



SUNBELT SOFTWARE

*COUNTER SPY*TM ENTERPRISE

User's Guide ***CounterSpy Enterprise***TM

Version 1.1

Use of this software is subject to the End User License Agreement found in this User Guide (the "License Agreement"). By installing the software, you agree to accept the terms of the License Agreement. Copyright (c) 2005 Sunbelt Software, Inc. All rights reserved. All products mentioned are trademarks or registered trademarks of their respective companies. Information in this document is subject to change without notice. No part of this publication may be reproduced, photocopied, stored in a retrieval system, transmitted, or translated into any language without the prior written permission of Sunbelt Software, Inc.

SBS400.1.1.B

Table of Contents

WELCOME	4
CounterSpy Enterprise Features.....	4
CounterSpy Enterprise Components.....	5
System Requirements.....	6
Obtaining CounterSpy Enterprise.....	7
Unpacking and Installing CounterSpy Enterprise	8
Running CounterSpy Enterprise.....	9
Downloading a Trial Version of CounterSpy Enterprise.....	10
Technical Support.....	11
QUICK START GUIDE	12
USING COUNTERSPY ENTERPRISE.....	15
How CounterSpy Enterprise Works.....	15
CONNECTING TO THE SERVER.....	18
GETTING TO KNOW COUNTERSPY ENTERPRISE.....	21
The CounterSpy Enterprise Toolbar.....	21
Pull down menus.....	22
Left pane.....	25
SYSTEM MANAGEMENT SECTION.....	26
Registration.....	27
Updates	29
Configuration	30
POLICY-BASED RULES.....	32
Creating Policies.....	32
Scheduling Scans	33
Setting Scan Options	34
Allowing Specific Threats	35
Setting Email Notifications	37
Setting Agent Options	39
Setting Actions.....	41
Manually Scanning Agents.....	42
AGENT DEPLOYMENT	44
What is an Agent?.....	44
Agent Communication.....	44
Deferred Communication	45
Deploying the Agent Software.....	45

Deleting and Reassigning Agents	49
VIEWING SCAN RESULTS	49
MANAGING ALL QUARANTINED ITEMS.....	52
MANAGING THREATS	52
REPORTS	53
Generating Reports and Report Options	54
Executive Summary Report.....	55
Infected Machine Summary Report.....	56
Infected Machines Detail Report	57
Machine History Report.....	58
Threats Found Summary Report.....	59
Threats Found Detail Report.....	60
Top Ten Infected Machines.....	61
Exporting Reports	62
UNDERSTANDING SPYWARE	63
What is Spyware?	63
How Spyware Gets Installed	64
Is All Spyware Hazardous?	66
Signs of Spyware Infection.....	66
Avoiding Spyware	67
Index.....	69
End-User License Agreement	73

Welcome

Welcome to CounterSpy Enterprise. CounterSpy Enterprise is designed to detect and remove a broad range of adware, spyware, and other malware from networks. It provides a policy-based, centrally managed solution that can be scaled to fit corporate needs. This chapter covers the core features and system requirements.

Features

Centralized Management - The central management console enables administrators to access and control agent deployment, threat database updates, quarantined spyware, configuration, agent policies, scan scheduling, and recommended actions to identified spyware threats.

Policy-based Rules - Use policies to define scanning options, and then assign agents to the policies.

Easy Deployment - Agents can be deployed directly from the Admin console by using push installation, or agents can be deployed by making and distributing a stand-alone installation package. The program supports multiple methods of agent deployment to allow enterprise customers flexibility in how agents are pushed to users' systems. Agents can be deployed using silent push install (using either WMI or RPC and admin shares), as an MSI file or a self-extracting executable. The deployment scheme supports Active Directory with grouping by Organizational Unit, the network browse list, or by IP address. This level of flexibility allows CounterSpy Enterprise to operate in workgroup, NT Domain, and Active Directory environments with ease.

Scanning Engine - CounterSpy Enterprise's agent scanning engine automatically scans users' systems for spyware threats. The scanning engine utilizes a robust threat signature database that includes constantly updated spyware threats from Sunbelt's spyware research team, as well as input from Sunbelt's ThreatNetSM. (ThreatNet is a worldwide network of users who report on new spyware outbreaks to Sunbelt through CounterSpy's consumer version.) The administrator can manually run a quick or deep scan of selected agent computers, or schedule scans. CounterSpy Enterprise's agent scanning engine automatically scans users' systems for spyware threats. Agents report on spyware to the central server, providing information about the spyware, assigning a threat level, and allowing the administrator one of four recommended actions: Ignore, Report Only, Quarantine, or Delete. Default actions can also be set to automatically address any spyware found based on spyware category as determined by the administrator.

Reports - Leveraging Crystal Reports, CounterSpy Enterprise includes seven pre-defined reports with the ability to generate custom reports. Included reports are: Executive Summary, Infected Machines Detail, Infected Machines Summary, Machine History, Threats Found Detail, Threats Found Summary, and Top 10 Infected Machines.

CounterSpy Enterprise Components

CounterSpy Enterprise Admin Console

The Admin Console serves as the central management console for CounterSpy Enterprise. From here, you can control agent deployment, threat database updates, quarantined spyware, configuration, scanning policies, scanning scheduling, and recommended actions for identified spyware threats. You can also view individual or group workstation data and generate reports.

CounterSpy Enterprise Server

The CounterSpy Enterprise Server stores the agent database, the threat database, and agent threat tracking information. The server uploads updated threat databases to agents, receives reports from agents (the primary traffic), and communicates with the Admin Console. This traffic can pass through firewalls that are configured to allow such traffic.

The CounterSpy Enterprise server communicates with agents by using short XML bursts (using the SOAP architecture). The number of servers is not limited under CounterSpy Enterprise licensing agreements. Depending on the domain model, an administrator can deploy as many servers, in as many locations as required.

Agent Software

Agent (client) software is installed onto computers on the network. Agents can be deployed directly from the Admin console with push installation (IP, network browse, or Active Directory machine account), or it can be deployed as a stand-alone installation package (self-extracting zip or MSI installation package). Agents report discovered spyware to the server. Agent threat databases are updated by the server.

System Requirements

Requirements for Admin Console and Policy Server

- Operating system requirements: Windows Server 2003 Server, Windows XP Professional, Windows 2000 Server with SP3, and Windows 2000 Professional with SP2.
- Minimum processor requirement is Pentium 400 MHz processor. A Pentium III or higher processor is recommended.
- Hard drive with at least 200 MB of free space is required.
- A minimum monitor display resolution of 1024 x 768 is required.
- An Internet connection is required.
- 512 MB of RAM is required.
- The server requires at least MDAC 2.6.
- The admin console requires Internet Explorer 5 or higher and MS .NET Framework 1.1.

Requirements for Workstation Agent

- Supports Windows XP Professional/Home and Windows 2000 Professional SP2 systems.

Note: Agent support for Windows NT 4 Workstation (SP6) and Windows 98SE/ME will be added in the coming months.

Obtaining CounterSpy Enterprise

CounterSpy Enterprise's most current version is available for download from the Sunbelt Software website. The latest spyware threat definitions will be included.

Purchasing Online

To purchase CounterSpy Enterprise online:

1. Go to Sunbelt-Software at: <http://www.sunbelt-software.com/product.cfm?page=about&id=400>
2. In the page that opens, scroll down and click the BUY NOW! button.



Figure 1: The BUY NOW! Button

The page that opens offers a description of CounterSpy Enterprise.

3. Click the Buy now and a form page opens.
4. Fill out the form on this page to ensure you receive Tech support and e-mail information on your product download. Fields with an asterisk (*) are required fields that must be filled out in order to download CounterSpy Enterprise.
5. When the form has been filled out, click the Continue button located next to the Reset button at the bottom of the form. (The "Reset" button will clear the form.)
6. Verify the contact information on the page that opens and fill in your payment information.
7. Click the Process My Order! button and a page opens with information and a download link for CounterSpy Enterprise.
8. Click the download link and download the .exe file.

After purchasing CounterSpy Enterprise, you will receive an e-mail containing your registration key and a text ReadMe file. Your CounterSpy Enterprise program contains an online Help system that can be accessed from the Help Menu from within CounterSpy Enterprise. Also, a PDF version of the CounterSpy Enterprise User's Manual is available from our **Resources** page at:

<http://www.sunbelt-software.com/product.cfm?page=whitepapers&id=400>

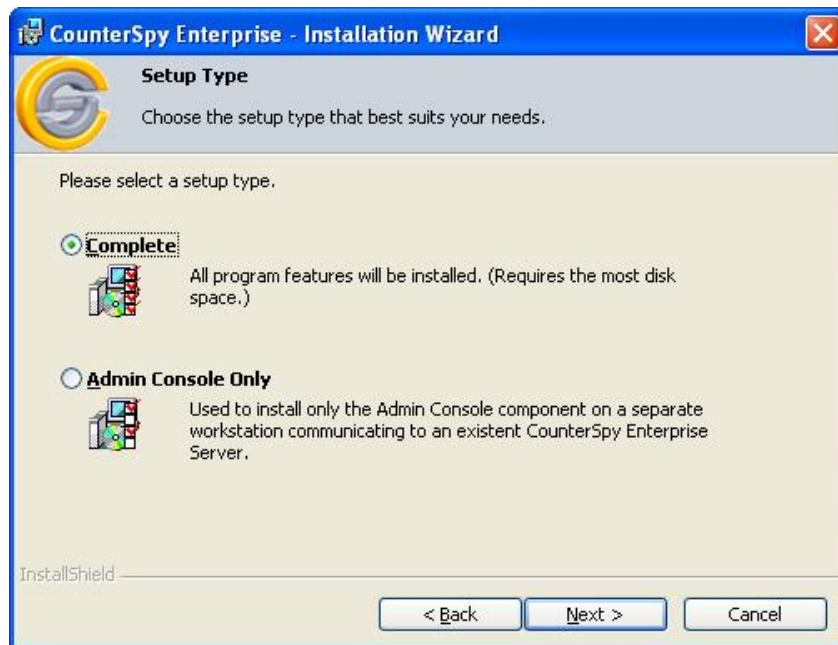
Purchasing by Telephone

You can order CounterSpy Enterprise by telephone by contacting Sunbelt Software at: 888-NTUTILS (688-8457) between 9:00am and 6:00pm EST, Monday – Friday.

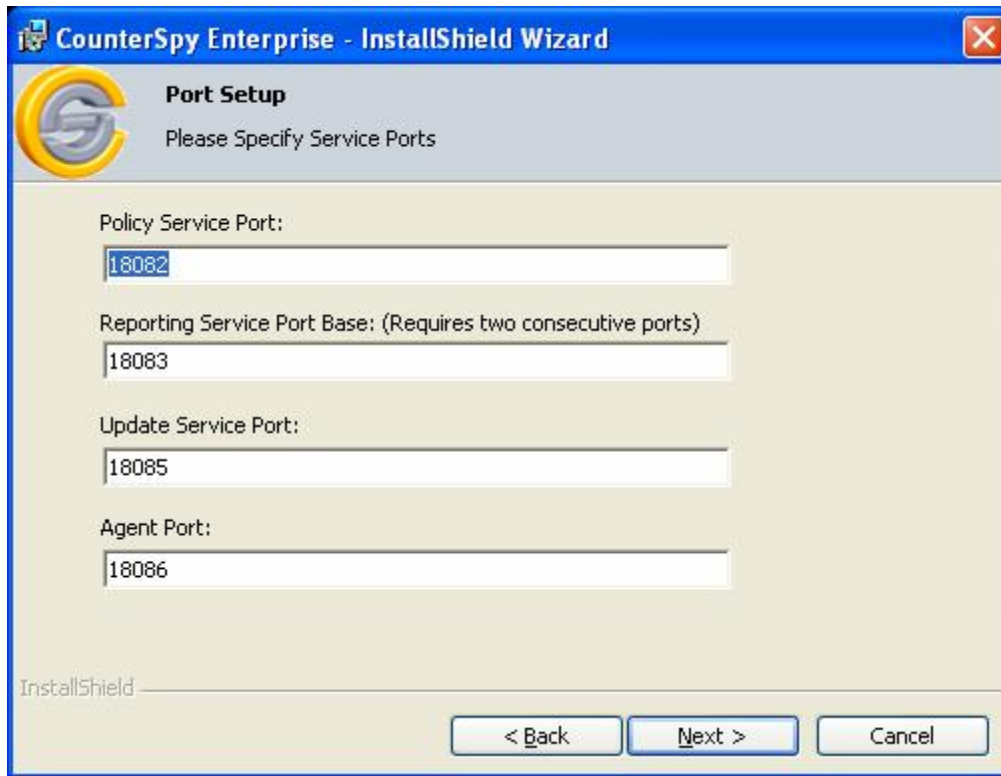
Unpacking and Installing CounterSpy Enterprise

1. Locate the CounterSpy Enterprise executable that you downloaded, make sure it is copied to your server; then, double click the file. This will begin the unpacking and installation of CounterSpy Enterprise
2. Follow the Installation instructions

The Setup type screen will display:



3. Choose Complete to install the entire admin console, policy service, update service and reporting service on the computer.
4. Choose Admin Console if you want to install the console only. This will allow you to remotely connect to a server running the CounterSpy Enterprise including the Policy, Update and Reporting services.
5. Continue the installation.
6. The Port Setup screen will display:



The default port numbers for the Policy Service, Reporting Service, Update Service and Agent are set to 18082, 18083, 18085 and 18086 respectively (18084 is also used for retrieving information to produce Reports). Sunbelt recommends choosing the default options for all of these ports. You may change the port numbers to ones that suit your organizations needs. However, port 18084 is required displaying reports.

7. Finish the installation. CounterSpy Enterprise will now be installed on your system.

Running CounterSpy Enterprise

To run CounterSpy Enterprise:

- Select your Windows Start button, then click **Programs>Sunbelt Software >CounterSpy>CounterSpy Enterprise**.

Before CounterSpy Enterprise is registered, it will be in an evaluation mode. This mode will limited you to installing a cumulative total of five agents and will run for a maximum of 30 days. Once your evaluation period has expired, you will only be allowed to uninstall and remove agents. Extended evaluation licenses are available from any Sunbelt Sales Representative.

Downloading a Trial Version of CounterSpy Enterprise

You can download a 30-day trial of CounterSpy Enterprise from the Sunbelt-Software web site at:

<http://www.sunbelt-software.com/product.cfm?page=about&id=400>.

Prior to registering, the program can be set to scan up to five machines for spyware in trial mode. CounterSpy Enterprise requires a key which will activate the program for full operation. Extended evaluation licenses are available from any Sunbelt Sales Representative. After the evaluation period expires, the Agent software may be removed using the Console.

When you purchase CounterSpy Enterprise from our Web site, you will receive an e-mail containing your registration key and a text ReadMe file.

A PDF version of the CounterSpy Enterprise User's Manual is available for download from the Resources page at:

<http://www.sunbelt-software.com/product.cfm?page=whitepapers&id=400>.

To download a trial of CounterSpy Enterprise:

1. Go to Sunbelt-Software at <http://www.sunbelt-software.com/product.cfm?page=about&id=400>.

At the top of the Sunbelt-Software Web page, just under the Sunbelt-Software logo is a second navigation bar.

