WebSpy Sentinel 3.2
User Guide

Please send all issues or queries to WebSpy Support (support@webspy.com)

This document is intended as a guide only. It aims to introduce the reader to issues that may be relevant to their organization, and to point out sources from which more detailed information may be obtained. It is **NOT** a substitute for professional legal advice.

Table of Contents

Overview of *WebSpy Sentinel*

WebSpy Sentinel is a program that enables you to record all web, mail newsgroup, telnet and FTP traffic on your network without the need for proxy server software. The logged data is stored in a log file format that can subsequently be imported into *WebSpy Analyzer* or Vantage and examined to identify Internet usage patterns of your employees or departments.

Sentinel log files can also be monitored by *WebSpy Live* for real time monitoring of your employees and department Internet activity. Visit www.webspy.com and follow the links to learn more about *Live* or see *Live's* Help for details on how to input log files for monitoring.

WebSpy Sentinel is made up of two parts: Sentinel Service, and Sentinel Management. Sentinel Service is the driver, which connects to your Network Device, and the service, which logs the data. The driver and the service are always installed together, so that the driver can 'see' all Internet traffic. Sentinel Management is used to configure the Sentinel Service running on multiple computers on the same network. You can install Sentinel Management on any computer on your network with access to all of the computers running Sentinel Service.

Note: For maximum logging with *WebSpy Sentinel,* you should place Sentinel Service on a computer that will have all network traffic flowing through or past it. If your Web/Mail/Newsgroup/Telnet/FTP traffic is split through two or more servers then you will have to install Sentinel Service on each of these servers to capture all Internet traffic for your organization. See Installing *WebSpy Sentinel* on page 5.

Sentinel Service captures all traffic passing through the network on which it is installed but only keeps (or logs) the protocols that you choose. You can log just the basic information about the Internet traffic you are seeing (i.e. source, destination, URL etc.) or you can capture all of the content of that traffic. See Protocol Configuration on page 12.

Please see Definitions on page 26 for an explanation of terms used in this manual.

What's New in Sentinel 3.2?

- POP3 and Secure Web –Sentinel 3.2 can now capture data from the POP3 and Secure Web protocols.
- Selective Name Resolution – Improve Sentinel's performance and efficiency by specifying the networks you want Sentinel to resolve usernames for.
- Extended log files - Sentinel now logs bytes sent & received, browser, query and status
- Automatically restarts capture – when you make changes to Sentinel's data capture settings, you no longer need to manually stop and start the service.
- Log per-protocol – You can now configure Sentinel to create one log file per protocol.
- Improved performance –Sentinel 3.2 has been optimized to improve capture speed and accuracy.

What happens when I use different operating systems?

- Any of the seven protocols can be captured if your computer is using Windows® 98 or above.
- All operating systems can capture full content (although this will affect machine performance). Only capture content if you require the captured information. This especially applies to HTTP (Web) traffic, due to the large quantity of data that will be captured. Regardless of whether content is captured or not, the logs will show you all of the Internet activity.
- Optimally, you would run WebSpy Sentinel on a computer using Windows NT®, Windows® 2000 or Windows® XP operating systems. Optimally, your Sentinel Server will have Windows Server® 2003, Windows® XP, Windows® Vista or Windows Server 2008.
- *WebSpy Sentinel* is memory and CPU intensive. The minimum requirements for *Sentinel* are a Pentium with 128MB of RAM. See the Sentinel Planning and Installation Guide for more information on the hardware requirements for installing *Sentinel.*

Getting Help

This guide is intended to help you work out how to effectively use *WebSpy Sentinel* to suit your organization's needs.

If you require more information on using *Sentinel*, please consult the Planning and Installation Guide and Sentinel Management's on-line Help.

WebSpy's website, http://www.webspy.com, provides documentation, FAQs and useful hints and tips for using WebSpy products.

Finally, you can contact WebSpy Support at support@webspy.com.

Installing *WebSpy Sentinel*

When you choose to install *WebSpy Sentinel*, there are a few preliminary steps you will need to go through to ensure *Sentinel* will work most effectively. These steps are:

- Determine your optimum installation point or points, where all the Internet traffic on your network passes in a form that *Sentinel* can use
- Decide the most efficient way for you to tap into the installation point(s)
- Remove any existing *WebSpy Sentinel 2.x* or *Sentinel 3.x* components from the computer that will be running *WebSpy Sentinel 3.2*

Once you have completed these steps, you can install *WebSpy Sentinel 3.2*.

Usually, you will only need one, or perhaps two, computers running Sentinel Service to capture all the Internet traffic on your network. You can install Sentinel Management on any computer with access to the computer(s) running Sentinel Service.

The Sentinel Service uses the WinPCap driver to monitor traffic flowing through network cards. You will notice this driver being installed when you install the Sentinel Service. More information about this driver is available from the WinPCap website, http://www.winpcap.org.

Refer to WebSpy Sentinel's Planning and Installation Guide for detailed instructions on how and where to install *WebSpy Sentinel*. This guide is available from the website, http://www.webspy.com.

