Stand Alone** - Enables the Threat Shield Agent to run without a connection to the Threat Shield server. See the Administrator's Guide [Chapter 1 'Stand Alone mode" on page 12](#) for more information. Select this to make this option available from the Threat Shield Manager.

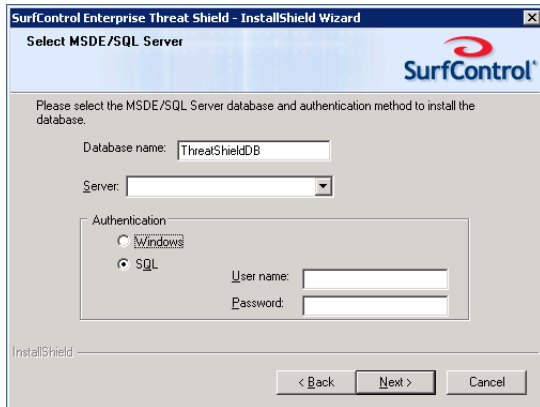
- 9 Click **Next>**.

- 10 You will be asked to choose a destination location:



- 11 Click **Next** to use the default of C:\Program Files\SurfControl\Enterprise Threat Shield. Alternatively click **Change** to navigate to the location that you want Enterprise Threat Shield to be installed in, then click **Next>**.

12 Use the next dialog to specify the MSDE/SQL database that you want to use:



Enter the following details:

- **Database name** - The default database name is ThreatShieldDB, change this if you wish to use another name or enter the name of an existing database, if you have one.
- **Server** - Select the server on which your MSDE/SQL database is stored.
- **Authentication** - Select the type of authentication that you wish to use.
  - Windows - Windows authentication uses your Windows network username and password.
  - SQL - Enter the User name and Password to your SQL server.



**Note:** SQL authentication is required by Enterprise Threat Shield Reporter. You will not be able to use the Reporter without it.

13 Click **Next>**.

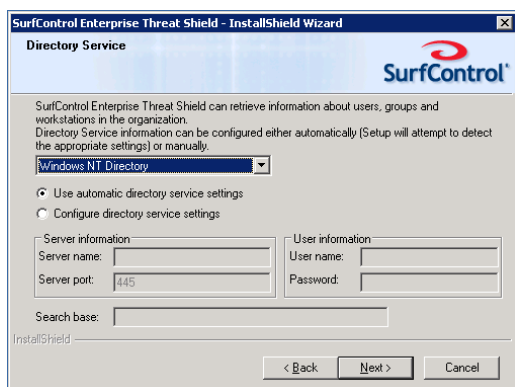
14 The next dialog enables you to specify Directory Service settings. You can choose from:

- Windows NT Directory (the default)
- Active Directory (Windows 2000 and up)
- NDS (Novell 4 and up)

## SETTING UP ENTERPRISE THREAT SHIELD

Select the Directory service you require then select how you want the service settings to be gathered:

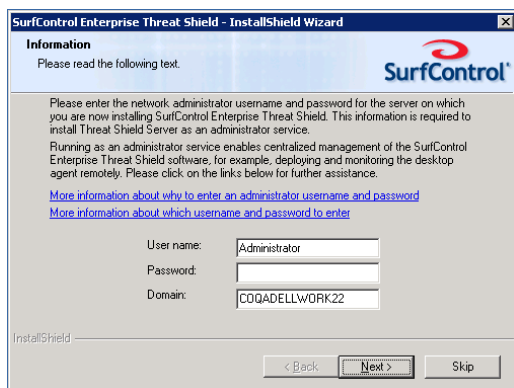
- **Use automatic directory settings** - This is the default setting and requires no further action.
- **Configure directory service settings** - This will enable some of fields beneath it. The fields that are enabled and the information that is asked for depend on what directory service you have chosen.



15 Click **Next>**.

16 The next dialog enables you to start the installation. Click **Install**. A status bar will indicate how the installation is progressing.

17 Threat Shield needs to run as an administrator service, so it must have the administrator username and password for the server on which it is being installed. Once the installation has finished, the next dialog will ask you for this information:



Fill in the fields as follows:

- **Username** - Enter the Administrator username for this machine. This must be the domain administrator's username.
- **Password** - Enter the Administrator password for this machine. This must be the domain administrator's password.
- **Domain** - Enter the domain that this machine is a part of, if this edit field is empty.

