

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 3.5.1

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 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.

Copyright ©1998-2006 SurfControl plc. All rights reserved.

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

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

Version 3.5.1 printed June 2006.

CONTENTS

NOTICES	1
ABOUT THIS GUIDE	1
Technical Support	1
BEFORE YOU START	2
SETTING UP ENTERPRISE THREAT SHIELD	3
Stage 1	3
Stage 2	5
Stage 3	5
Remote deployment	6
Stand Alone Remote Deployment	7
Installing using a Logon script	8
Stand Alone Independent Installation	9
Registering Enterprise Threat Shield	10
FURTHER CONFIGURATION	11
Implementation Strategies	11
Creating a quick policy	13

ABOUT THIS GUIDE

This Starter Guide will help you to install Enterprise Threat Shield with the default settings, so that you can begin 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. To access the SurfControl Knowledge Base, visit <http://kb.surfcontrol.com/>.

You can download updated documentation from www.surfcontrol.com. Select **Downloads > User Guides** from the main menu, then select the documents you want to download. You can download the Best Practices Guide, located at http://www.surfcontrol.com/uploadedfiles/SETS_Best_Practice_Guide.pdf for information on the right way to implement SurfControl Threat Shield.

TECHNICAL SUPPORT

Visit www.surfcontrol.com/support. To speak to a technical support representative, call SurfControl Technical Support:

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

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:

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

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

Component	Requirement	
Network Operating System	<ul style="list-style-type: none">Microsoft NT NetworkMicrosoft Active DirectoryNovell NDS V4 or above	

If your environment does not meet these recommendations you can 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, thus keeping network traffic to a minimum.

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 3 stage process:

Stage	Page
Stage 1: Download and Install Enterprise Threat Shield	3
Stage 2: Launch Threat Shield Manager	5
Stage 3: Deploy the Agents	5

STAGE 1

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.



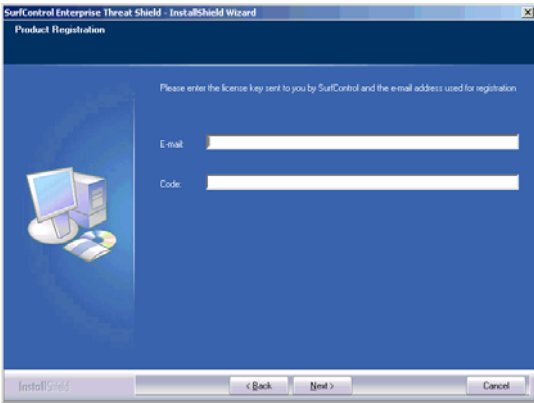
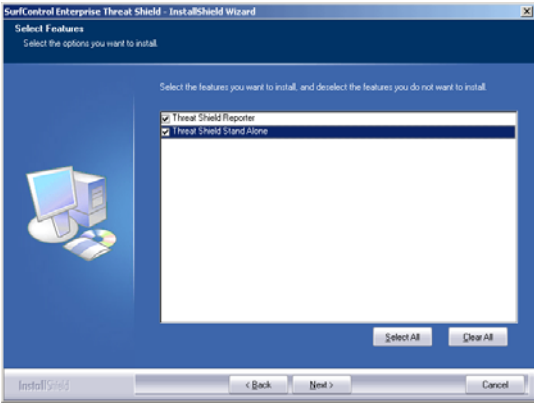
Note: Central initiation is available for Windows 2000 and Windows XP Pro clients.

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).

Procedure 1 Installing Threat Shield on the server

Step	Action
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	Once 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.
5	The next dialog box enables you to register the product.