Removing Sentinel 2.x or 3.x Components

If you are upgrading from *Sentinel 3.x* to *Sentinel 3.2* you should ensure that *Sentinel 3.x* has been completely removed from the computer that you are installing *Sentinel* on. You can do this using Add/Remove Programs from the Control Panel on your computer.

If you have previously used a similar product to *Sentinel*, you may find that installed components from that product will interfere with *Sentinel's* operation. It is recommended that you ensure all such components are removed. If this is not possible, you should contact the product's vendor for full un-installation instructions.

Installing Sentinel 3.2

To install *WebSpy Sentinel*, simply run the provided installation program on each Sentinel Server, and the computers you want to manage these servers from.

Hint: If you want to install just Sentinel Service or just Sentinel Management onto the computer, choose the Custom installation option, and select the appropriate component to install.

After installation, you must configure *WebSpy Sentinel* using Sentinel Management so that it monitors the correct network device for each Sentinel Server.

To do this:

1. Start Sentinel Management
2. From the server list in Sentinel Management, select the Sentinel Server that you want to change the network device for
3. Click on the **Connect** button on the toolbar if necessary
4. If the Connect to dialog appears, enter your user name and password, then click **OK**
5. If necessary, go to the Home view by clicking on the navigation link at the top of Sentinel Management
6. Click on the Network Device 'select a different device' link to open the Select Network Device dialog
7. Select the appropriate network device from the dialog then click **OK**

8 Click on the **Start** button on the toolbar of Sentinel Management. *Sentinel* will now start capturing data on the network device currently listed next to Network Device in the Home view.

Note: By default, all servers have the user name of 'admin' and password of 'webspy'. You should change this password as soon as possible, see Changing your Password on page 24 for instructions on how to do this.

Please see Starting Data Capture on page 11.

Uninstalling Sentinel 3.2

You can uninstall *WebSpy Sentinel* using Add/Remove Programs in your computer's Control Panel. Uninstalling *Sentinel* will not remove folders or files created by the software itself. This will include all your configuration files and log data that *Sentinel* collected. If you do not wish to keep this information you will need to delete any folders remaining in the location that you originally installed *Sentinel*. However if you are reinstalling *Sentinel* and wish to keep your previous configurations and log data you do not need to delete the files and folders.

Registering Sentinel

If you do not register *WebSpy Sentinel*, your trial will run out thirty days after you first use the program. Once your trial has run out, your Sentinel Servers will no longer capture data.

You will need to register Sentinel Management, and then Sentinel Management will unlock all of the Sentinel Servers you are currently connected to. You can manually unlock other servers at a later time if necessary. See also Unlocking Sentinel Servers on page 8.

To register Sentinel Management, go to **Tools | Registration Wizard** to launch the Registration Wizard.

There are two parts to the registration process:

- Requesting an unlock code; and
- Entering an unlock code to register your copy of *Sentinel*

If you have any problems with the registration process, please contact support@webspy.com.

Note: Your computer must have an active Internet connection to be able to register your software.

If, for any reason, you need to reinstall *Sentinel*, use the Registration Wizard to request a new unlock code. You will not be able to use your old unlock code. Please contact WebSpy Support if you have any problems registering your software.

Requesting an Unlock Code

To request an unlock code:

1. Launch the Registration Wizard by choosing **Tools | Registration Wizard** from the main menu
2. Once the Registration Wizard is open, you need to enter your details into the Registration Details and User Contact Details pages of the wizard
   WARNING:
   These details are essential for WebSpy Ltd. to generate a successful unlock code for your copy of *Sentinel*. If you do not supply your correct details, WebSpy Ltd. cannot confirm that you have purchased your software, and an unlock code will not be generated for you.
3. After you have entered all your details, the Submission page will show you the progress of your submission
4. If it is successful, you will be able to click **Finish** to complete the wizard

Once the wizard has been completed, an unlock code for the software will be emailed to the address you provided in the User Contact Details page. You will now need to enter your unlock code.

Entering your Unlock Code

After you have requested an unlock code, you will receive an email containing that unlock code. This unlock code needs to be entered into the Registration Wizard.

To enter your unlock code:

1. Launch the Registration Wizard by choosing **Tools | Registration Wizard** from the main menu of Sentinel Management
2. Copy the unlock code from the registration email
3. On the Enter Unlock page of the wizard paste the unlock code that you copied from the email into the Unlock Code edit box
4. Click **Next**
5. Your unlock code will be verified, and your registration confirmed
6. To close the wizard, click **Finish**

Sentinel Management will now automatically unlock all of the Sentinel Servers you are currently connected to.

Unlocking Sentinel Servers

Once you have registered Sentinel Management, Sentinel Management will automatically unlock all Sentinel Servers that you are currently connected to.

If you are not connected to a server, Sentinel Management will not be able to unlock that server automatically.