2. Click the Download link in the navigation bar and the "Downloads" page opens.
3. Fill out the form on this page to ensure you receive Tech support and e-mail information on your product download. Fields with an asterisk (*) are required fields that must be completed in order to download CounterSpy Enterprise.)
4. When the form has been filled out, click the Download button located next to the Reset button at the bottom of the form. (Reset will clear the form.)

After clicking the Download button a page will open with the downloadable executable link.

5. Click the executable link and the Explorer download window opens.
6. Click the Save button and CounterSpy Enterprise will begin downloading.

After downloading the file, you are ready to unpack and install CounterSpy Enterprise.

NOTE: Prior to registering, the program will scan up to five machines for a maximum of 30 days and then become inoperable. CounterSpy Enterprise requires a registration key which will activate the program for full operation (see Registering below).

Technical Support

If the information in this guide does not resolve a situation or question that you have, or if you have a question about updating your version of CounterSpy Enterprise, please contact the Sunbelt Customer Support Center. You will find the contact information is below:

Telephone (USA)	1-877-673-1153
Telephone (International)	1-727-562-0101
E-main	support@sunbelt-software.com
Web site URL	www.sunbelt-software.com/kb.cfm
Hours:	9 a.m. to 6 p.m. EST

Quick start guide

In order to rapidly orient you to the features of CounterSpy Enterprise, you can use the following “quick start” to get up and running.

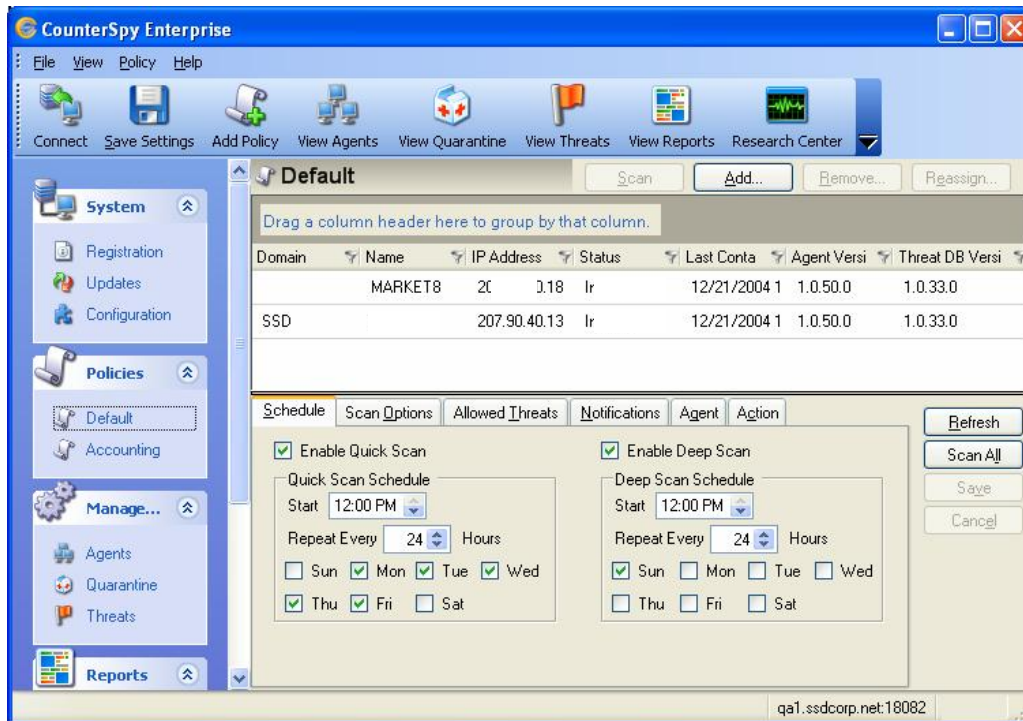
1. Install CounterSpy Enterprise, using the default options.
2. Launch the CounterSpy Enterprise console and connect to the machine onto which you just installed the program. For the Server name, use the machine onto which you have installed the program. For user name and password, use a name that has administrative privileges to that system. Leave the port number as the default 18082.



The screenshot shows the CounterSpy Enterprise console login interface. At the top, the 'COUNTERSPY' logo is prominently displayed. Below the logo, the Sunbelt Software logo and the website 'www.sunbelt-software.com' are visible, along with a copyright notice for 2004. The main area of the window contains a login form with the following fields: 'Server' (a dropdown menu showing 'Computer.domain.net'), 'Port' (a text box containing '18082'), 'User name' (a text box containing 'administrator'), 'Password' (a text box with masked characters), and 'Domain' (a dropdown menu showing 'domain.net'). There is also a 'Save Password' checkbox and two buttons labeled 'Logon' and 'Cancel'.

Launch CounterSpy Enterprise Console

3. Enter your registration number. In evaluation mode, leave the registration number blank. If you have an extended evaluation number, enter it.
4. On the left pane, select the Default Policy under Policy.



Add machines to the policy

5. Add a machine to the policy by choosing **Add** in the upper right-hand corner.
6. Choose a machine from the domain to which you have administrative privileges. Note that if you have simple file sharing enabled on that system, you will not be able to deploy an agent from the console. Instead, you will want to choose Manual Deploy from the Policy pull-down menu, which will allow you to create a self-extracting file installation package or an MSI file.
7. After adding a machine to a policy, you can deploy and agent. Click Deploy Agent on the toolbar to open the Agent Deployment Wizard; then go through the wizard.
8. After the agent is deployed, select the Agent and click the Scan button on the default Policy window (or by right-clicking on the agent) to find and detect spyware on that system.
9. Press Refresh on the right-hand side to update the status of the scan. (Note that a Quick Scan can be extremely fast—often under a minute.)
10. Once the scan is completed, go to Agents under the Management section on the left-hand pane to view the scan results.
11. From there, select the machine and below, you will see the list of quarantined spyware and a scan history.

Congratulations!

You've just cleaned a system of spyware using CounterSpy Enterprise!

For further information, refer to the documentation. Also, don't hesitate to contact one of our friendly technical support people at www.sunbelt-software.com/support (choose "Ask a Question") for any assistance you may need.

Using CounterSpy Enterprise

CounterSpy Enterprise uses standard Windows interface conventions to help you accomplish your tasks in a familiar environment.

While most advanced users are familiar with these conventions, we have clarified a few to make sure you are able to use the product to its full effectiveness:

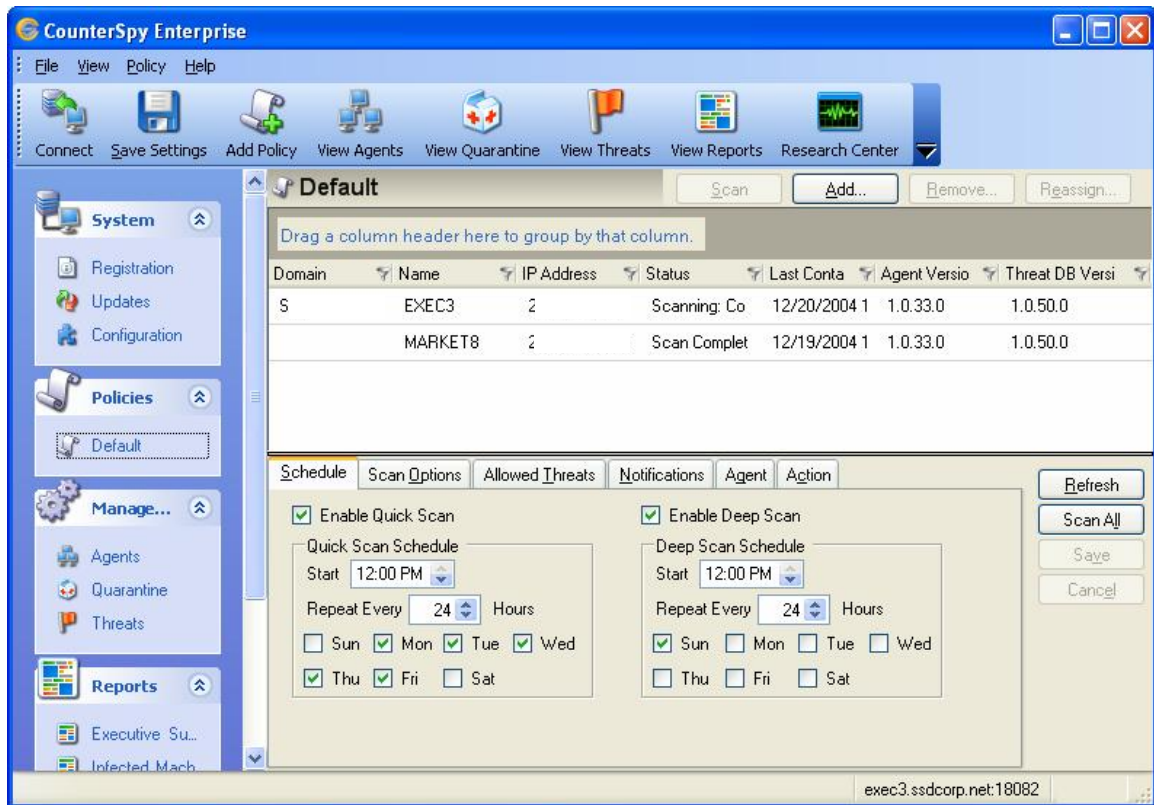
1. Moving the toolbar and the pull-down menus. You can move these toolbars and pull-down menus by simply dragging them using the drag bars on the left to a new location.
2. Columns. You can sort by column headers by clicking on the column name. You can also filter items by choosing the filter (🔍) icon.
3. The major sections (System, Policies, Management and Reports) can be expanded or contracted by pressing on the expansion button (⌵) or the contraction button (⌶).

How CounterSpy Enterprise Works

CounterSpy Enterprise allows you to create policies and assign machines to that policy via Active Directory with grouping by Organizational Unit, the network browse list, or by IP address. Agents can be deployed using silent push install (using either WMI or RPC and admin shares), as an MSI file, or as a self-extracting executable that you can install via login scripts, Add to a Group Policy, or by letting the end user install via a Web page. This level of flexibility allows CounterSpy Enterprise to operate in workgroup, NT Domain, Active Directory environments with ease. From a single admin console, you control installation of the agent, scheduling, and threat database updates for just a few dozen, hundreds, or thousands of machines to protect your entire network from over 36 categories of spyware.

The Management Console

The CounterSpy Enterprise Management Console was built from the ground up with the goal to get you easy and fast control over policies, assigning the correct policy to the right groups of workstations, and being able to either immediately either 'quickscan' or 'deepscan' for spyware or schedule it for running at a later time.



CounterSpy Enterprise Admin Console

Active Directory Support: Create a policy, and interface with AD to assign this policy to any group of workstations.

Spyware Severity Level: There are many categories of Spyware, some are relatively harmless, others are an immediate emergency. You can select what action to take for which category on a global or workstation level.

Four Ways to Deploy Agents - From your Admin Console you assign agents to a Policy. From there the agents will be deployed via a silent push-install. Apart from that, the agent is available as an "MSI" file and an .exe that you can install via login scripts, deploy with SMS, add to an Active Directory Group Policy, or let the end user install via an Intranet web page.

Protects from a Wide Range of Spyware Threats - Sunbelt Software has its own dedicated Spyware Research Team that does independent spyware research but also gets a continuous feed of newly detected spyware from Sunbelt's ThreatNet. Our Research Team will test removal methods of any spyware and update the spyware threat database in near real-time. CounterSpy Enterprise scans for and removes 36 different categories of spyware from "Adware to Worms."

Browse Spyware Threats - To browse the thousands of threats in the database, check out the "Spyware Library Browser". Scan For In-Memory Threats, In Registry and on Disk: CounterSpy Enterprise allows you to scan for these threats, either with the "scan now" button or scheduled. It provides options for both quick-scan and deep-scan that you can run at different times.

Schedule Your Scans: CounterSpy Enterprise scheduler lets you manage scan times and locations from your Admin Console.

E-mail Alerts: you can specify who gets an email when critical spyware has been detected on a user's workstation.

Compatibility with Other Tools: CounterSpy Enterprise allows transparent coexistence with other security tools like Firewalls, VPN's and Anti-Virus products.

Enormous Admin Time-saver: Your Admin Console is the central point of control for all the threat database updates. Clients do not need to download their own threat database updates via the Net saving bandwidth. CounterSpy Enterprise Server and CounterSpy Enterprise agents on your workstations communicate via XML/SOAP and the threat database is optimized for size so does not cause a lot of network traffic.

Client Server Architecture, .Net Compliant

CounterSpy Enterprise has a Client Server architecture, is .NET compliant, and consists of three components. The Admin Console, CounterSpy Enterprise Server and the CounterSpy Enterprise Agents that sits on each workstation. Agents communicate to the Server via short and small SOAP/XML bursts, preventing bandwidth bottlenecks. CounterSpy Enterprise supports both the MS Access and MS SQL Server databases for easy scalability to any number of agents.

Flexible and Complete Reporting

CounterSpy Enterprise has Crystal Reports built in, and comes with seven canned reports, but you can generate your own custom reports if you need anything specific. Here are your built-in, ready-to-run reports. You may never need anything more than these...

- Executive Summary
- Infected Machines Detail
- Infected Machines Summary
- Machine History
- Threats Found Detail
- Threats Found Summary
- Top 10 Infected Machines

Connecting to the Server

The number of servers is not limited under CounterSpy Enterprise licensing agreements. All that is required is sufficient licenses for deployed agents. Depending on the domain model, an administrator can deploy as many servers, in as many locations as required.

To connect to server when starting CounterSpy Enterprise:

1. On a machine with console installed, click on the CounterSpy Enterprise icon. Enter or select a server name or IP address. This will be the server on which CounterSpy Enterprise is installed. CounterSpy Enterprise includes the CounterSpy policy service, CounterSpy reporting service and the related database. If you installed CounterSpy Enterprise on your local system, type the machine name of your local system.
2. Enter a Port number. The port number is the one assigned to the Policy Service during installation. The default port is 18082.
3. Enter your User Name and Password. You must have administrator rights to the console machine and any agent machines.
4. Enter or select a domain or workgroup name.
5. Check Save Password to retain login information for future connections.
6. Click Logon.