18 Click **Next>**.

19 The next dialog will tell you that the setup has completed successfully and will give you the option of reading the README (recommended) and launching the Threat Shield Manager. Click **Finish** to complete the installation.


- 20 If you left the 'Yes, I want to launch the application now' option checked, and you have chosen to evaluate Enterprise Threat Shield you will see the following dialog:



Click **Try**. This dialog will appear every time you launch the Threat Shield Manager until the trial period is over. Once the 30 day limit is reached, you will only be given the option to **Register** or **Contact Sales**. You will be unable to launch Threat Shield Manager until this is done.

## STAGE 2 - LAUNCH THREAT SHIELD MANAGER

Threat Shield Manager is the user interface for configuring policy rules. It also communicates with the Threat Shield server, which then relays this information to the Threat Shield Agents.

Launch Threat Shield Manager by clicking the Enterprise Threat Shield desktop icon .

## STAGE 3 - DEPLOY THE AGENTS

Deploy Enterprise Threat Shield's Agent on the workstations in the network. For more information See "Implementation Strategies" on page 23. This Agent runs as a stealth application on each workstation in the network and is completely invisible to the end user.



**Note:** You must have Microsoft File and Printer Sharing installed and running on the workstation before deploying the Agent.

Four methods are available for deploying the Agent. The method used depends on the network operating system in use:

- Remote deployment
- Installing using a logon script
- Stand Alone remote deploy
- Stand Alone independent installation

### REMOTE DEPLOYMENT

Before you deploy the Threat Shield client, use the checklist below to ensure your server and workstations meet the requirements for remote deployment. If your environment does not meet these requirements, you can deploy Threat Shield using a logon script.

#### Workstation requirements


In order to remotely deploy the client on the workstation, the workstation must:

- Be turned on.
- Have a user logged on. If a user is not logged on and you deploy, the deployment automatically occurs at log-on.
- Be within the same domain as the Threat Shield server.
- Run a Windows NT, 2000, XP Professional or Windows Vista operating system.
- Have only one IP address.
- Have a workstation name that can be resolved by DNS (or, if the workstation has an NT operating system, WINS must be configured).
- Have file and printer sharing enabled.
- Have the following ports open for both the workstation and the workstation's firewall:
  - 139 - open by default on Windows operating systems
  - 445 - open by default on Windows operating systems
  - 3751
  - 3753

For more information about deploying Windows firewall settings, refer to [Deploying Windows Firewall Settings with Group Policy](#) on Microsoft Technet.

#### Installing Agents remotely


To install Agents remotely;

- 1 Open the Workstation Deployment and Status window either by selecting Workstation Deployment and Status from the Threat Shield Manager Tools menu or by clicking  in the toolbar.
- 2 Select each checkbox that corresponds to the computer on which you would like to run the Agent. See the Administrator's Guide: [Chapter 1 'Activating the Deployment Process'](#) on page 11.

## STAND ALONE REMOTE DEPLOYMENT

This enables you to remotely deploy the Agent in Stand Alone mode.

To deploy the Agent in Stand Alone mode:

- 1 Open the Workstation Deployment and Status window either by selecting Workstation Deployment and Status from the Threat Shield Manager Tools menu or by clicking  in the toolbar.
- 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 **Switch Stand Alone on** from the pop-up menu. The workstation icon/s will change to that of a laptop to show that these workstations are now set to Stand Alone mode.
- 5 Select the Deploy check-box corresponding to these workstations to deploy them in Stand Alone mode. Refer to the Administrator's Guide: [Chapter 1 'Using Stand Alone mode' on page 12](#) for more information.

## INSTALLING USING A LOGON SCRIPT

Installing using a logon script enables you to set up Threat Shield to install the Agent as soon as the end-user logs in. This will be done without the user's intervention. In fact the user won't even be aware that this is happening:

- If you don't want to use Stand Alone mode, insert the following command into the user's logon script:  
`start \\servername\EnterpriseThreatShield\ThreatShieldAgent.exe`  
 where 'servername' is the name of the server where Enterprise Threat Shield is installed.
- If you want to be able to deploy the Agent in Stand Alone mode follow steps 1 and 2 below.

