



Best Practices Guide:
SurfControl Enterprise Threat Shield 3.1
rev2.1, November 2005

Enterprise Threat Protection

NOTICE

© 2005 SurfControl. All rights reserved. SurfControl, SurfControl E-mail Filter, SurfControl Web Filter, SurfControl RiskFilter, SurfControl Mobile Filter, SurfControl Enterprise Threat Shield, SurfControl Report Central, Single Management Console, Virtual Control Agent, Anti-Spam Agent, Anti-Virus Agent, Virtual Learning Agent, Virtual Image Agent, and the LexiMatch logos are registered trademarks and trademarks of SurfControl plc. All other trademarks are properties of their respective owners.

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.

The purpose of this document is to provide best practice recommendations for deployment, implementation, and configuration of Enterprise Threat Shield. These recommendations are collected from experiences with customers since the first release of the product.

This guide provides specific recommendations for:

- Implementing Threat Shield into your environment.
- Installing Threat Shield Server.
- Deploying the Threat Shield agent to workstations.
- Configuring the Threat Shield Manager.

IMPLEMENTATION

SurfControl's Enterprise Protection Suite protects against threats as they attempt to penetrate your network through the three threat vectors: over the internet, through e-mail, and at the workstation through client-to-client desktop applications. SurfControl Enterprise Threat Shield stops network threats such as spyware, viruses, zombie attacks, etc., from entering your network at the desktop.

Unlike SurfControl Web Filter and SurfControl E-mail Filter, Enterprise Threat Shield has a client component that resides on the workstation, and has the power to delete files and applications. The way in which Enterprise Threat Shield identifies threats and handles these threats must be configured by you, and differs greatly from organization to organization. Because of its inherent granularity, SurfControl recommends that you analyze your environment before choosing how to identify spyware and remove it from your network.

Because every network is different, it is extremely important that you fully test Threat Shield and optimize your configuration in your environment before pushing it out to your entire enterprise.

THE IMPORTANCE OF AN IMPLEMENTATION PLAN

Enterprise Threat Shield protects against malicious threats that infect the workstation via desktop applications by giving you control over those applications -- control over what applications and files you allow, and which *action* Threat Shield takes if it detects something on the workstation that's not allowed.

This *action* can range from logging the details of what Threat Shield found (such as which workstations had the most spyware or which workstations use peer-to-peer) to preventing files from being loaded onto the workstation, to actually deleting files.

SurfControl recommends that you fully test Threat Shield before deploying it across the enterprise. This is best accomplished by deploying the agent to a limited number of computers (SurfControl recommends under ten), and configuring this test group with the rules and corresponding actions you would like to use for the entire enterprise. During this process, SurfControl recommends that you run reports and continually analyze the changes Threat Shield is making to the test workstations. If you also have SurfControl Web Filter, you can run Web Filter reports on internet categories (e.g., Spyware, Peer-to-Peer, etc.) relevant to desktop activities.

Customers are often surprised by the results from this testing process. Although Threat Shield provides out-of-the-box spyware protection, it is important that you configure the nuances of this protection to fit your own environment. Otherwise, you may inadvertently configure Threat Shield to delete files that are not spyware files, or you may configure Threat Shield to needlessly scan for allowed desktop applications, or scan too frequently, or scan during high productivity periods.

Depending on the needs of your organization, SurfControl recommends one of the implementation strategies listed below.

Long-Range Assessment Implementation Plan

This is the most-recommended implementation, since it allows for the maximum amount of time to fully assess your environment and unique needs and behaviors that Threat Shield can address. This approach provides a deep understanding of problems on the network, but takes 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 using the Long-Range Assessment method:

- 1 Disable all the rules.
- 2 Change the default rules so that they only have the “Generate Report” action.
- 3 Deploy the agent to your entire network.
- 4 Assess the impact and success of the deployment.
- 5 Examine the reports.
- 6 Create or modify rules incrementally for more active enforcement.
- 7 Examine the reports.
- 8 Further modify rules, 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 using the Targeted method:

- 1 Deploy the agent to the workstations you have identified as needing spyware or application control (50 or fewer workstations).
- 2 Assess the impact and success of the deployment.
- 3 Configure rules that remove spyware and/or targeted desktop activities.
- 4 Examine the reports.