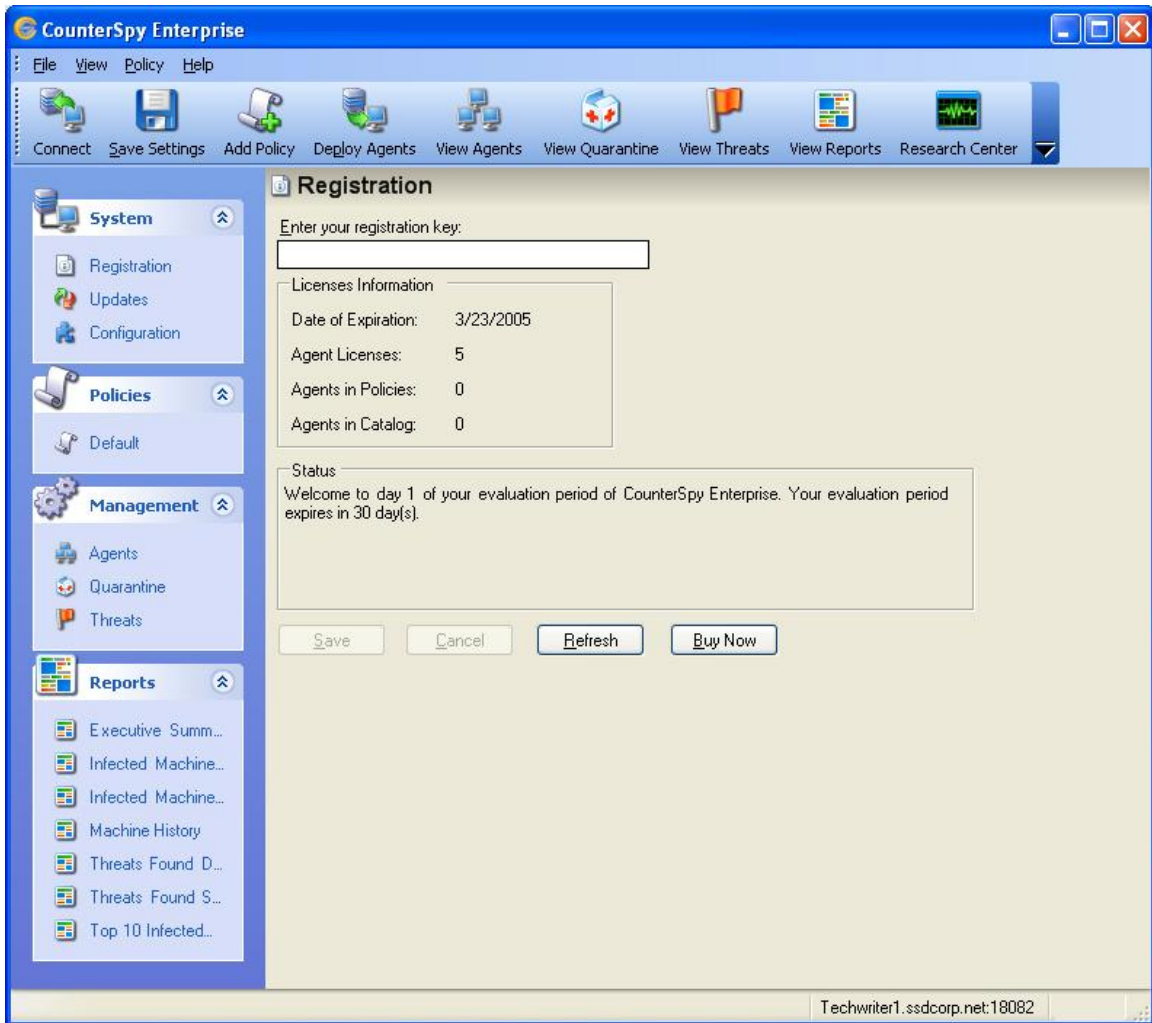
The image shows a login dialog box for CounterSpy. At the top, the text "COUNTERSPY" is displayed in a large, stylized font. Below this, the Sunbelt Software logo and name are visible on the left, and the website "www.sunbelt-software.com" and copyright information "Copyright © 2004 Sunbelt Software. All rights reserved." are on the right. The main area of the dialog contains several input fields: "Server:" with a dropdown menu showing "qa", "Port:" with a text box containing "18082", "User name:" with a text box containing "e", "Password:" with an empty text box, and "Domain:" with a dropdown menu showing "S". At the bottom left, there is a checkbox labeled "Save Password" which is currently unchecked. At the bottom right, there are two buttons: "Logon" and "Cancel".

Login to the Policy Server

To connect to a server from inside CounterSpy Console:

1. Click Connect on the Toolbar.
2. On a machine with console installed, click on the CounterSpy Enterprise icon. Enter or select a server name or IP address. This will be the server on which CounterSpy Enterprise is installed. CounterSpy Enterprise includes the CounterSpy policy service, CounterSpy reporting service and the related database. If you installed CounterSpy Enterprise on your local system, type the machine name of your local system.
3. Enter a Port number. The port number is the one assigned to Policy Service during installation. The default port is 18082.
4. Enter your User Name and Password. You must have administrator rights to the console machine and any agent machines.
5. Enter or select a domain or workgroup name.
6. Check Save Password to retain login information for future connections.
7. Click Logon.

Once connected to a server, you will get the CounterSpy Enterprise console registration screen.



CounterSpy Enterprise opening screen




Getting to know CounterSpy Enterprise


CounterSpy Enterprise is laid out by function, with the top toolbar and pull-down menus providing many functions that are also available on the left pane.





The CounterSpy Enterprise Toolbar



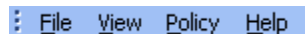
The CounterSpy Enterprise toolbar gives you quick access to commonly used CounterSpy Enterprise features. By default, the toolbar appears at the top of the CounterSpy Enterprise screen. You can move it to another location by clicking the vertical bar to the left of the word "Connect". The toolbar includes the following buttons.

 Connect	Connect —Connects to a CounterSpy Enterprise policy server. This will be the server on which a CounterSpy Enterprise policy service is installed. If you installed CounterSpy Enterprise on your local system, type the machine name of your local system
 Save Settings	Save Settings —Saves your settings for the pane which is active. For example, if you made a configuration change in the Agent pane, you could save the new settings by choosing this option. Note: If you make a change without choose Save Settings, you will be prompted to save the changes when you exit the program or change panes.
 Add Policy	Add policy —Adds a policy, from which you can deploy agents and manage them according to your policy-based preferences. For more information, refer to the Policies section on page 25.

 <p>Deploy Agents</p>	<p>Deploy Agents—Opens the Agent Deployment Wizard to walk you through deploying a new agent.</p>
--	--

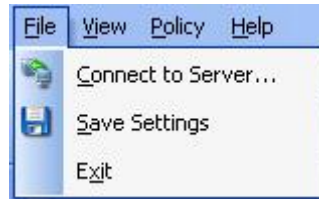
 <p>View Agents</p>	<p>View Agents—Takes you to the agent pane. For more information on agents, see the section on Agents on page 37.</p>
 <p>View Quarantine</p>	<p>View Quarantine- Takes you to the Quarantine pane, where you can view items that have been quarantined by the CounterSpy Enterprise agents.</p>
 <p>View Threats</p>	<p>View Threats— Takes you to the CounterSpy Enterprise Threat Database. This is a listing of all threats that are detected by agents. For more information, refer to the Threats section on page 43.</p>
 <p>View Reports</p>	<p>View Reports—Takes you to the Reports pane. For more information on Reports, refer to the Reports section on page 44.</p>
 <p>Research Center</p>	<p>Research Center—Takes you to Sunbelt's spyware research center, where you can research spyware threats discovered by Sunbelt, submit new spyware found, and more.</p>

Pull down menus



The pull-down menus include four pull-downs: File, View, Policy and Help. You can move the toolbar to another location by clicking the vertical bar to the left of the word "File". The toolbar includes the following items.

File menu



File menu

The file menu provides the following features:

Connect to Server - Connects to a CounterSpy Enterprise policy server.

Save Settings - Saves your settings for the pane which is active. For example, if you made a configuration change in the Agent pane, you could save the new settings by choosing this option. Note: If you make a change without choose Save Settings, you will be prompted to save the changes when you exit the program or change panes.

View menu



View menu

The view menu provides access to the following features:

Registration - Takes you to the Registration Pane

Updates - Takes you to the Updates pane

Configuration - Takes you to the Configuration pane

Policy - Selects a Policy.

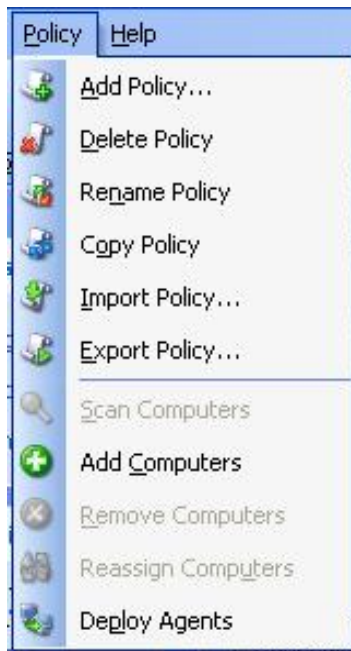
Agents - Takes you to the Agent pane.

Quarantine - Takes you to the Quarantine pane.

Threats - Takes you to the Threats pane.

Hide Group By Box - Removes the “Group By” box in the various panes.

Policy menu



Policy menu

The Policy pull-down menu provides a range of features related to Policies, computers and agent deployment.

Add, Delete or Copy Policies —Each of these menu items allow you to create, remove or copy policies.

Import Policy— Allows you to import an XML file with policy information. These

XML files are created with the Export Policy feature.

Export Policy—Allows you to create an XML file with pre-defined Policy information for whatever policy is selected.

Scan Computers—Scans systems for spyware. The active policy (whichever one you have on the screen) will be the policy used for scanning.

Add Computers—Adds computers to the selected policy.

Remove Computers—Removes selected computers from a policy.

Reassign Computers—Assigns selected computers to a different policy. You will need to have a policy created before you can assign a computer to it.

Deploy Agents—Deploys selected agents on a selected system.

Left pane



Left pane

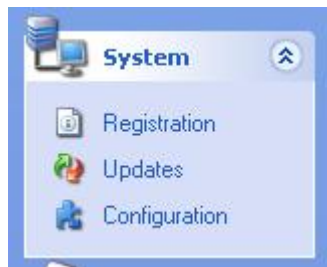
The **System Management** section gives you the ability to manage your configuration, updates and registration.

The **Policy** section allows you create and manage policies.

The **Management** section allows you manage agents, the spyware threat database and quarantined spyware.

The **Reports** section gives you access to CounterSpy Enterprise's reports.

System Management Section

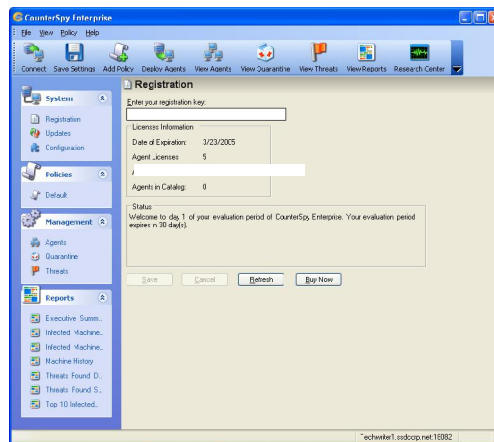


System management section

Under the System Management section, there are three primary pages related to managing your CounterSpy Enterprise configuration. These are Registration, Updates and Configuration.

Registration

The Registration page is displayed when CounterSpy Enterprise starts. If it is the first time CounterSpy Enterprise has been used, enter the registration key. No registration number is needed in evaluation mode. If you have an extended evaluation key, enter it.



CounterSpy Enterprise registration screen

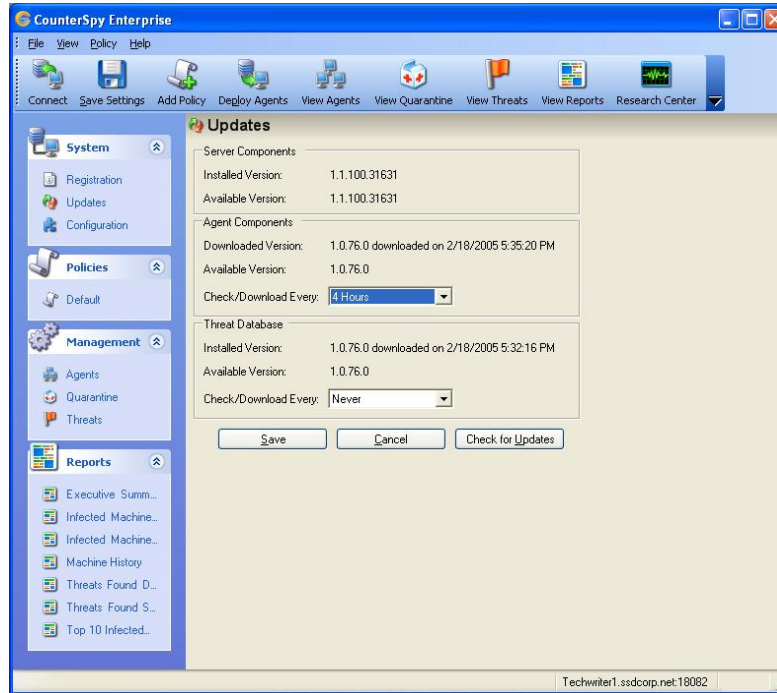
When using CounterSpy Enterprise, you can return at anytime to the Registration page to view registration and license details.

To view registration and license information:

1. Expand System in the left pane, and then click Registration.
2. Under Licenses Information, an administrator can review:
Date of Expiration - when the CounterSpy Enterprise license agreement expires
Agent Licenses - how many agent licenses are authorized by the registration.
Agents in Policies - how many agents are currently deployed and assigned to policies.
3. Under Status, an administrator can review the status of the current registration:
Eval Mode (allows usage until evaluation period expires)
Normal Mode (good for normal usage)
Over Usage (more machines deployed than are licensed)
One Month Countdown (countdown for maintenance)
Expired Updates (expired maintenance)
Expired Evaluation (the evaluation period has expired)
Revoked Registration (unrecognized license, please call customer service)
4. Click Refresh to view the most current registration information.
5. Click Buy Now to access the Sunbelt Software, CounterSpy Enterprise Website or to purchase additional licenses.

Updates

On the Updates page, you can manually update the CounterSpy Enterprise server with current CounterSpy Enterprise components, and can set a schedule for automatic updates of agent and threat database components.



CounterSpy Enterprise updates screen

Whether or not updates are automatically passed from server to agent depends upon your Agent settings in the Policy to which the agent is assigned.

To manually update all components:

1. Expand System in the left pane, and then click Updates.
2. Click Check for Updates.

Server and Agent Updates

Server and Agent updates are self-installing updates that are designed to replace existing software code. They are designed to extend or adjust product performance.

In some instances, updating the Server or Agent updates will require a reboot of the server or (rarely) the client system where the agent resides. Updating these components is only recommended if the administrator is in a position to perform a reboot.

To schedule agent updates:

1. Expand System in the left pane, and then click Updates.
2. Under Agent Components, set Check/Download Every to how frequently CounterSpy Enterprise will check for agent component updates.
3. Click Save.