To install Agents using a logon script:

- 1 Download the SETSAgent.msi from the SurfControl Web site to a shared folder that has 'read' access for Everyone. In the Step 2 example this would be \\Server1\EnterpriseThreatShield.
- 2 Insert the following command line into the users' logon script:

```
msiexec /i <path to .msi file (e.g. \\Server1\EnterpriseThreatShield\SETSAgent.msi)>
SA_SRV_NAME=<the name of the server where Enterprise Threat Shield is located>
SA_cli_PASSWD=<uninstall protection password> /qn /l <log file path and name>.
```

```
Example: msiexec /i \\Server1\EnterpriseThreatShield\SETSAgent.msi)
SA_SRV_NAME=Server1 SA_CLI_PASSWD=Abc123 /qn /l C:\SETSAgentInstall.log
```

The following are parameters that can be entered:

- SA\_CLI\_PASSWD= <password> - this password will be used for uninstall authentication.
- SA\_CLI\_UNINST\_PASSWD= <password> - the password that must be entered in order to uninstall the product. This is only relevant when you use a logon script to uninstall Enterprise Threat Shield. During the uninstall, this is the only flag that will be used.
- SA\_SRV\_NAME= <Threat Shield server name (or IP address)>. This parameter MUST be entered.

## SETTING UP ENTERPRISE THREAT SHIELD

- `SA_CONT_INSTALL` - specifies whether the installation must continue in the event of the connection to the server failing.

You can also enter the following .msi flags during the installation if required:

- `/i` - to be used for regular installation or maintenance. Can also be used for installation in unattended mode.
- `/qn` - to be used for quiet install(no user interface while installing).
- `/uninstall` - for removal when running in unattended mode.
- `/l<log file name>` - to specify where install logs should be written to (used mainly for debugging purposes).

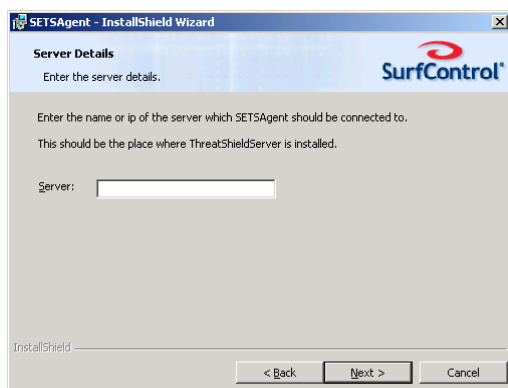
For more information regarding logon scripts, please refer to your Novell or Windows network manual. You can also deploy the Agent via Group Policy. For more information see “A - Using Group Policy” on page 88 of the Administrator’s Guide Appendix.

## STAND ALONE INDEPENDENT INSTALLATION

Stand Alone Independent Installation enables you to manually install the Agent at the workstation, or to install it using a Group Policy Object.

To perform a Stand Alone independent installation:

- 1 Download a copy of `SETSAgent.msi` from the SurfControl Web site onto the client on which you are installing the Threat Shield Agent.
- 2 Double-click the `SETSAgent.msi` to start the installation.
- 3 When you see the Welcome screen, click **Next**.
- 4 In the next dialog box enter the name or IP address of the machine on which Enterprise Threat Shield is installed:



- 5 Click **Next**.

- 6 Once you click **Next** you will see a dialog box asking you to create a password for uninstalling the client:
  - **Enter Password** - Enter a password.
  - **Re-enter Password** - Re-enter the password.



- 7 This password will be copied across to the .msi file and works in the same way as the SA\_CLI\_UNINST\_PASSWD parameter listed in the previous section on page 19. If you don't want to add a password, you can leave the text boxes blank.
- 8 Click **Next**.
- 9 A Ready to Install dialog box will appear. Click **Install**. This will download all of the files that the client will need to function in Stand Alone mode.
- 10 Click **Finish**.