Setting up Enterprise Threat Shield

Step	Action	
		<ul style="list-style-type: none"> • E-mail - Enter the e-mail address that you used when you registered the product. • Code - Enter the serial code sent to you from SurfControl to this e-mail address.
6	<p>The next dialog box enables you to specify the features that you want to include with this installation of Enterprise Threat Shield:</p> <ul style="list-style-type: none"> • Threat Shield Reporter - Enables you to run reports to analyze the violation and usage data collected by the system. • Stand Alone - Enables the Threat Shield Agent to run without a connection to the Threat Shield server. <p>See the Administrator's Guide Chapter 2 'Stand Alone mode" on page 14 for more information.</p>	
		<ul style="list-style-type: none"> • Reporter - Select to install the feature that can run reports on data use. • Stand Alone - Select to make this option available from the Threat Shield Manager.
7	Click Next .	
8	You will be asked to choose a destination location. Click Next to use the default of C:\Program Files\SurfControl\Enterprise Threat Shield or click Change to select a different destination then click Next .	
9	Click Install in the next dialog box to install Threat Shield.	

Step	Action
10	Threat Shield needs to run as an administrator service so must have the administrator username and password for the server on which it is being installed.
	<div data-bbox="312 432 847 831" style="display: inline-block; vertical-align: top;"> </div> <div data-bbox="903 411 1374 632" style="display: inline-block; vertical-align: top; margin-left: 20px;"> <ul style="list-style-type: none"> • Username - Enter the Administrator Username for this machine. • Password - Enter the Administrator password for this machine. • Domain - Enter the domain that this machine is a part of, if this edit field is empty. </div>
11	You will now see the Setup Complete dialog box. Click Finish .

STAGE 2

Launch Threat Shield Manager. Threat Shield Manager is the user interface for configuring policy rules. It also communicates with the Threat Shield Agent software that searches specified areas of the network.

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

STAGE 3

Deploy Enterprise Threat Shield's Agent on the workstations in the network. For more information see “Implementation Strategies” on page 11. 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, or XP Professional 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.


Procedure 2 Installing Agents remotely

Step	Action
1	Open the Workstation Deploy and Status window either by selecting Workstation Deploy 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 2 'Activating the Deployment Process' on page 13.

STAND ALONE REMOTE DEPLOYMENT

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

Procedure 3 Stand Alone Remote Deploy

Step	Action
1	Open the Workstation Deploy and Status window either by selecting Workstation Deploy 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: <ul style="list-style-type: none"> • 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. Right-click the node you wish to apply Stand Alone to.
3	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.
4	Select the Deploy check-box corresponding to these workstations to deploy them in Stand Alone mode. Refer to the Administrator's Guide: Chapter 2 'Using Stand Alone mode" on page 15 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 or awareness.

- If you don't want to use Stand Alone mode insert the following command into the user's logon script:
`start \\server\EnterpriseThreatShield\ThreatShieldAgent.exe`
- If you want to be able to deploy the Agent in Stand Alone mode follow Procedure 4.


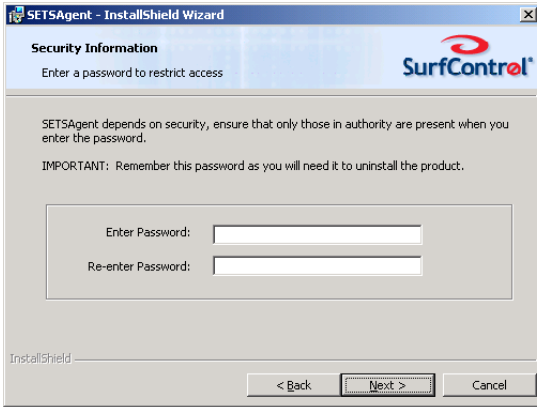
Procedure 4 Installing Agents using a logon script