Threat Database Updates

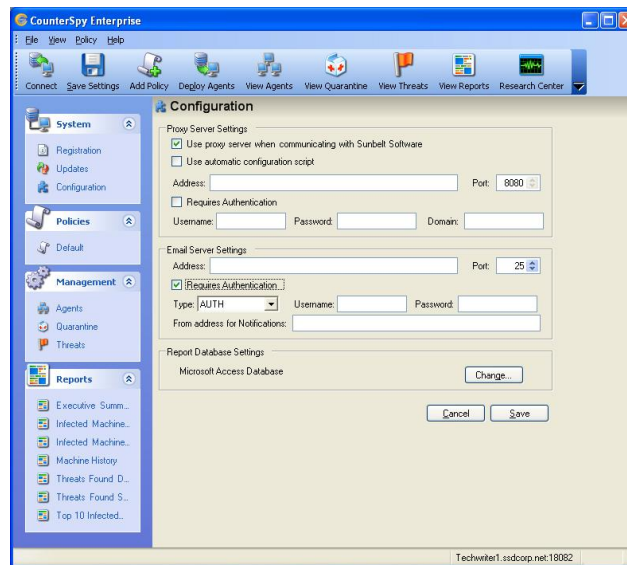
Threat Database updates are updates to CounterSpy Enterprise's spyware definition files, and are the result of research from Sunbelt's spyware research team. They contain specific signature information about spyware threats. Keeping current with the latest definitions is critical, as they allow CounterSpy Enterprise to detect and remove the latest discovered spyware, adware, trojans and worms.

To schedule threat database updates:

1. Expand System in the left pane, and then click Updates.
2. Under Threat Database, set Check/Download Every to how frequently CounterSpy Enterprise will check for Threat Database updates.
3. Click Save.

Configuration

The configuration section sets optional parameters for CounterSpy Enterprise, including proxy server settings (if any) and email settings. The email settings will allow you to get notifications about what spyware is found by policy and severity.



CounterSpy Enterprise configuration screen

To set Proxy Server Settings

1. Expand System in the left pane, and then click Configuration.
2. Select the Use Proxy server when communicating with Sunbelt Software box to activate Proxy Server settings.
3. Enter the Proxy server IP address; then enter which Port to use, or select the Use automatic configuration script box to automatically select the port.
4. Click Save.

To set Email Server Settings

5. Expand System in the left pane, and then click Configuration.
6. Enter the SMTP Server Address.
7. Enter the SMTP Server Port to use.
8. Check Require Authentication, and then enter the Username and Password. If authentication is required for the email, mark the check box **Select an authentication type**.
9. Enter a From address for notifications; then, click Save.

To change the Report Database Settings

1. Expand System in the left pane, and then click Configuration.
2. Click **Change...** under Report Database settings. The Report Database Location dialog box opens.
3. Make a selection:
 - Select **Microsoft Access**, click **Browse**, go to the location or you database; then, click **OK**.
 - Select **SQL Server**; then, enter the server information.
4. Click OK.

Note: It is recommended that you use either the Access database shipped with CounterSpy Enterprise or select the SQL server option. The report tables will be available with either of these options. If you choose to use another Access database you will have to recreate the tables or use a copy of the database included with the software.

Policy-Based Rules

Creating Policies

Use policies to define scanning options, and then assign agents to the policies. In this way, an administrator can group computers and handle special workstation needs. CounterSpy Enterprise ships with a default policy.

In a policy an administrator will define the scanning schedule, scanning options, what specific threats are allowed, how to handle notifications, how agents are updated, if agents see an icon when their machine is being scanned, what message agents see when a reboot is required, and what actions to take when specific threats are encountered.

To add a policy:



CounterSpy Enterprise Toolbar

1. Click Add Policy on the menu bar, or choose Policy menu | Add Policy.
2. Enter a name for the new policy. Policy names must be unique.



Left pane Policy Selection

To delete a policy:

1. You must first Remove or Reassign all agents to another policy before deleting the current policy (you cannot delete the Default policy).
2. Expand Policies in the left pane, and then select the policy to be deleted.
3. Confirm that you wish to delete the policy by click the Yes button.

To rename a policy:

1. Expand Policies in the left pane, and then select the policy to be renamed.
2. Choose the Policy menu | Rename Policy.
3. Enter a name for the policy. Policy names must be unique.
4. Click OK to accept the new policy name.

To add a policy by copying another policy:

1. Expand Policies in the left pane, and then select the policy to be copied.
2. Choose the Policy menu | Copy Policy.
3. Enter a name for the new policy. Policy names must be unique.

To add a policy by importing it from a saved policy file:

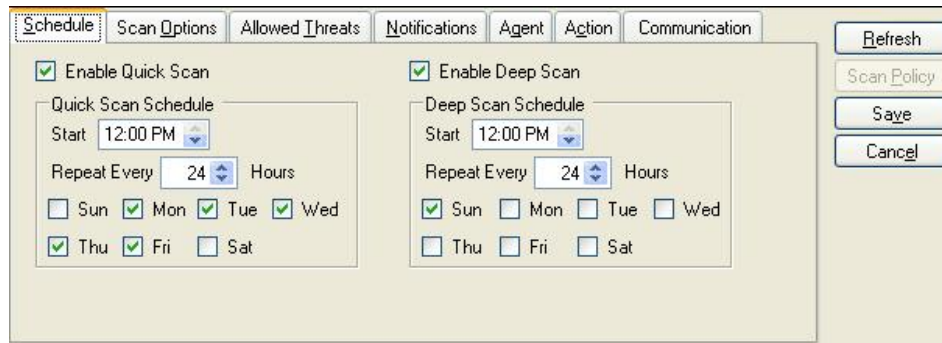
1. Choose Policy menu | Import Policy.
2. Select a policy XML file from Import Policy dialog.
3. And click the open button.
4. Enter a name for the new policy name.
5. Only the settings of the exported policy will be imported. Agents that were on the policy before it was exported will be added to the new imported policy.

To export policy settings to an XML:

1. Expand Policies in the left pane, and then select the policy to be exported.
2. Only the policy settings will be saved into the XML file. Agents on the policy will not be exported.
3. Enter a name for the XML file that the policy settings will be saved into.
4. Click the Save button.

Scheduling Scans

Use the Schedule tab within a policy to define when spyware scans are performed on the computers assigned to that policy. Only computers that have agents deployed to them will be scanned.



Schedule tab in policy settings

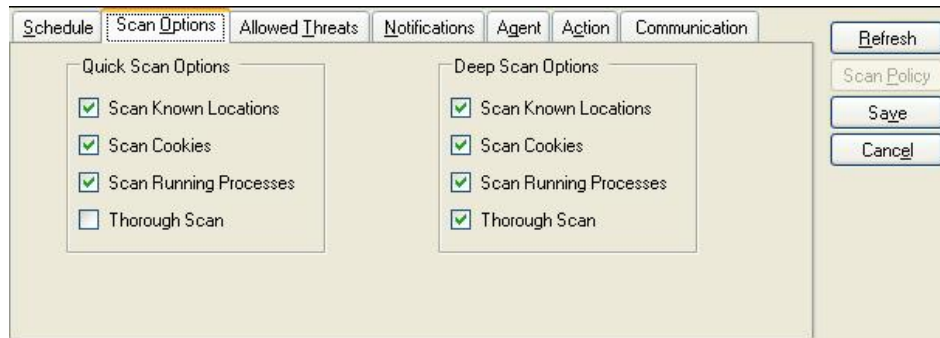
To define scan schedules:

1. Expand Policy in the left pane, and then select the policy to be modified.
2. Click the Schedule tab.
3. Click Enable Quick Scan to set a schedule for quick scans. A Quick Scan runs a complete scan of the computers. This takes only a few minutes, and can detect more than 99% of known spyware threats.
4. Click Enable Deep Scan to set a schedule for a deep scan. A deep scan is an in-depth scan of a user's system including memory, processes, files and more. Although this scan is very accurate, it takes longer to run and consumes more resources.
5. Select a Start Time for the scan.
6. Select when the scan should repeat. The scan will repeat every x number of hours until midnight then stop and wait for the next scheduled scan time.
7. Select the day(s) of the week when the scan will run.
8. Click Save.

Setting Scan Options

Use the Scan Options tab of a policy to define exactly what kind of scan is performed on the computers assigned to that policy.

Set options for both Quick Scans and Deep Scans. The settings here are in effect when the scan(s) scheduled on the Schedule tab run. They are also in effect when the administrator performs a manual scan of one or more computers assigned to that policy.



Scan Options in policy settings

To define scan options:

1. Expand Policy in the left pane, and then select the policy to be modified.
2. Click the Scan Options tab.
3. Click to select options for Quick Scans and for Deep Scans.

Scan Known Locations - Checks all locations where spyware is known to attack.

Scan Cookies - Scans for Internet cookies that are known spyware. These could be used to track Web habits or provide targeted advertising.

Scan Memory and Running Processes - Runs an in-depth scan of any processes currently running in memory. It also checks each process that is loaded to see if it is spyware.

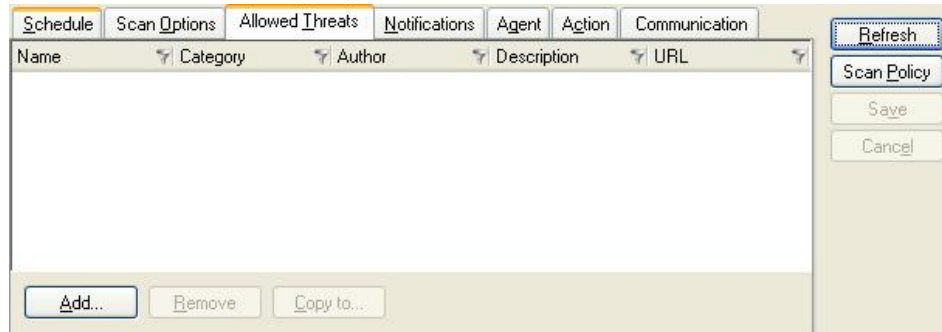
Thorough Scan - A detailed in-depth scan of the system. Although this scan is very accurate, it takes much longer to run and consumes more resources.

4. Click Save to save settings.

Allowing Specific Threats

Some programs that CounterSpy Enterprise flags as spyware might actually be legitimate tools needed within your organization like remote access tools, such as Radmin or VNC. CounterSpy Enterprise lets an administrator set up exceptions for those programs. This lets an administrator fine-tune policies to fit the needs of a wide variety of computer users.

Use the Allowed Threats tab within a policy to define Allowed Threats. Once allowed threats are defined for one policy, an administrator can copy them to other policies.



Allowed Threats in policy setting

To add a program to a policy's Allowed Threat list:

1. Expand Policy in the left pane, and then select the policy to be modified.
2. Click the Allowed Threats tab.
3. Click Add and browse to the threat to be allowed.
4. Click Save to add the selection to the Allowed Threats list.

To delete a program from a policy's Allowed Threat list:

1. Expand the Policy common tasks in the left pane, and then select the policy to modify.
2. Click the Allowed Threats tab.
3. Select the threat to be removed from the list.
4. Click Remove.
5. Click OK to confirm the deletion.

To copy Allowed Threats from one policy to another:

1. Expand Policy in the left pane, and then select the policy to modify.
2. Click the Allowed Threats tab.
3. Select the threat or threats to be copied.
4. Click Copy.
5. Select the policy to which the allowed threat(s) will be copied.

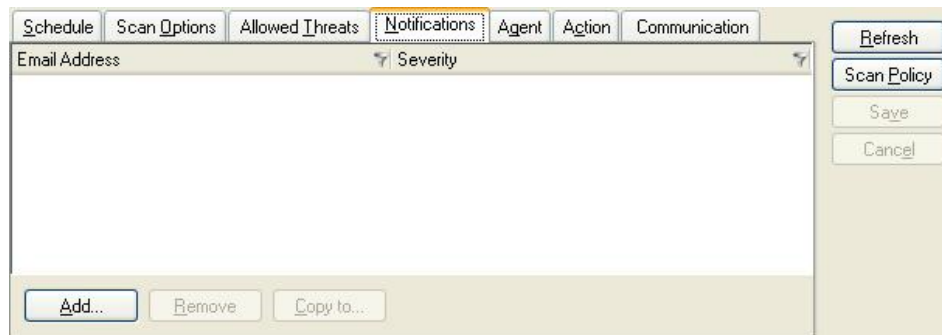
Setting Email Notifications

Notifications alert you when different severities of spyware are found and reported to the Reporting Service. A single email will be sent for each agent that finds spyware to the list of email addresses defined in the Notifications tab. The emails will be sent using the SMTP email server defined in the Configuration pane.

You will only receive notifications on specific types of threats based on the severity level selected in the Notifications tab. If the action for a threat category is set to ignore in the Actions tab no email notification will be sent for that threat if it is detected. All other actions will generate notification emails based on the settings in the Notifications tab.

The following severity levels are available for notifications:

- **ExtremelyCritical** - sends a notification email only for threats marked with this severity level in the threats database.
- **HighlyCritical** - sends a notification email for threats marked with this severity level and threats marked ExtremelyCritical in the threats database.
- **ModeratelyCritical** - sends a notification email for threats marked with this severity level and the two above threat levels.
- **LessCritical** - sends a notification email for threats marked with this severity level and the three above threat levels.
- **NonCritical** - sends a notification email for threats marked with this severity level.



Notifications tab in policy setting

To add a notification definition to a policy:

1. Expand Policy in the left pane, and then select the policy to be modified.
2. Click the Notifications tab.
3. Click Add.
4. Enter the email address where the notification is to be sent.
5. Select a severity setting. The severity setting specifies what conditions will cause an email message to be generated and sent to the recipient.

To modify an email address or a threat level defined for an email address:

1. Expand Policies in the left pane, and then select the policy to be modified.
2. Click the Notifications tabs.
3. Click into the area where the email address is displayed and retype or edit the email address.
4. Click the Severity level in the second column and choose another severity level from the drop down menu that is displayed.
5. Click the Save button on the right hand side to save the new policy setting.

To delete a notification definition from a policy:

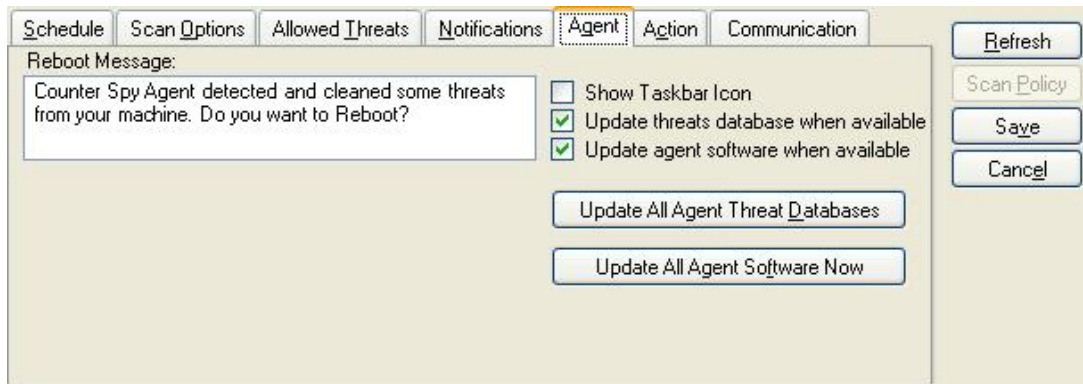
1. Expand Policies in the left pane, and then select the policy to be modified.
2. Click the Notifications tab.
3. Select the notification to delete.
4. Click Remove.
5. Click the Save button on the right hand side to save the policy.