- .
- .
- .
- Implementation**

- 5 Choose the next group to receive spyware or application control (50 or fewer 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

This is the least-recommended implementation, since a rule that works on one machine may not be the best for all.

The Rapid Response implementation plan may be best for you 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).

To implement using the Rapid Response method:

- 1 Configure a rule for the problem.
- 2 Deploy the agent to one workstation.
- 3 Confirm success of the deployment and the rule's impact on the user and workstation.
- 4 Turn off the rule.
- 5 Deploy the agent to the entire network.
- 6 Turn the rule on for the entire network.
- 7 Examine reports and modify the rule as needed.

INSTALLING THREAT SHIELD SERVER

Enterprise Threat Shield can share a server with other applications; however SurfControl recommends that you do not install Threat Shield on a server running SurfControl E-mail Filter or SurfControl Web Filter. This configuration has not been tested and is not a supported installation.

SYSTEM REQUIREMENTS

Your sever must meet the following minimum requirements to install Enterprise Threat Shield:

Table 1 System Requirements

Supported Operating Systems	Windows 2000 Server Windows Server 2003
Applications	Microsoft .net Framework 1.1 Microsoft IIS v5 or above MSDE or Microsoft SQL Server 2000 (for Reporter) Microsoft Internet Explorer 5.5 or higher (for Reporter)
Processor	Pentium ® IV or above
Memory	256 MB or above (dependant upon network load and whether Threat Shield is the only software on the server)
Disk Space	70 MB for application
Other	Network file system: Microsoft NT / Microsoft Active directory / Novell NDS v4 or above Database: Microsoft SQL Server 2000 or MSDE for the Enterprise Threat Shield Reporter

MULTIPLE SERVERS

If you have multiple locations, multiple domains, or multiple WANs, you may need to install Threat Shield on multiple servers. When you have multiple Threat Shield servers, you must manage each server separately.

SERVER REQUIREMENTS

In order to deploy remotely, the Threat Shield server must have:

- Access to the shared folder on the workstation.
- A static IP address.
- An administrator logged on who has administrative rights on the workstation.
- The following ports open:
 - 139 (NetBIOS).
 - 445.
 - 3751. (**Note:** For details on changing this port, refer to page 7.)

Threat Shield can deploy to Windows or Novell environments. Make sure you select the appropriate directory service in the Settings dialog box prior to deployment.

DEPLOYMENT WITH A LOGON SCRIPT

If remote deployment is not appropriate for your organization, you can deploy Threat Shield using a logon script. To deploy the Threat Shield client in this way, add one of the following lines to the logon script for any Novell Client, Windows user, or group policy:

Windows Logon Script

```
start \\ETSservername\EnterpriseThreatShield\ThreatShieldAgent.exe
```

where: *ETSservername* is the name or IP address of the ETS server.

[Click here](#) for Microsoft's instructions on creating a logon script.

Novell Logon Script

```
@\\ETSservername\EnterpriseThreatShield\ThreatShieldAgent.exe
```

where: *ETSservername* is the name or IP address of the ETS server.

[Click here](#) for Novell's instructions on creating a logon script.

OPTIONAL CONFIGURATION: CHANGING THE “HEARTBEAT” PORTS

Enterprise Threat Shield uses ports 3751 and 3753 for the “heartbeat” communication between the Enterprise Threat Shield Server and the workstations. Depending on your environment, you may want to change these ports to ones you already have open on your firewall. For NAT settings, consult the documentation for your firewall.