Step	Action
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	<p>Insert the following command line into the users' logon script:</p> <pre>msiexec /i <path to .msi file (e.g. \\servername\sharefolder\SETSAgent.msi)> SA_SRV_NAME=<the name of the server where ETS is located> SA_cli_PASSWD=<uninstall protection password> /qn /i <log file path and name>.</pre> <p>Example: <code>msiexec /i \\Server1\EnterpriseThreatShield\SETSAgent.msi SA_SRV_NAME=Server1 SA_CLI_PASSWD=Abc123 /qn /i C:\SETSAgentInstall.log</code></p>
3	<p>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 is an example of the script showing available parameters:</p> <pre>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></pre> <p>FOR EXAMPLE:</p> <pre>cscript SETSAgentGenMst.vbs SETSAgent.msi customer.mst /server:ETS server /passwd:abc123 /continue:1</pre> <p>The following are parameters that can be entered:</p> <ul style="list-style-type: none"> • SA_CLI_PASSWD= <password> - this password will be used for uninstall authentication. • SA_CLI_UNINST_PASSWD= <password> - the password that must be entered during uninstal. • SA_SRV_NAME= <Threat Shield server name (or IP address)>. This parameter MUST be entered. • SA_CONT_INSTALL - specifies whether the installation must continue in the event of the connection to the server failing. <p>You can also enter the following .msi flags during the installation if required:</p> <ul style="list-style-type: none"> • /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).
4	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 "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.

Procedure 5 Stand Alone Independent Installation

Step	Action
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	The next dialog box asks for the name or IP address of the Threat Shield server. Enter this information and click Next .
	 <ul style="list-style-type: none"> • Server - the name or IP address of the machine on which Enterprise Threat Shield is installed.
5	Once you click Next you will see a dialog box asking you to create a password for uninstalling the client. This password will be copied across to the .msi file and works in the same way as the SA_CLI_UNINST_PASSWD parameter in Step 3, Procedure 3. If you don't want to add a password, you can leave the text boxes blank and click Next .
	 <ul style="list-style-type: none"> • Enter Password - enter a password • Re-enter Password - re-enter the password
6	Click Next .
7	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.
8	Click Finish .

Setting up Enterprise Threat Shield

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.

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.

Procedure 6 Obtaining a registration code for Enterprise Threat Shield

Step	Action
1	In the Threat Shield Manager main window, select About from the Help menu. The About Threat Shield Manager window is displayed.
2	Click Order to access the SurfControl web site. A registration form is displayed.
3	Complete the registration form. 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.

Procedure 7 Implementing the Long-Range Assessment method

Step	Action
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.

Procedure 8 Implementing using the Targeted method

Step	Action
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.

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.

Procedure 9 Implementing using the Rapid Response method

Step	Action
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:

Procedure 10 Monitor violations

Step	Action
1	Click the Workstation Activity toolbar icon  or select Workstation Activity from the Tools menu. You will see the Workstation Activity window, showing violations in real time.
2	Once the Workstation Activity window is open it will show the workstation involved, the rule that was violated (if any), the date that this occurred and the associated message. No violations that occurred prior to opening the window will be shown.
3	Use this information to create your policy.

Stage 2



Create a policy to manage these violations.

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

Term	Description
FileWatch	Controls the storage of unauthorized files or applications. FileWatch searches for 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.
WriteWatch	Controls the downloading or copying of unauthorized files/applications into file system folders. WriteWatch monitors and protects areas of the network or local drives from infection by recreational or malicious files or applications. It also detects, terminates and cleans existing spyware, and stops new installations.
.exeWatch	Controls the unauthorized usage of applications. It monitors running applications, such as Spyware, 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.
BrowseWatch	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 usage.

Further Configuration

Procedure 11 Creating the policy

Step	Action
1	Choose one of the methods outlined in the preceding Implementation Strategies section as a means of implementing the policy.
Create a new Who component	
2	Right-click the Who node in the Component tree and select Add 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.
Create a new .exeWatch component	
4	Right-click the .exeWatch node in the Component tree and select Add from the drop-down menu. By default the object's name will be .exeWatch 3 and the working days and hours will be selected.
5	Click the All button  to ensure that this rule will be applied during all hours.
Create a new rule	
6	Select Add from the Rule menu. A new rule will appear with the default name of Rule 3.
7	Select Who 2 and .exeWatch 3 to be part of Rule 3
8	Click the Transmit configuration toolbar icon  or select Transmit configuration from the File menu.
9	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. <i>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.</i>