To copy Email Notifications definitions from one policy to another:

1. Expand Policies in the left pane, and then select the policy that has the notification definitions to copy, and then click the Notifications tab.
2. Select the notification email addresses to copy by holding down the Ctrl key while selecting the rows with you mouse.
3. Click the Copy to... button.
4. Select the policy to which notifications definitions will be copied.

Setting Agent Options

These options affect the behavior of the agent on the installed computer.



Agent tab in policy setting

Displaying a Taskbar Icon on a computer that has an installed agent

When checked, a Taskbar icon will be displayed to indicate to the user that the CounterSpy Enterprise Agent is installed and running on a computer. This option does not take affect until the user logs off and logs back in.

To control display of a Taskbar icon:

1. Expand Policies in the left pane, and then select the policy to modify.
2. Click the Agent tab.
3. Select or deselect Show Taskbar Icon.
4. Click the Save button on the right hand side to save the policy settings.

Displaying a reboot message

When the actions taken after a scan and removal of spyware require that a computer be restarted, an administrator can display a custom message to communicate this to the user. Use the Agent tab to create a message that will be displayed to the user when a reboot is required.

To display a reboot message:

1. Select the policy to modify, and then click the Agent tab.
2. In the Reboot Message box, type the message to be displayed when a reboot is required.
3. Click the Save button on the right hand side to save the policy settings.

Updating Agents

Updating CounterSpy Enterprise agent software and threat databases on agent workstations is important. It's the only way to keep ahead of constantly evolving spyware threats.

Configuration settings control how often the CounterSpy Enterprise server checks for and downloads updates. Settings on the Agent tab in a policy defines when the agents assigned to that policy receive updates.

Agent software and threat definitions can also be updated manually from the Agent tab of a policy.

To define an update schedule for agents:

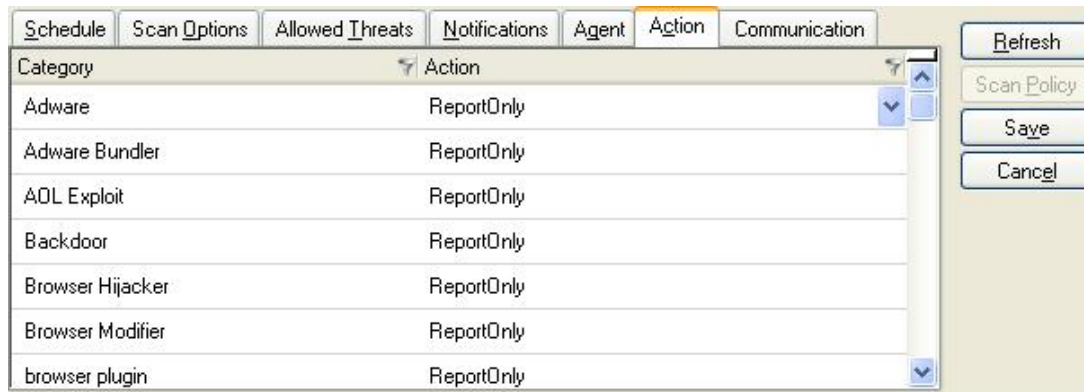
1. Expand Policy in the left pane, and then select the policy to modify.
2. Click the Agent tab.
3. Select Update threats database when available to enable automatic updates of the threat database.
4. Select Update agent software when available to enable automatic updates of agent software.

To manually update all agents assigned to a policy:

1. Expand Policy in the left pane, and then select the policy that has agents that need to be updated.
2. Click the Agent tab.
3. Click Update All Agent Threat Databases to immediately update spyware definitions.
4. Click Update All Agent Software Now to immediately update CounterSpy Enterprise agent software.

Setting Actions

Each piece of spyware that CounterSpy Enterprise discovers requires an action. Use the Actions tab of a policy to specify actions for each threat. Use the drop-down list to select the action CounterSpy Enterprise is to perform on each selected spyware.



Action tab in policy setting

If CounterSpy Enterprise identifies a threat that needs to be allowed, the threat can be added on the Allowed Threats tab of a policy.

- Ignore - Select this action to temporarily ignore a threat until the next time a spyware scan is run.
- Report Only - Send a notification for this, but take no other action.
- Quarantine - Select this action to safely remove this threat from a computer, while storing it in spyware quarantine. Any threats in spyware quarantine will not run on the computer and the administrator can restore these items back to their original state should it be necessary. (Note, some spyware cannot be quarantined, only deleted.)
- Delete - Select this action to completely and permanently remove the threat from a computer.

The default action for each threat is ReportOnly.

Changing the IP Address

Use the Communications tab to change the IP address for the Policy, Update, and Reporting services without rebooting the server or workstation.

The screenshot shows a software interface with a tabbed menu at the top: Schedule, Scan Options, Allowed Threats, Notifications, Agent, Action, and Communication. The 'Communication' tab is selected. Below the tabs are three service configuration panels. The 'Policy Service' panel has an 'Address' field with '207.90.40.100', a 'Port' field with '18082', and a checked 'Save as IP Address' checkbox. The 'Update Service' panel has an 'Address' field with '207.90.40.100', a 'Port' field with '18085', and a checked 'Save as IP Address' checkbox. The 'Reporting Service' panel has an 'Address' field with '207.90.40.100', a 'Port' field with '18083', and a checked 'Save as IP Address' checkbox. To the right of these panels are four buttons: Refresh, Scan Policy, Save, and Cancel.

Communication tab in policy setting

To change the IP address for the Policy, Update, and Reporting services

5. Select a policy from the left pane.
6. Click the Communication tab.
7. Update the address and/or port numbers
8. Click **Save**.

Manually Scanning Agents

An administrator can manually scan one or all of the agents assigned to a policy. During a scan, the agent status changes to show what is happening, e.g., Scanning memory, Scanning Registry, Scanning Cookies, or Scanning Files. When a scan is finished, the status displays "Scan Complete".

To scan all agents:

1. Expand Policies in the left pane, and then select the policy that has agents that need to be scanned.
2. Click the Scan All button in the upper right hand corner to initiate a scan on all computers that have agents installed assigned to that policy.

To scan one or more agents:

1. Expand Policies in the left pane, and then select the policy that has agents that need to be scanned.
2. Select the agents that require a scan.
3. Click the **Scan** button in the upper right hand corner to initiate a scan on the selected agents, or choose **Policy menu>Scan Computers**.

Agent Deployment

What is an Agent?

CounterSpy Enterprise Edition relays on agents in order to scan and remove spyware. The agent is a service that runs on a user's machine and takes orders from the Policy Server component.

Requirements

OS: Windows 98se/ME/NT/XP/2000/2003

Memory: At least 20 megs of disk space and typically 15 megs of RAM

Components / Location

The agent is installed to: C:\Program Files\Sunbelt Software\CounterSpy\Agent

Once the agent is installed, all configuration and control is done by the Policy service, the only user interface on the agent is a system tray icon (which can be disabled by policy).

Agent Communication

An agent will listen on 18086 for communication from the Policy service. Communication occurs when changes are made to that agent's policy or when the administrator requests the agent to perform a task, like scanning or un-quarantining an item.

In addition to listening for communication the agent will send a heartbeat type of communication back to the Policy service on port 18082 every 5 minutes. This communication is typically less than 1kb in size and lets the Policy service know the current status of the agent (install, scanning, etc). Additionally, the agent will pickup and process any pending commands on the policy server. See Deferred Communication on page 45.

The agent will also communicate back to the Update service (same machine as the Policy service by default) over port 18085. This check occurs every 5 minutes, prior to any scan and whenever the agent restarts. As well the Policy service will contact the agent over port 18086 to let it know that updates are available. If updates are available they will be pulled down over this port by the agent and installed. Updates to the agent may be up to 8 MB in size whereas updates to the threat database are typically less than 200KB.

Lastly, the agent will communicate back to the Report Service (same machine as the

Policy Service by default) over ports 18083 and 18084. The agent will initiate this communication when a scan is completed and the results need to be posted back to the Report Service.

It is important to note that the only thing that will initiate communication to the agent is the Policy service. The other services and even the CounterSpy Enterprise Administrative Console will never initiate communication to the agent.

Deferred Communication

Because of the variety and disparity of network topology it is will not be uncommon for the Policy service to be unable to contact the agent over port 18086. Among the more common reasons: the remote machine could be offline, there could be firewall blocking the request or the agent may be in a private subnet behind a NAT device. For these reasons the Policy service will use deferred communication if the agent can not be contacted to complete a request.

The deferred communication is done automatically by the Policy service. If you use the CounterSpy Administrative Console to tell an agent to do an action and the agent cannot be contacted you will see the status change to "Pending". This means that the command has been queued on the policy server and the next time the agent contacts the Policy service it will be given the queue of actions.

If you need to remove queued action, you can, but you must remove ALL deferred actions for ALL agents.

To remove ALL queued actions:

1. Stop the Policy Service
2. Delete "C:\Program Files\Sunbelt Software\CounterSpy\Enterprise\AgentsDeferredActions.xml"
3. Start the Policy Service

Deploying the Agent Software

Adding Machines to a Policy

Once a policy is designed to meet the needs of a computer or a group of computers, computers can be assigned to that policy. There are two methods of adding machines to a policy; manually via the CounterSpy Enterprise Console or automatically via an agent installation package. When a computer is added to a policy via the CounterSpy Enterprise Console the option to install the agent to that machine will be given.

Once a machine is removed from the policy the agent will continue to run but will stop doing any actions until assigned to another policy. After an agent is added to a policy, it appears in that policy's agent list. The listing includes name, policy, status (installed, not

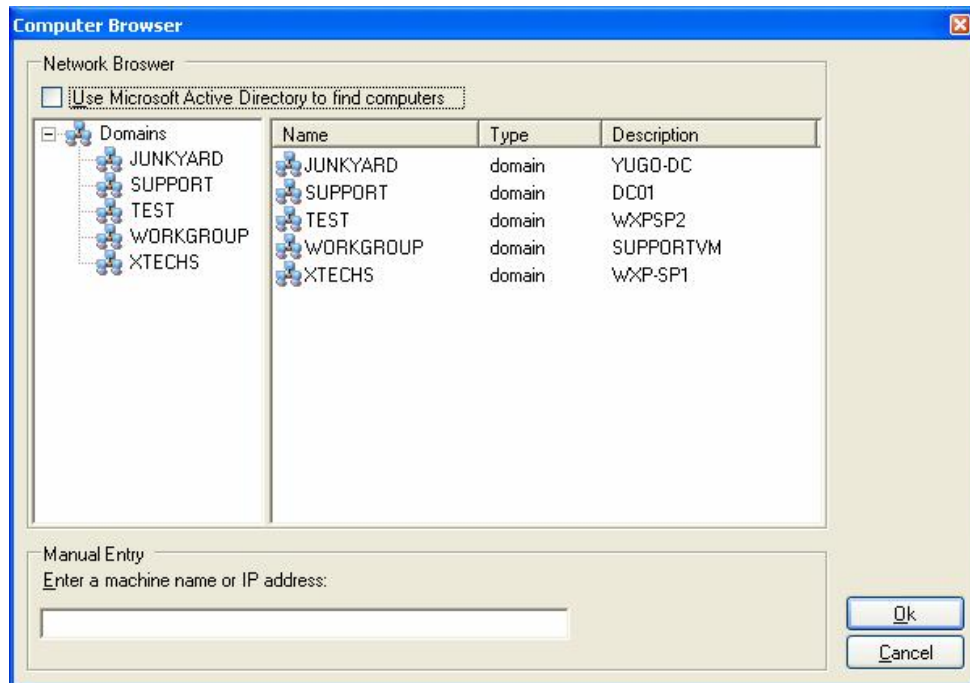
install, scan status, offline, pending request), last scan, and what version of threat database and CounterSpy Enterprise Agent software is installed.

Additionally a list of all machines with agents or that have had agents will be under **Management >Agents**.

There are 2 distinct methods of assigning machines to a policy and getting the agent installed, manually and automatically.

To Add a Machine To a Policy:

1. Expand Policy section in the left pane, and then select the policy to which an agent will be added.
2. Click Add (located to the right of the policy name) or select Policy>Add Computers from the toolbar, this will bring up the add computer interface from which you may:
3. Type an IP address.
4. Use the Network Browser to select a computer(s) to add.
5. Check "Use Microsoft Active Directory" in order to find machine accounts in the active directory.



Example of the Add Computers screen

After adding the machine to a policy you have the option to deploy the software to the remote machine. If you choose not to install the agent at this time, you can initiate the installation later by selecting Policy>Deploy Agents from the menu bar. You must have administrative rights to the remote machine in order to push the agent. If the account you are logged into currently does not have administrative rights you will be prompted for an account that does.

When deploying an agent using an automated Push/Pull installation, the target machines must have either WMI enabled or you must have access to the default administrative shares (C\$) and remote registry. There are several items to make sure of on the target machines in order for this type of installation to succeed. These are:

- The target machine is turned on and you have administrative rights to the machine.
- “Simple File Sharing” is turned off.
- The Windows Firewall (or any other firewall software, such as ZoneAlarm) is turned off or configured to allow administration traffic.

To deploy an agent using automated /push/pull installation

1. Expand Policy section in the left pane; then, select the policy to which an agent was added.
2. Click Deploy Agents on the toolbar. The Agent Deployment Wizards opens.
3. Click **Next**.
4. Select **Automated Push Pull Installation**; then, click **Next**.
5. Click **Next** again.
6. Select an agent from the list; then, click **Next**.
7. Review your selections; then, click **Next**. The agent installs.
8. Click **Next**; then, **Finish**.

To manually install a deployment package

1. Expand Policy section in the left pane, and then select the policy to which an agent will be added.
2. Click **Deploy Agents** on the toolbar. The Agent Deployment Wizard opens.
3. Click **Next**.
4. Select Deployment Package (Manual Installation); then, click **Next**.
5. Make a selection:
 - MSI Installer The MSI install will be composed of an MSI file called "CSEAgent-<policy name>.exe" and a text file called "<POLICY NAME> MSI Command.txt" that contains the installation options. In the future there will be a tool provided by Sunbelt that will generate a .MHT file for use in installing the agent via GPO.
 - MSI Installer with a Microsoft Installer Transformation (MST) file. A generic MSI file is created along with an MST file that contains all of the necessary settings to install an agent to the selected policy. The MSI file must be used with the MST file.
 - Self Extracting Executable The Self Extracting Executable is an executable file named " CSEAgent-<policy name>.exe."

Deploying an agent using a Deployment Package is recommended if you have a large number of agents to install or you wish to deploy using automated management software (such as Microsoft SMS), network logon scripts, NT or AD Group Policies, or any other scripted method of installation.

6. When the agent is installed in this manner the first action it will take when coming online will be to contact the policy server and request to be added to the policy selected in step #1. As long as the policy server contacted is the one used to create the installation package the machine will be joined to the policy and given a copy of the current policy settings. If the agent cannot contact the policy server the agent service will fail. Select either Windows Installer (MSI) or Self Extracting Executable. You will then be prompted to where the agent installation file(s) will be saved.

Deleting and Reassigning Agents

An administrator can delete agents from policies, or reassign an agent to another policy.