Once you have completed these stages, Enterprise Threat Shield will be able to carry out the following without any further configuration:

- **Spyware Logging** - Detection of spyware by FileWatch and WriteWatch will be reported on. Any spyware detected by .exeWatch will be reported on then terminated.
- **Application and Media Logging** - Any violation of databases such as P2P, IM and Games will be reported on. Also, detection of any media formats supported in the Enterprise Threat Shield content section by WriteWatch or FileWatch will be reported on.

Although Threat Shield provides out-of-the-box spyware protection, it is important that you configure this protection to fit your own environment. Be aware, however, that Enterprise Threat Shield is a powerful tool which, if configured incorrectly, can delete files that are not spyware files. Other problems which could arise from incorrect configuration are:

- Needlessly scanning for allowed desktop applications.
- Scanning too frequently.
- Scanning during high productivity periods..

All of these potential problems are easy to prevent if you deploy Enterprise Threat Shield in the manner recommended by SurfControl, see the following section for details on how to do this. You can also use the Enterprise Threat Shield Best Practices Guide which is available from the SurfControl User Guides page of the SurfControl Web site.

## SETTING UP ENTERPRISE THREAT SHIELD

### REGISTERING ENTERPRISE THREAT SHIELD

The Enterprise Threat Shield's software technology license enables you to update your software and database and create your own customized databases.

To obtain a registration code for Enterprise Threat Shield:

- 1 In the Threat Shield Manager main window, select **About** from the Help menu. The SurfControl Enterprise Threat Shield window is displayed.
- 2 Click **Contact Sales** to access the SurfControl Web site. Navigate to the sales office for your area and click the e-mail link.
- 3 Send the message to SurfControl sales. SurfControl will then send you the registration code by e-mail.
- 4 From the Help menu, select **Register** and enter the registration code in the relevant field.

# FURTHER CONFIGURATION

---

Because every network is different you MUST fully test Enterprise Threat Shield and optimize the configuration in a smaller environment, before pushing it out to your entire enterprise.

## IMPLEMENTATION STRATEGIES

SurfControl recommends one of the implementation strategies listed below.

### Long Range Assessment Implementation Plan

This is the recommended implementation, since it allows time to fully assess which of your environment's unique needs and behaviors Threat Shield can address. This approach enables you to gain a deep understanding of problems on the network. It does however, take the longest time to fully implement, since it emphasizes collecting data, before enforcing rules.

The Long Range Assessment Implementation plan may be best for you if your organization has:

- Time to gather data and analyze it to guide your rule-building.
- The need to understand what end-point problems might exist.

To implement the Long Range Assessment method:

- 1 Change the default rules so that they only have the "Generate Report" action.
- 2 Deploy the Agent to your entire network.
- 3 Assess the impact and success of the deployment.
- 4 Examine the reports.
- 5 Create or modify rules incrementally for more active enforcement.
- 6 Examine the reports.
- 7 Modify rules again, if necessary.

### Targeted Implementation Plan

This is the best implementation if you know which users or workstations are infected with the most spyware, or are most in need of desktop application (e.g., IM, games, P2P) control.

To implement the Targeted method:

- 1 Deploy the Agent to the workstations you have identified as needing spyware or application control (this must be 50 workstations or less).
- 2 Assess the impact and success of the deployment.
- 3 Configure rules that remove spyware and/or targeted desktop activities.
- 4 Examine the reports.
- 5 Choose the next group to receive spyware or application control (up to 50 workstations), and deploy the Agent to these.
- 6 Repeat steps 2, 3, and 4 until you have deployed the Agent and are using rules for everyone in the network.

## FURTHER CONFIGURATION

### Rapid Response Implementation Plan

Though quick to implement, the Rapid Response implementation plan is not recommended for most organizations, and is only suitable if your organization has:

- A pervasive, clearly defined, disruptive spyware problem.
- A willingness to deal with individual deployment issues (as long as most of the workstations are cleaned and protected).



**Note:** SurfControl would always recommend that you use the Long Range Assessment or Targeted method by preference.

---

To implement the Rapid Response method:


- 1 Configure a rule for the problem using the Administrator's Guide for reference if necessary.
- 2 Deploy the Agent to one workstation.
- 3 Confirm success of the deployment and the rule's impact on the user and workstation.
- 4 Deploy the Agent to the entire network.
- 5 Examine reports and modify the rule as needed.