To change the default ports Enterprise Threat Shield uses:

- 1 Locate **ThreatShield.ini** in \Program Files\SurfControl\Enterprise Threat Shield\Data.
- 2 Open ThreatShield.ini in Notepad.
- 3 Under **[TCPGeneral]**, change **Port2=3751** and **Port1=3753** to reflect the ports you want Enterprise Threat Shield to use.
- 4 Save and close the file.
- 5 Re-start the Enterprise Threat Shield server.

CONFIGURING THREAT SHIELD MANAGER

The following provides information regarding recommended settings on the Threat Shield server. You can make each setting from the Enterprise Threat Shield Manager.

THE SETTINGS DIALOG BOX

In the Settings dialog box, you can configure database connection settings, directory service settings, security settings, and update settings. To open the Settings dialog box from the Enterprise Threat Shield Manager, click the **Tools** menu and select **Settings**.

SurfControl recommends that you configure the settings listed below.

General

Under the **General** tab, if you select **Display Users** or **Display Workstations**, users or workstations become available for creating Who components for your rules. By default, both of these settings are unchecked.

In most environments, you can configure the Enterprise Threat Shield Manager to display users in the Who section of your rules component tree. In larger environments with many domain users or NDS users, the process of populating the list of users can take some time. This is because the Enterprise Threat Shield must pull all user information from your domain controller or NDS server.

For this reason, SurfControl recommends that you start by **not** displaying users.

Report File

SurfControl recommends that your users use only Internet Explorer to access Threat Shield Reporter. Under the **Report File** tab, you see the URL that users can use to access Threat Shield Reporter.

Here, set up a user account for a Threat Shield Reporter administrator, and an account for a user who can only view reports. You must create an administrator account to use the Reporter. For more information on setting up Threat Shield Reporter, see the **Reports** section of this guide.

Database

Under the **Database** tab, create and configure the database you will use for reports. You *must* create and configure a database before you can use the Threat Shield Reporter. For more information on setting up the Threat Shield Reporter database, see the **Reports** section of this guide.

Updates

SurfControl's Global Threat Experts regularly make additions to SurfControl's Threat Databases. If you have **Auto update** checked, Enterprise Threat Shield automatically checks for updates to the Threat Databases.

SurfControl recommends that you leave **Auto update** checked to ensure that your Threat Shield databases are current.

RULES

SurfControl generally recommends the following rule settings, although these recommendations can vary depending on which implementation strategy you are using.

FileWatch

To optimally and safely use FileWatch, use the following settings:

- **If you are deploying the agent to all workstations at once and FileWatch is part of an enabled rule, FileWatch immediately begins scanning all workstations included in the rule as soon as deployment occurs.**

SurfControl recommends that you enable rules that use FileWatch *after* initial deployment. This staggers the onset of FileWatch scans, balancing network resources.

- Change FileWatch to run weekly rather than the default setting of daily. Schedule FileWatch to run every Thursday, so when scanning your workstations, it will use the most recent Threat Shield Databases, which update on Wednesdays.

To change the scheduled FileWatch scan, select the FileWatch object from the Threat Shield Components tree, and click the **Schedule** button at the bottom of the screen.

For rules that apply to many users, SurfControl does not recommend selecting **Now** as a scheduled task. Rather, select **Now** only when you want to immediately run a scan on a single workstation, or on a few workstations.

- .
- .
- **Configuring Threat Shield Manager**

- Keep the default settings in the **Actions** tab, where you **do not** delete the files discovered by FileWatch. Only after you have run FileWatch using the various databases and have assessed the necessity of the files it detects on the workstations should you delete any files.
- If you have redundant instances of FileWatch, Threat Shield will make redundant scans. SurfControl recommends that you limit the number of FileWatch rules by consolidating the content that FileWatch scans for into a single rule.

For example, rather than creating a rule that uses FileWatch to scan workstations for spyware, and a separate rule that uses FileWatch to scan workstations for P2P, create one Content component that includes both spyware and P2P and use it in conjunction with FileWatch.