To remove an agent from a policy:

1. Expand Policy in the left pane, and then select the policy to which the agent is currently assigned.
2. Select the agent.
3. Click Remove (located to the right of the policy name).

To reassign an agent to another policy:

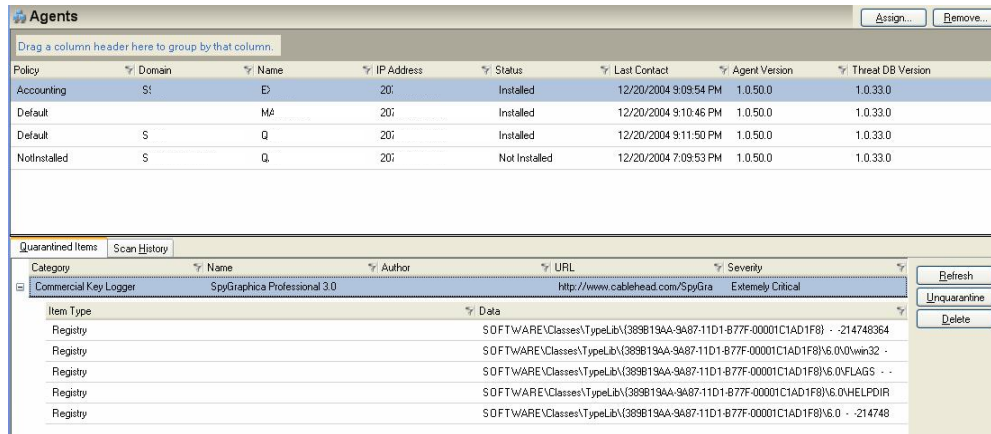
1. Expand Policy in the left pane, and then select the policy to which the agent is currently assigned.
2. Select the agent.
3. Click Reassign (located to the right of the policy name).
4. Select a policy.
5. Click **OK**.

Viewing Scan Results

CounterSpy Enterprise lets you view spyware activity in several different ways. By moving between the Agents, Quarantine, and Threats pages, you can get a good view of what spyware is threatening the entire system. Reports are another tool that can help make patterns visible and address specific needs.

Results of scans are viewed on the Agents pane. By clicking on an agent, you can review what spyware was quarantined and the scan history for each agent on the network.

Note: If there is an item in the Quarantined Items list that needs to be removed from quarantine that can be done here on the Agents page.



CounterSpy Enterprise Agents screen

To view spyware found by agent:

1. Click on Agents under the Management pane.
2. Select an agent on the list.

Click the Quarantined Items tab to view all currently quarantined items for that agent. Click the plus sign (+) beside a listing to view more details.

On the top of the Quarantined Items tab are a number of various column headers. You can sort by these column headers by clicking on the column name. You can also filter by choosing the filter (🔍) icon.

The column headers are:

Category—The class of spyware (Adware, Toolbar, Trojan, etc.)

Name—The specific name of the spyware threat

Author—The maker of the spyware.

URL—The URL where the spyware might be found.

Severity—The ranked severity of the threat.

9. Click the Scan History tab to view scan history for the selected agent. Scan history is sorted by date. When expanded, scan history displays any items found during the scan. Click the plus sign (+) beside a listing to view more details.

On the top of the Scan History tab are a number of column headers. You can sort by these column headers by clicking on the column name. You can also filter by choosing the filter (🔍) icon.

The column headers are:

Date Found—The date of the scan.

Agent version—The version number of the agent used to find the spyware.

Threat DB version—The version number of the threat database used to find the spyware.

Found Threat—The total number of threats found on the date (including registry entries, cookies, etc.).

Found Cookies—How many cookies were found

Found Registry— The number of registry entries found.

Found Files—The number of files found.

Found Memory—The number of in-memory spyware processes found.

Deleted—The number of threats deleted.

Ignored—The number of threats ignored.

Quarantined—The number of threats quarantined.

To Unquarantine or Delete an item:

1. To unquarantine: Select an item in the Quarantined Items list, and then click Unquarantine button on the right.
2. To delete the item permanently: Select an item in the Quarantined Items list, and then click the Delete button on the right
3. You can also right-click on a specific threat to choose Unquarantine, Delete or get more information on the threat.

Managing All Quarantined Items

There are two ways to deal with quarantined items.

- On a machine by machine basis, an administrator can unquarantine or delete items through the Agents page, by using the Quarantined Items tab.
- On an enterprise level, the Quarantine page is the way to manage any quarantined items.

The Quarantine pane displays all quarantined items in the enterprise. For each quarantined item, the following is displayed: Category, Name, Author, URL, and Severity.

To manage quarantined items:

1. Choose Quarantine under the Management section.
2. Select an item in the quarantine list. When an item is selected, the bottom of the pane displays all agents that have the item quarantined, as well as scan history for when the item was quarantined.
3. Click the Occurrences tab to see all agents that have the item quarantined and the scan history.
4. Click the Detail tab to see additional information about the threat, as well as a link to even more information on the CounterSpy Enterprise Website.
5. Click Unquarantine to remove the item from quarantine, or click Delete to delete the item
6. Choose how much action to take: machine, policy, or entire enterprise.

Managing Threats

The Threats page displays all quarantined items. For each spyware item, an administrator can see the basic information about that piece of software.

CounterSpy Enterprise lets an administrator view spyware activity in several different ways. By moving between the Agents, Quarantine, and Threats pages, an administrator can get a good view of what spyware is threatening the entire system. Reports are another tool that can help an administrator recognize patterns and address specific needs.

To manage threats:

7. Expand System in the left pane, and then click Threats.
8. Select an item in the Threats list.
9. Click the Occurrences tab to see details about when the threat was found, what agents have the threat, and what policies are affected.
10. Click the Details tab to view more details about the threat.

Reports

CounterSpy Enterprise lets an administrator view spyware activity in several different ways. By moving between the Agents, Quarantine, and Threats pages, an administrator can get a good view of what spyware is threatening the entire system. Reports are another tool that can help make patterns visible and address specific needs.








Leveraging Crystal Reports, CounterSpy Enterprise includes several pre-defined reports, and offers the ability to create custom reports. These pre-defined reports include:

- **Executive Summary** - Includes the Severity of Threats Found, the Top 10 Threats Found, Infected vs. Uninfected, and Number of Threats by Category.
- **Infected Machines Summary** - Machine name, Threat, and Number of Times Infected.
- **Infected Machines Detail** - View trends over selected time period, more detail.
- **Computer History Report** - Troubleshoot policy, see threats by machine and what action was taken.
- **Threats Found Summary** - Each threat that was found, along with the number of times it occurred.
- **Threats Found Detail** - Each threat that was found, the machine on which it was found, and the number of times it occurred
- **Top 10 Infected Machines** - machine names, scan dates, what was found, what was deleted, and what was quarantined.

Generating Reports and Report Options

On every report you must select the date range that you wish to run the report against. This is done by setting the “From” and “To” fields at the top of the report and pressing “View”. This will generate the report. Note that this may take some time depending upon the amount of time specified and the amount of information in the database.

Toolbar options:

	<p>Navigation—Allows you to navigate your report. The options are: First Page, Back One Page, Forward One Page, Last Page, Go To Page</p>
	<p>Print—Prints the current report</p>
	<p>Refresh—Refresh the current report’s information from the database.</p>
 	<p>Export—Allows you to export the current report to a variety of formats: .rpt, .pdf, .xls, .doc, .rtf</p> <p>GroupTree—Enables the viewing of individual machines to the left of the report.</p>
	<p>Zoom- Allows you to change the zoom on the report.</p>
	<p>Search- Allows you to search the report.</p>

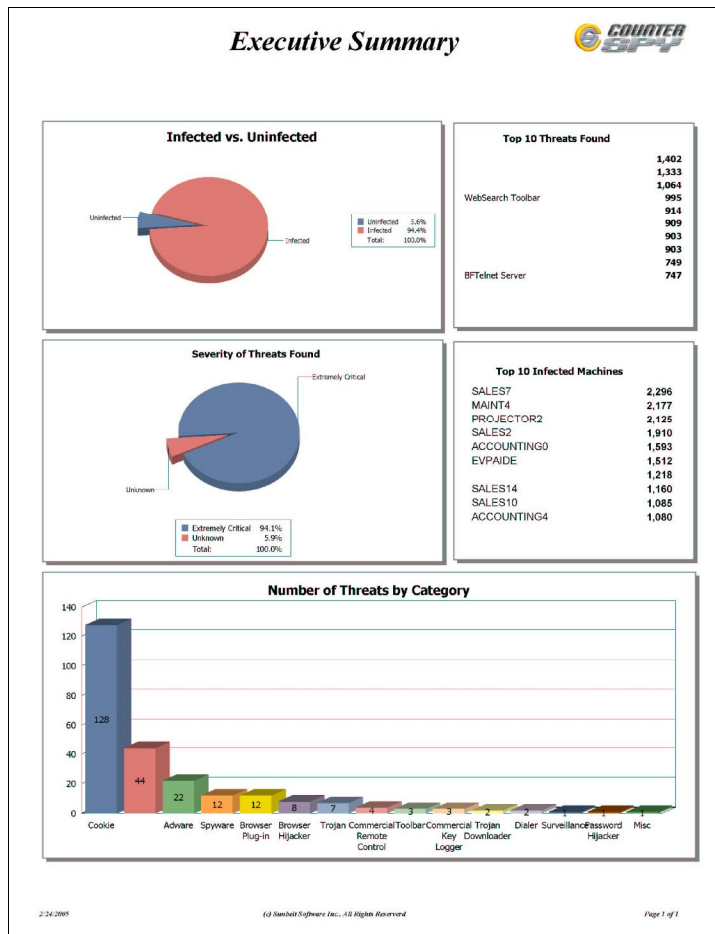
Executive Summary Report

The Executive Summary offers a high level view of spyware infection and progress towards correcting the problem. The Executive Summary displays at a glance what threats are the most problematic, what percentage of threats are severe, how many computers on the network are infected, and what types of spyware are the most troublesome.

The Executive Report includes the Severity of Threats Found, the Top 10 Threats Found, Infected vs. Uninfected, and Number of Threats by Category. Presented in a colorful and easily understood format, the Executive Summary Report is well suited for sharing with other team members and management.

To view an Executive Summary Report:

1. Expand Reports in the left pane, and then select Executive Report.
2. Expand Reports in the left pane; then, select the type of report to be viewed.
3. Select the report to be viewed; then, the tools at the top to navigate the report.



Infected Machine Summary Report

The Infected Machines Summary report lists problems by machine name. Each machine is listed; along with how many times that machine was found to be infected.


The Infected Machines Summary Report includes the Machine name and Number of Times Infected.

To create an Infected Machine Summary Report:

- Expand Reports in the left pane, and then select Infected Machine Summary Report.

To view an Infected Machine Summary Report:

1. Expand Reports in the left pane, and then select the type of report to be viewed.
2. Select the report to be viewed.
3. Use the Crystal Report tools at the top to navigate the report.

<i>Infected Machines - Summary</i>		
Machine	# of Threats Found	
ACCOUNTING0	3	
ACCOUNTING1A	26	
ACCOUNTING4	18	
ACCOUNTING5	1	
ACCOUNTING6A	2	
ACCOUNTING7	6	
ADMINASSIST99	1	
MAINTABY	1	
MARKET1	24	
MARKET10	2	
SALES20	18	
SALES6	2	
SALES9	9	
TECH2	1	
TECH2	2	

13/08/2004 © Insubite Software Inc., All Rights Reserved Page 1 of 2

Infected Machines Detail Report

The Infected Machines Detail report lists problems by machine name. Each machine is listed, along with what threats were discovered and how many times each of those threats was found on the machine. The Infected Machines Detail Report includes the Machine name, Threat, and Number of Times Infected. It allows an administrator to view trends over selected time periods, and has more detail than the Infected Machine Summary Report.

To view an Infected Machine Detail Report:

1. Expand Reports in the left pane, and then select Infected Machine Detail Report.
2. Expand Reports in the left pane, and then select the type of report to be viewed.
3. Select the report to be viewed; then, use the tools at the top to navigate the report.

<i>Infected Machines - Detail</i>		
ACCOUNTING3	GeoCities	# of Times Found 1
	SpyGraphics ProfessionalB.0	1
ACCOUNTING5A	AdsRemote.Scripps.com	# of Times Found 1
	Advertising.com	1
	ATDMT.com	1
	BFast.com	1
	Bluestreak.com	1
	casalemedia.com	1
	ClickAgents.com	1
	Com.com	1
	cookie.monster	1
	Data.Coremetrics.com	1
	DoubleClick	1
	FastClick.com	1
	Fredentics.com	1
	managaming	1
	My Search Bar	2
	Rut.com	1
	ServedbyAdvertising.com	1
	tickle	1
	Travelocity.com	1
	TribalFusion.com	1
ValueClick.com	1	
Z1.Adserver.com	1	
Zedo	1	
ACCOUNTING4	ABetterInternet	# of Times Found 1
	AdTraffic.com	1
	Advertising.com	1
	ATDMT.com	1
	DoubleClick	1
	FastClick.com	1
	HuntBar	1
	IEPlug	1
	Mediaplex.com	1
	NewDot.biz	1
	Passport.com	1
	Qksrnet	1
	QuestionMarket.com	1
	Rut.com	1
	ServedbyAdvertising.com	1
	tickle	1
Twain Tech	1	
Z1.Adserver.com	1	
ACCOUNTING6	SideStep	# of Times Found 1
ACCOUNTING5A	ATDMT.com	# of Times Found 1
	SpyGraphics ProfessionalB.0	1
ACCOUNTING7	AdsRemote.Scripps.com	# of Times Found 1
	BargainBuddy	1
	Data.Coremetrics.com	1
	My Search Bar	2
	SpyGraphics ProfessionalB.0	1

12/20/2004

(c) InsubitecTightware, Inc., All Rights Reserved.

Page 7 of 39

Machine History Report

The Machine History report gives a detailed scan history for each machine. For each machine, this report displays the scan dates, what threats were found, and what actions were taken. The Machine History Report is a good way to troubleshoot policies.

To view a Machine History Report:

1. Expand Reports in the left pane, and then select Computer History Report.
2. Expand Reports in the left pane, and then select the type of report to be viewed.
3. Select the report to be viewed; then, use the tools at the top to navigate the report.