# CREATING A QUICK POLICY

Once you have decided how you are going to implement a policy, you can create a quick policy in two stages:

## Stage 1

Check for activity that contravenes your organization’s Acceptable Usage Policy. To do this:

- 1 Click the Workstation Activity toolbar icon  or select **Workstation Activity** from the **Tools** menu. You will see the Workstation Activity window, showing triggered rules in real time. The Workstation Activity window will show the workstation involved, the rule that was triggered (if any), the date that this occurred and the associated message. Anything that occurred prior to the window being opened will not be shown.
- 2 Use this information to create your policy.

## Stage 2

Create a policy. To create a policy you will need to use the following objects:


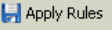
**Table 6** Objects

Term	Mandatory	Description
<b>Who</b>	Yes	Defines who the rule will apply to.
<b>Content</b>	Yes - unless this is just a BrowseWatch rule, or the rule just uses WriteWatch to block writing to a removable drive.	Define the files and applications that the rule should look for.
<b>FileWatch</b>	No, but you MUST include at least one Watch object.*	FileWatch searches for, and controls, applications such as games, P2P (Peer-to-peer), IM (Instant Messaging) and spyware, as well as music/video file types, such as MP3 and Mpeg.
<b>WriteWatch</b>	No, but you MUST include at least one Watch object.*	Monitors and protects areas of the network, and local drives, by controlling the downloading and/or copying of unauthorized files and applications. It also detects and terminates the running of existing spyware. .
<b>.exeWatch</b>	No, but you MUST include at least one Watch object.*	Controls the unauthorized use of applications, and loading of modules such as .dlls. It monitors running applications such as Spyware, MP3 file swapping or messengers.
<b>BrowseWatch</b>	No, but you MUST include at least one Watch object.*	Identifies Web browsing activity and monitors actual time spent at Web sites and Web pages. It detects the duration of active Web browsing, providing information about real interaction time as well as how long a browser is open.

\* Watch objects include FileWatch, WriteWatch and .exeWatch.

## FURTHER CONFIGURATION

To create the policy:

- 1 Choose one of the methods outlined in the preceding Implementation Strategies section as a means of implementing the policy.
- 2 Right-click the **Who** node in the Rule Objects tree and select **New** from the drop-down menu.
- 3 Add the workstations that appeared in the Workstation Activity monitor at Stage 1.  
By default, the object's name will be Who 2. See [Chapter 2 'Who' on page 28](#) of the Administrator's Guide for detailed information on creating Who objects.
- 4 Right-click the **Content** node in the Rule Objects tree and select **New** from the drop-down menu.
- 5 Add the databases that contain the files/applications that need monitoring. For example: if you need to control Spyware, add the Spyware Shield database to the Selected Databases pane. If you need to files that are not included in these databases, create a custom database then add it using the User-defined Databases section. See [Chapter 2 'Content' on page 30](#) of the Administrator's Guide for detailed information on creating Content objects.
- 6 Right-click the **.exeWatch** node in the Rule Objects and select **New** from the drop-down menu. By default the object's name will be .exeWatch 3 and the working days and hours will be selected.
- 7 Click the **All** button  to ensure that this rule will be applied during all hours. See [Chapter 2 '.exeWatch' on page 48](#)
- 8 Select **Add** from the Rule menu. A new rule will appear with the default name of Rule 3.
- 9 Select Who 2 and .exeWatch 3 to be part of Rule 3.
- 10 Click the **Apply Rules** toolbar icon  or select **Apply Rules** from the **File** menu.
- 11 The Threat Shield Agents will be updated the next time the Agent polls the server. The policy will apply to all users specified in step 2 and detect the specific file types and applications defined in step 3.



**Note:** Agents receive changes to policies only when the Agent initiates, or the Agent polls the server. The heartbeat of the poll is one-at-a-time, so the more workstations there are, the greater the lag. This means that in a company where there are a lot of Agents, there may be a time lag before the configuration is propagated to all clients.