- While you can use FileWatch to remove the games included with Windows operating systems, these applications return when you reboot the workstations. SurfControl recommends that instead, you use .exeWatch to restrict usage of these games.

WriteWatch

For rules that use WriteWatch, SurfControl recommends that you monitor activity for a period of time before taking aggressive action.

SurfControl recommends that initially, you **do not** set the WriteWatch action to terminate the write activity. This is particularly important if you use a custom database for a rule combined with WriteWatch, as certain files may be necessary for your organization.

Only once you determine that the activity WriteWatch detects is not valuable to your company's production should you set WriteWatch to terminate the write activity.

.exeWatch

For rules that use .exeWatch, SurfControl recommends that you monitor activity for a period of time before taking aggressive action.

SurfControl recommends that initially, you **do not** set .exeWatch to terminate or delete the application files. This is particularly important if you use a custom database for a rule combined with .exeWatch, as certain executable files may be necessary for your organization.

Only once you determine that the applications .exeWatch detects are not valuable to your company's production should you set .exeWatch to terminate the application. Furthermore, SurfControl recommends that you monitor the results of this setting before setting .exeWatch to delete the application files.

BrowseWatch

BrowseWatch monitors internet activity on your network and reports this information to your Reporter database. If a user is currently browsing when BrowseWatch generates a report, the browsing session splits into multiple database entries.

To keep database size at a minimum, SurfControl recommends that you make the following settings in rules that incorporate BrowseWatch:

- Set BrowseWatch to generate a report at a minimum of every 60 minutes.
- Create exclusions for internal traffic (e.g., your internal web site), and for any other sites you are not interested in seeing in BrowseWatch reports.

REPORTS

To analyze Threat Shield's activity in your network, SurfControl recommends that you take advantage of the Threat Shield Reporter. SurfControl recommends that you use the Reporter to view what types of activity each of your rules detects. Based on that information, you can determine if you want to configure your rules to take more aggressive measures, such as removing files or terminating activity.

To use Threat Shield Reporter, you must install the following in addition to SurfControl Enterprise Threat Shield:

- Microsoft IIS version 5 or above.
- Microsoft SQL server 2000 or MSDE (residing on or off the Threat Shield server).

Note: MSDE has a 2 GB file size limit.

Additionally, you must make some initial configuration settings to use the Enterprise Threat Shield Reporter, as shown below.

DATABASE SOFTWARE

In order to use the Threat Shield Reporter, you must have Microsoft SQL Server 2000 or MSDE.

You can use an existing SQL server, or you can download and install MSDE from SurfControl's web site and install it on a server. This can be the same server on which you install Enterprise Threat Shield. To download MSDE from SurfControl's web site, click [here](#).

CONFIGURING REPORTS

Once you have SQL or MSDE running, you must create a database and configure the Threat Shield Reporter.

To set up Threat Shield Reporter with SQL or MSDE:

- 1 Open the Enterprise Threat Shield Manager.
- 2 Click the **Tools** menu and select **Settings**.
- 3 Click the **Database** tab.
- 4 From the **Database type** drop-down menu, select **SQL Server**.
- 5 In the **Database name** field, name your database (ThreatShieldDB by default).
- 6 In the **Server name** field, enter the name or IP of your SQL or MSDE server (127.0.0.1 if it is MSDE on the same server as Threat Shield server).
- 7 In the **User Name** and **Password** fields, enter the information for a user with SQL administrative privileges (you must use SQL authentication).
- 8 Choose your history information.
- 9 Click the **Test Connection** button to make sure your database connection has been established. This action creates the Threat Shield report database.
- 10 Click the **Reporter** tab.
- 11 Set an administrator name and password for viewing and editing reports.
- 12 Create a user name and password to view reports only.
- 13 Click **OK**.

To launch the Threat Shield Reporter:

- 1 Click the **File** menu and select **Open Threat Shield Reporter**.
- 2 Enter a user name and password and click **Login**.