Machine History

Machine Name	ACCOUNTINGIA
Scan Date	12/16/2004 11:23 PM
Action	Quarantined
Threat Name	AdsRemote.Scripps.com
Type	Data
File	adsremote.scripps - c:\documents and settings\default user\cookies\system@adsremote.scripps[1].txt
File	advertising - c:\documents and settings\default user\cookies\system@advertising[1].txt
File	atdmt - c:\documents and settings\default user\cookies\system@atdmt[2].txt
File	bfast - c:\documents and settings\default user\cookies\system@bfast[1].txt
File	bluestreak - c:\documents and settings\default user\cookies\system@bluestreak[1].txt
File	casalemedia - c:\documents and settings\default user\cookies\system@casalemedia[1].txt
File	clickagents - c:\documents and settings\default user\cookies\system@clickagents[1].txt
File	com - c:\documents and settings\default user\cookies\system@com[2].txt
File	cookie.monster - c:\documents and settings\default user\cookies\system@cookie.monster[1].txt
File	data.coremetrics - c:\documents and settings\default user\cookies\system@data.coremetrics[1].txt
File	doubleclick - c:\documents and settings\default user\cookies\system@doubleclick[1].txt
File	fastclick - c:\documents and settings\default user\cookies\system@fastclick[2].txt
File	fastclick - c:\documents and settings\default user\cookies\system@fastclick[3].txt
File	fredericks - c:\documents and settings\default user\cookies\system@fredericks[1].txt
File	maxservicing - c:\documents and settings\default user\cookies\system@maxservicing[1].txt
Memory	6e055a9d9b9f30716c3802e3acc84684 - c:\program files\mysearch\bar\history\search
Folder	0 - c:\program files\mysearch\bar
Folder	0 - c:\program files\mysearch\bar\history
Folder	0 - c:\program files\mysearch\bar\settings
Registry	SOFTWARE\MySearch\bar - 2147483646
File	edge.ru4 - c:\documents and settings\default user\cookies\system@edge.ru4[1].txt
File	servedby.advertising - c:\documents and settings\default user\cookies\system@servedby.advertising[2].txt
File	tickle - c:\documents and settings\default user\cookies\system@tickle[1].txt
File	travelocity - c:\documents and settings\default user\cookies\system@travelocity[1].txt
File	tribalfusion - c:\documents and settings\default user\cookies\system@tribalfusion[2].txt
File	valueclick - c:\documents and settings\default user\cookies\system@valueclick[1].txt
File	z1.adserver - c:\documents and settings\default user\cookies\system@z1.adserver[1].txt
File	zedo - c:\documents and settings\default user\cookies\system@zedo[2].txt
Scan Date	12/17/2004 04:43 PM
Action	Quarantined
Threat Name	ATDMT.com
Type	Data
File	atdmt - c:\documents and settings\default user\cookies\system@atdmt[1].txt
File	doubleclick - c:\documents and settings\default user\cookies\system@doubleclick[1].txt


12/20/2004
(c) TrendMicro, Inc., All Rights Reserved
Page 3 of 20

Threats Found Summary Report

The Threats Found Summary report gives a top-level view of problems by threat. For each threat, this report displays how many times the threat was found.

To view a Threats Found Summary Report:

1. Expand Reports in the left pane, and then select Threats Found Summary report.
2. Expand Reports in the left pane, and then select the type of report to be viewed.
3. Select the report to be viewed; then, use the tools at the top to navigate the report.

<i>Threats Found - Summary</i>		
Threat	# of Occurrences	
180search Assistant	1	
2020Search	2	
ABetterInternet	1	
Ad.Trafficmp.com	2	
AdsRemote.Scripps.com	2	
Advertising.com	3	
ATDMLT.com	6	
BargainBuddy	2	
BFast.com	1	
Bluestreak.com	2	
casalemedia.com	1	
Centrport.net	1	
Claria	2	
ClearSearch	1	
ClickAgents.com	1	
Com.com	1	
cookie-monster	1	
DashBar	2	
Data.Coremetrics.com	3	
DoubleClick	5	
eAcceleration.OOdlz.Revenge	1	
eAcceleration.Stop Sign	1	
FastClick.com	4	
Fredericks.com	1	
GeoCities	1	
Gigatech Superbar	1	
Hotbar	1	
HuntBar	1	
IEPlugin	6	
IncrediFind	1	
LinkExchange.com	1	
maxserving	1	
Mediaplex.com	2	
MidAddle	3	
My Search Bar	2	
NewDotNet	1	
One-Time-Offer	1	
Passport.com	1	
Powerscan	1	
PriceGrabber	1	
Qksrv.net	1	
QuestionMarket.com	1	
ReaMNC	1	
Ru4.com	2	
SearchEye Hijacker	3	
Servedby.Advertising.com	3	
ShopAtHome	1	
SideStep	1	
SpyGraphica Professional 3.0	13	
Tafbar	1	
tickle	2	
Travelocity.com	1	
TribalFusion.com	2	
Twain Tech	2	
ValueClick.com	1	
VX2 Transponder	1	
WildTangent	1	
Z1.Adserver.com	3	
Zedo	2	


12/20/2004 © Insuborn Software Inc., All Rights Reserved. Page 2 of 2

Threats Found Detail Report

The Threats Found Detail report gives a detailed look at problems by threat. For each threat, this report displays what machines had that threat and how many times the threat was found on each machine.

To view a Threats Found Detail Report:

1. Expand Reports in the left pane, and then select Threats Found Detail report.
2. Expand Reports in the left pane, and then select the type of report to be viewed.
3. Select the report to be viewed; then, use the tools at the top to navigate the report.

<i>Threats Found - Detail</i>		
180Search Assistant	MARKET1	# of Times Found 1
2020Search	MARKET1 SALES9	# of Times Found 1 1
ABetterInternet	ACCOUNTING4	# of Times Found 1
Ad.Trafficmp.com	ACCOUNTING4 SALES20	# of Times Found 1 1
AdsRemoteScripps.com	ACCOUNTING4 ACCOUNTING7	# of Times Found 1 1
Advertising.com	ACCOUNTING4 ACCOUNTING4 SALES20	# of Times Found 1 1 1
ATDMT.com	ACCOUNTING4 ACCOUNTING4 ACCOUNTING4 SALES20 SALES9	# of Times Found 1 1 1 1 1
BargainBuddy	ACCOUNTING7 MARKET1	# of Times Found 1 1
BFast.com	ACCOUNTING4	# of Times Found 1
Bluestreak.com	ACCOUNTING4 SALES20	# of Times Found 1 1
casalemedia.com	ACCOUNTING4	# of Times Found 1
Centrport.net	SALES9	# of Times Found 1
Claria	MARKET1	# of Times Found 1

11/28/2004 (c) Insubac-Software Inc., All Rights Reserved. Page 2 of 5

Top Ten Infected Machines

The Top Ten Infected Machines report gives a detailed look at problems on the machines that are most often infected. For each machine, this report displays a scan history that shows when scans took place, how many problems were found, how much spyware was quarantined, and how much spyware was deleted.

To view a Top Ten Infected Machines Report:

1. Expand Reports in the left pane, and then select Top Ten Infected Machines report.
2. Expand Reports in the left pane, and then select the type of report to be viewed.
3. Select the report to be viewed; then, use the tools at the top to navigate the report.

ACCOUNTING3	3
ACCOUNTING1A	26
ACCOUNTING4	18
ACCOUNTING6A	2
ACCOUNTING7	6
MARKET1	24
MARKET10	2
SALES20	18
SALES8	9
TECH22	2

12/28/2004 © Trend Micro Software Inc., All Rights Reserved Page 1 of 2

Exporting Reports

CounterSpy Enterprise reports give an administrator a variety of ways to look at spyware data. Reports can be exported in the following formats: Crystal Reports (.rpt), Adobe Acrobat (.pdf), Microsoft Excel (.xls), Microsoft Excel Data Only (.xls), Microsoft Word (.doc), and Rich Text Format (.rtf).

To export a report:

1. Expand Reports in the left pane, and then select the report category to which the report belongs.
2. Select the report.
3. Click **Export**.
4. In the Export Report dialog, navigate to the location where the file will be saved.
5. Enter a file name.
6. Select a file format.
7. Click **Save**.

Understanding spyware

What is Spyware?

Spyware is software that is installed onto a computer without the user's knowledge or permission. It collects personal information, like the Web sites that have been visited or even user names and passwords. Spyware is often associated with adware. Adware also is installed onto a computer without the user's knowledge. Adware generates a stream of unsolicited advertisements, affecting productivity. These advertisements often contain pornographic images or other material that users could find inappropriate. The extra processing that is required to support spyware or the display of adware advertisements could tax computers and hurt performance. There are programs that are downloaded that can affect a browser's home page or search page settings.

Spyware is used for two general purposes: surveillance and advertising. Surveillance software includes key loggers, screen capture devices, and Trojans. Corporations, private detectives, law enforcement, intelligence agencies, or even suspicious spouses would use this kind of spyware. Advertising spyware is installed along with other software or when ActiveX controls are downloaded from the Internet. In the hopes of targeting the user's interests, advertising spyware can log information about a user, including passwords, email addresses, Web browsing history, online buying habits, a computer's hardware and software configurations, and personal information, such as the name, age, or sex of the user.

Spyware programs fall into these categories:

- **Adware** is software that displays advertisements. Some adware can generate a stream of unsolicited advertisements that clutter the desktop and affect productivity. The advertisements can contain inappropriate images or content. The extra processing required to track viewing habits or display advertisements can tax a computer and hurt system performance.
- **Spyware** is software that collects personal information and computer or Web usage information from a computer, usually to facilitate advertising. Spyware programs can be bundled as a hidden component on other software packages, or it can be downloaded from the Internet. These little programs are almost always secretly installed on a computer and try to run without being detected.
- **Browser Plug-ins** are applications that get installed into a Web browser. Plug-ins can come in the form of toolbars, or can take the form of a search or navigation feature. They can also be extra task buttons on a Web browser. Although some plug-ins are designed to perform useful functions, many plug-ins are harmful to a computer. They often have complete access to the Web browser, and can modify, spy or even redirect tasks as they are performed.
- **Browser Hijackers** are malicious programs that change Web browser settings, usually altering the default start (home) and search pages. A browser hijacker can modify nearly every part of a Web browser, including adding bookmarks and redirecting searches to alternate sites.

- **RAT** (Remote Administration Tool). These are trojan-type software programs that provide someone (the attacker) with the ability to remotely control a computer. The attacker usually has full access, while the computer listens on the Internet for instructions.
- **Key Loggers** are programs that run in the background, recording all the keyboard entries (keystrokes) that are made on a computer. Keystrokes are logged, and then the log is hidden for later retrieval. The log can then be secretly shipped by email or over the Internet.
- **Remote Installers** are programs that are installed onto a computer without the user's knowledge. Once installed, remote installers connect to a remote server and download more programs and files. These new files are installed on the computer, again without the user's knowledge.
- **Commercial Key Loggers** are surveillance programs that are installed by someone who has access to a computer. They are used to explicitly monitor the activity of computer users. These types of programs can be installed so that they remain hidden from other users. Commercial Key Loggers can be purchased from commercial vendors.
- **Dialer**. This type of software uses a computer's modem to dial a phone number. Most dialer programs connect to toll numbers without the user's awareness or permission, running up phone charges on their phone bill.
- **Low Risk Adware** is adware that is designed to do something like show advertisements via popups. What's different is that the user gives permission for this type of adware program to be installed. It conforms to program standards, which are usually presented prior to downloading and installation. A low risk adware program will not transmit personal or identifiable information.
- **File Sharing Programs**, also known as P2P (peer to peer), are popular applications. They are used to share files, such as movies and music, across the Internet. Many freeware and shareware file sharing programs such as Grokster, Kazaa and Bearshare bundle adware with their product. Download the product, get the adware. Sometimes they are also bundled with spyware software. Although most file sharing programs themselves are safe, the adware and spyware programs that come with them could be dangerous.

How Spyware Gets Installed

A lot of content that is available on the Internet is not designed to covertly watch the user's actions. Unfortunately, many internet "freebees," as well as some over-the-counter software programs are secretly bundled with spyware. After all, spyware can give advertisers an inside look at what interests someone online. It can also lead to the disclosure of sensitive personal or company data.

There are many ways that spyware can get installed on a user's computer. Sometimes spyware hides in another program that is being installing. Sometimes spyware fools a user into downloading and installing it, by pretending to be something useful.

Types of Spyware Installations

Below are some various types of spyware installations.

- **Drive-by Download** - A program that is automatically downloaded to a user's computer, often without the user's consent or even the user's knowledge. Unlike a pop-up download, which asks for the user's permission (albeit in a calculated or devious manner), a drive-by download is invisible. It can start automatically when someone visits a Web site or views an HTML email message. Frequently, a drive-by download is installed along with other applications.

For example, file sharing programs might include downloads for spyware that track and report user information for targeted marketing purposes. An adware program that generates pop-up advertisements using that information might be downloaded at the same time as the tracking and reporting programs. If the user's computer's security settings are lax, it can be possible for drive-by downloads to occur without any action on the user's part.

- **Commercial Product Installation Bundling** - When commercial or shareware programs are downloaded, a user can get more than just the programs, like lots of additional spyware.
 - Grokster (a popular peer-to-peer file sharing program) installation can lead to the installation of BullGuard, Cydoor, EBates Moe Money Maker, GAIN, Golden Retriever, IGetNet, IPinsight, King Solomon's Casino, MyWay Speedbar, NetPalNow.com, NewtonKnows, Purity Scan, Sidestep, and Webhancer.
 - iMesh (another file sharing program) includes GAIN, Cydoor, Hotbar, eZula TopText, New.Net, CommonName, SideStep, NetPal, FavoriteMan, VX2, FlashTrack, and BonziBuddy.
- **Misrepresentation of Intention** - A product that promises to block ads, might actually deliver them. A product that promises to stop spyware might actually be a method of installing spyware.
- **Misrepresentation of Source** - A product might claim to be from a well-known, trustworthy company. Spyware can display a Web page that resembles, for example, a Microsoft product installation page, when it is not a Microsoft product at all.
- **Silent Download and Execution of Arbitrary Code** - This occurs when an already installed program causes the download and installation of other programs, without the user's consent or knowledge. Those other programs are usually spyware or adware.
- **Commercial Spyware, Keyloggers and RATs** - Commercial spyware products, such as ISpyNow, are small enough to be attached to an email. Commercial spyware products can be quite stealthy, too.
 - NETObserve Keylogger logs Internet conversation, window activity, application activity, clipboard activity, printing, keystrokes, Web site activity, and captures screenshots via Webcam.
 - STARR does not show up as an icon, appear in the Windows system tray, appear in Windows Programs, show up in the Windows task list, slow down the operation of the computer it is recording, and cannot be uninstalled without a pre-specified password.

Is All Spyware Hazardous?

Not all threats detected by a spyware scan are hazardous enough for an administrator to remove.

Cookies

The least hazardous of all threats are cookies. A cookie cannot decrease the security of a computer. In most cases, cookies that are detected as spyware threats are those that provide cross-site tracking, in order to build profiles about a user and provide more targeted marketing.

File sharing programs

Most file sharing programs are not completely hazardous, however when a user installs file sharing programs, like Morpheus, Kazaa, or iMesh, they often install additional spyware or adware programs onto their computer.

File sharing programs may or may not tell a user that they are doing this; if they do tell, they will do so in the license agreement. Unless users read the license agreement carefully, there is no way of knowing whether or not additional programs are going to be installed. Because of this, some P2P file sharing programs are hazardous and some are not hazardous.

Low risk adware

Generally, if the software EULA (End User License Agreement) is not violated, then software is generally not considered spyware. In the case of a program like Alexa, which is detected by CounterSpy as potential spyware, Alexa itself is not spyware, because it conforms to its license agreement. In fact, Alexa's license agreement is very straightforward. It describes every point of contact with Alexa's remote servers.

If you run Alexa and it serves a purpose to you, then do not remove it. If you want to be completely certain that Alexa is not acting as spyware, remove the 'related Links' feature of the product or remove Alexa completely by using the Windows Add/Remove Programs feature.

Signs of Spyware Infection

Below are some signs that a user's computer might be infected with spyware.

- The Web browser home page is set to an undesirable Web site and it cannot be changed.
- Problems with pop-up advertisements both online and offline.
- The computer is running slower than normal, and the connection to the Internet is not as fast as it used to be.
- There is abnormal network activity on the modem or broadband connection device

(cable or DSL modem).

- Favorite search engines are redirected to a non-familiar search engine or unrelated Web site.
- Items that the user did not add begin showing up in the Favorites list or Start-up menu.

Avoiding Spyware

The computer users on the network can do a lot to avoid exposing their computer to spyware attacks. Here are some Internet and computer tips, as well as notes about some common spyware traps for an administrator to share.

Click Responsibly!

Before spyware can be installed on a computer, the user usually has to **click** on something. Make this a rule: Don't click anywhere, unless you know it's safe.

Avoid Popup Ads or Dialogs

Creators of deceptive software use popup ads and dialogs to trick people into loading their software. For example, you open your browser and up pops a dialog box. It asks if you want to download software. "Click Yes or No." **Don't do it!** Do not click EITHER Yes or No. It's unlikely that clicking "No" might not make the popup go away. It more likely that you'll help download spyware to your computer.

Here's what to do. Try to close the Web page or dialog by clicking the "X" in the top right corner of the window. If that does not close the window that asked you to download something, close your browser. Restarting a browser to continue using the Internet is better than allowing your computer to be attacked by spyware.

Avoid Unsolicited Email "Spam!"

Always delete unsolicited email. Never open them. Unsolicited email is also called spam. It can use Internet Explorer or your email client to push spyware onto your computer. Get rid of unsolicited email without reading it when you can; turn off the preview pane to delete messages without opening them. Learn how to use any Junk email filters offered by your email provider.

In Outlook 2003, Tools | Options, click on the Security tab and select Change Automatic Download Settings. Make sure "Don't download pictures or other content automatically in HTML email" is checked.

Watch out for Free Software Downloads

Don't install anything without knowing exactly what it is. Your computer can become the target of spyware when you download internet data, such as utilities, games, toolbars, media players, or other software. Be careful about installing software directly from Web sites. Read all disclosures, including license agreements and privacy statements. Read the end-user license agreement (EULA) carefully, as some EULAs will actually tell you that if you install the program in question, you've also decided to install some spyware with the software. Check independent sources as well, as some EULAs won't tell you about spyware.

Watch out for Internet Cookies

While they may not be the worst form of spyware, information gathered via cookies can sometimes be matched with information gathered elsewhere to provide surprisingly detailed profiles of you and your browsing habits. Learn to use the options in your browser that allow you to clear the cache and off-line files. That's where cookies linger. Remember, though, if you dump the cookies, you can no longer rely on your computer to automatically log you into Web sites. You'll have to have passwords handy, so gather that information before you start removing those and all the other cookies that have landed on your computer as a result of your Internet usage.

Be Careful About Using File Sharing Programs

Also known as P2P (peer to peer), file sharing programs are popular applications. They are used to share files, such as movies and music, across the Internet. Many freeware and shareware file sharing programs such as Grokster, Kazaa and BearShare bundle adware with their product. Beware! Download the product, you get the adware, too.

Although most file sharing programs themselves are safe, the adware and spyware programs that might come with them could be dangerous. Never download executables via P2P, because you can't be absolutely certain what it is that you are downloading. It's a good idea to only download executables from reputable vendors or well-known and endorsed sites.

Index

.Net Compliant	17	Buy Online	7
Active Directory Support	16	Centralized management	
Adding Machines	43	Admin Console	5
Adding Machines to a Policy and Deploying the Agent Software	43	Centralized Management	4
Agent		Components	
Agent Deferred Communication	43	Agent Software	5
Components and Location.....	42	CounterSpy Enterprise Admin Console	5
start the policy service	43	CounterSpy Enterprise Server	5
stop policy service	43	Configuration.....	29
system requirements	42	set email server settings	30
what is an agent	42	set proxy server settings.....	30
Agent Communication.....	42	Connecting to the server	18
Agent Deployment	42	CounterSpy Enterprise Admin Console.....	5
Agent Software	5	CounterSpy Enterprise Components.....	5
Agents		CounterSpy Enterprise Features.....	4
define update schedule	39	CounterSpy Enterprise Server	5
deleting and reassigning.....	46	CounterSpy Enterprise Toolbar.....	21
displaying a reboot message.....	38	Creating Policies	31
displaying taskbar icon	38	Crystal Reports	17
manually scanning.....	41	default port numbers	9
manually update	39	Deleting and Reassigning Agents	46
reassign an agent to another policy.....	46	Deploy Agents	16
remove an agent from a policy	46	Deployment	
setting options	38	adding machines.....	43
unquarantine or delete.....	48	agents.....	42
updating.....	39	deploy agent software.....	43
Allowing Specific Threats	34	manually add a machine to a policy.....	44
Avoiding spyware		MSI installer.....	45
Avoid Popup Ads or Dialogs.....	65	self extracting executable	46
Avoid Unsolicited Email "Spam!"	65	Displaying a reboot message	38
Click Responsibly!	65	Displaying a Taskbar Icon on a computer that has an installed agent.....	38
Free Software Downloads	66	Downloading a Trial Version of CounterSpy Enterprise	10
Internet Cookies	66	Easy Deployment	4
Using File Sharing Programs.....	66	Email notifications	
Avoiding Spyware	65	add notification to policy	37

copy notifications from policy.....	37	Pull down	22
delete notification from policy	37	view	23
Modify threat level for email address	37	Minimum processor requirement.....	6
End-User License Agreement.....	71	Requirements for Workstation Agent	6
Executive Summary Report	53	Monitor Display Resolution	6
Exporting Reports	60	MSI installer	45
File menu	22	Obtaining CounterSpy Enterprise.....	7
Getting Started		Order by Telephone	7
Connecting to the server.....	18	Order Online.....	7
How CounterSpy Works	15	Ordering Online.....	7
Management Console	15	PDF Manual	7
Using CounterSpy Enterprise	15	Policies	
Hard Drive Requirement	6	adding.....	31
How CounterSpy Works.....	15	automatically add machines to policy	45
How Spyware Gets Installed.....	62	copying	32
Commercial Product Installation Bundling ...	63	creating.....	31
Commercial Spyware, Keyloggers and RATs	63	define update schedule for agents.....	39
.....	63	deleting	31
Drive-by Download	63	displaying a reboot message	38
Misrepresentation of Intention	63	displaying a taskbar Icon on a computer	38
Misrepresentation of Source.....	63	exporting.....	32
Silent Download and Execution of Arbitrary		importing.....	32
Code.....	63	manually add machines	44
Infected Machine Summary Report.....	54	renaming.....	32
Infected Machines Detail Report.....	55	setting actions.....	40
License	71	updating agents	39
License Agreement.....	71	Policy menu	24
Login to policy server	19	features.....	24
Machine History Report	56	Policy-based Rules	4
Management Console.....	15	Policy-Based Rules	31
Managing All Quarantined Items.....	49	Pull down menus.....	22
Managing Threats	50	Purchasing by Telephone	7
Manual	7	Quarantine	
Manually Scanning Agents.....	41	managing items	49
manually update all components.....	28	view spyware by agent	47
Menu		Quarantine pane	49
file.....	22	Quick start guide	12
policy	24		

RAM Requirement	6	options	33
Registration.....	26	scheduling	32
Reporting	17, 51	view results.....	47
create a Machine History Report	56	view spyware by agent	47
create a Threats Found Summary Report	57	schedule agent updates.....	28
create a Top Ten Infected Machines Report.....	59	Scheduling Scans	32
create an Executive Summary Report	53	Self extracting executable	46
create an Infected Machine Detail Report	55	Server and Agent Updates.....	28
create an Infected Machine Summary Report	54	Setting Actions	40
Crystal Reports.....	17	Setting Agent Options	38
Executive Summary.....	53	Setting Email Notifications	36
exporting.....	60	Setting Scan Options	33
exporting reports.....	60	Signs of Spyware Infection.....	64
generating reports	52	Spyware	
Infected Machine Summary Report	54	adware	61
Infected Machines Detail Report.....	55	Avoiding Spyware	65
Machine History Report	56	Browser Hijackers.....	61
Threats Found Detail Report	58	Browser Plug-ins.....	61
Threats Found Summary Report	57	Commercial Key Loggers	62
Top Ten Infected Machines	59	Cookies.....	64
view a Machine History Report	56	Dialer	62
view a Threats Found Summary Report	57	File sharing programs	64
view a Top Ten Infected Machines Report	59	File Sharing Programs	62
view an Executive Summary Report.....	53	hazards.....	64
view an Infected Machine Detail Report	55	How Spyware Gets Installed.....	62
view an Infected Machine Summary Report	54	Key Loggers.....	62
Reports	4, 51	Low risk adware.....	64
Requirements for Admin Console	6	Low Risk Adware	62
Requirements for Policy Server	6	RAT (Remote Administration Tool)	62
Running CounterSpy Enterprise	9	Remote Installers.....	62
Scan		Signs of Spyware Infection	64
all agents	41	Spyware.....	61
scan one agent	41	understanding spyware.....	61
Scanning Engine	4	What is Spyware?.....	61
Scans		Spyware Severity Level.....	16
define scan options.....	34	System management	
define schedules.....	33	configuration	29

System Management Section	26	View Quarantine	22
System Requirements.....	6	View Reports	22
Telephone Orders	7	View Threats.....	22
Threat Database Updates	29	Top Ten Infected Machines.....	59
ThreatNet	4	Unpacking and Installing CounterSpy Enterprise	8
Threats		Update agents.....	39
add to allowed threat list.....	35	Updates.....	28
allowing.....	34	database.....	29
copy allowed threats.....	35	Updating Agents.....	39
delete from allowed threats list	35	User License	71
email notifications	36	User License Agreement.....	71
managing.....	50	Using CounterSpy Enterprise.....	15
severity levels	36	View menu	23
Threats Found Detail Report.....	58	features.....	23
Threats Found Summary Report.....	57	view registration and license information	27
Toolbar.....	21	Viewing Scan Results	47
Add policy.....	21	Welcome	4
Connect	21	Windows 2000 Professional.....	6
Research Center	22	Windows 2000 Server	6
Save Settings	21	Windows Server 2003 Server.....	6
View Agents.....	22	Windows XP Professional	6

End-User License Agreement

SUNBELT SOFTWARE DISTRIBUTION, INC.

End-User License Agreement for SUNBELT CounterSpy Enterprise(TM)

PLEASE CAREFULLY REVIEW THE FOLLOWING TERMS AND CONDITIONS OF THIS SOFTWARE LICENSE (THE "LICENSE AGREEMENT"). THIS LICENSE IS A LEGALLY BINDING CONTRACT BETWEEN YOU (THE "LICENSEE") AND SUNBELT SOFTWARE DISTRIBUTION, INC. ("SUNBELT").

Introduction: The following software license terms and conditions apply to all of the software (the "Software") following this license. If, after reviewing the terms and conditions which follow this paragraph, you do not wish to be bound by its provisions, do not download the Software or, if the software has been delivered by CD ROM, destroy the CD ROM or return it to Sunbelt. If the Software has already been downloaded then immediately delete the Software. Once the Software has been downloaded or accessed all of the provisions of this License Agreement apply, even if the Software is subsequently deleted or returned. Any use of the Software by the Licensee shall constitute unqualified acceptance of this Agreement.

License: The Software is provided on a non-exclusive, non-transferable basis, and may not be copied, modified, or enhanced without the advance written authorization of Sunbelt. The Software includes significant elements, including its organization, algorithms, and logic, which Sunbelt has maintained as confidential information, which constitute trade secrets of Sunbelt, and which are protected by U.S. patent and/or copyright law and international treaty. Licensee agrees not to attempt to disassemble, reverse compile, or reverse engineer the software. The Software under this Agreement is the exclusive property of Sunbelt. This License Agreement does not grant Licensee any ownership right or title to, or interest in the Software or any part thereof, and Sunbelt retains all such rights, title, and interest.

Disclaimer of Warranty: THE SOFTWARE IS PROVIDED "AS IS" AND WITHOUT WARRANTY EXCEPT AS PROVIDED IN THE FOLLOWING PARAGRAPH. SUNBELT DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND WARRANTIES OF NON-INFRINGEMENT AND PERFORMANCE.

Limited Warranty: Sunbelt warrants that the Software covered by this License will, for a period of thirty (30) days following its installation, operate in accordance with the specifications found in the manual accompanying the Software.

Limitation of Liability: Sunbelt makes no representations or warranties that the operation of the Software will be uninterrupted or error free, or that it will produce the results desired by the Licensee. Sunbelt does not agree to provide modifications, enhancements, improvements or bug corrections, even if errors in the Software are reported to Sunbelt. Sunbelt shall not be liable for any special, incidental or consequential damages (including damages for loss or business, loss of profits, business interruption, etc.) arising from Licensee's use, or the inability of Licensee

to use, the Software, even if Sunbelt has been advised of the possibility of such damage.

Licensee Remedy: If Sunbelt is liable to Licensee for the breach of any of Sunbelt's obligations under the License, Licensee's sole and exclusive remedy shall be, at Sunbelt's option, to either receive a refund for the price Licensee paid for the use of Sunbelt's Software (less any taxes, shipping fees, etc.), or the repair or replacement of any defective Software.

Limitation on Exports: Licensee agrees that Licensee will not export or re-export the Software outside of the United States to any individual, business, third party, or other entity, or to any country subject to United States export restrictions. Any Licensee who receives the Software outside the United States agrees not to re-export the Software except as permitted by laws of the United States.

U.S. Government Rights: If you are obtaining Software on behalf of any part of the United States Government, the Software shall be deemed "commercial Software" and "commercial computer Software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

Miscellaneous: Licensee may make one backup copy of the Software, provided Licensee agrees not to grant access to such backup Software to any other individual or business entity. Licensee agrees not to alter or delete any copyright notice which is included with the Software. Except as expressly stated herein, there are no other agreements, understandings between the parties, or obligations on the part of Sunbelt relative to the Software. The laws of the State of Florida shall apply to the terms of this License Agreement.

YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT AND UNDERSTAND IT, AND THAT BY INSTALLING OR USING THE SOFTWARE YOU AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. YOU FURTHER AGREE THAT THIS AGREEMENT IS THE COMPLETE AND EXCLUSIVE STATEMENT OF THE RIGHTS AND LIABILITIES OF THE PARTIES. THIS AGREEMENT SUPERSEDES ALL PRIOR ORAL AGREEMENTS, PROPOSALS OR UNDERSTANDINGS, AND ANY OTHER COMMUNICATIONS BETWEEN US RELATING TO THE SOFTWARE OR THIS AGREEMENT.

2/09/2005

REV 2092005.1300