To unlock the server manually:

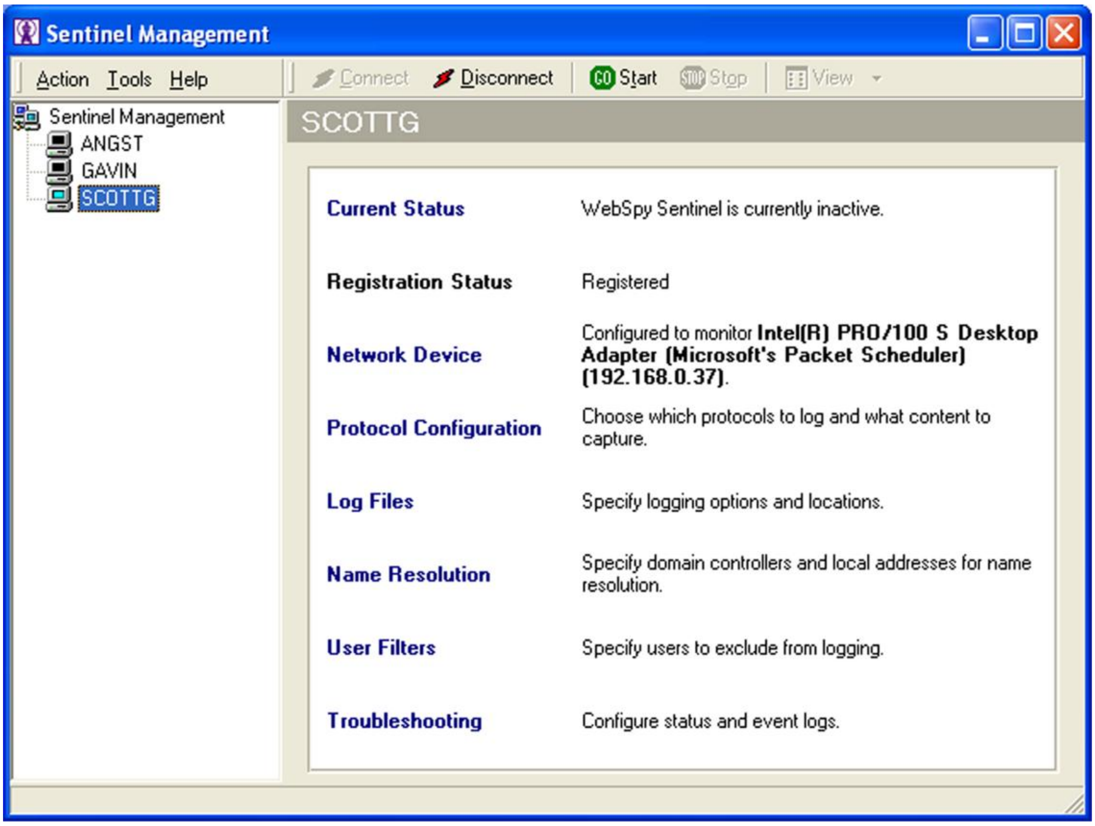
1. Start Sentinel Management
2. From the server list in Sentinel Management, select the server you wish to connect to
3. Click on the **Connect** button on the toolbar if necessary
4. If the Connect to dialog appears, enter your user name and password, then click **OK**
5. Select **Action | Unlock Server** from the main menu, or right-click on the server and select 'Unlock Server' from the pop-up menu that is displayed

Note: Once *WebSpy Sentinel's* trial period has expired, your Sentinel Servers will not capture data unless you register *Sentinel* and unlock each of the servers.

Sentinel Management

After installation, you can manage Sentinel Service via Sentinel Management. From Sentinel Management you can:

- See which computers on your network are running Sentinel Service via a server list
- Start and stop data capture
- Change the network device data is captured on
- Add/remove protocols from the list of protocols to be logged
- Choose the location of *Sentinel's* log files
- Configure name resolution
- Apply user filtering to the log files captured
- Choose the location and configure *Sentinel's* event log files



Current Status	WebSpy Sentinel is currently inactive.
Registration Status	Registered
Network Device	Configured to monitor **Intel(R) PRO/100 S Desktop Adapter (Microsoft's Packet Scheduler) (192.168.0.37)**.
Protocol Configuration	Choose which protocols to log and what content to capture.
Log Files	Specify logging options and locations.
Name Resolution	Specify domain controllers and local addresses for name resolution.
User Filters	Specify users to exclude from logging.
Troubleshooting	Configure status and event logs.

Figure 1 - Sentinel Management - Home View

When you start Sentinel Management, any Sentinel Servers running on the same TCP/IP sub network will automatically be detected. If you have Sentinel Servers running on different TCP/IP sub networks within your organization's network, they will not be automatically detected. Generally, if you have routers separating sections of your network, you will need to manually add servers in different sections to be able to administer those servers.

You can also manually add a server using its name or IP address. You may need to do this if you accidentally delete a server. To do this, click on 'Sentinel Management' in the server list and select **Action | Add Server** from the main menu. Type the new name of the server into the Host Name dialog that is displayed.

You can then connect to any of these Sentinel Servers by selecting the server name from the server list and entering your password if necessary. See Connecting to a Sentinel Server on page 10.

Once you have connected to that server, you can see:

- The number of data packets Sentinel Service has logged
- The registration status of the server, and
- The current network device used to capture data

If you click on the Log Files link, you will be able to see the location of the stored log files. See Log Files on page 15.

You can start or stop data capture for the selected computer using the **Start** and **Stop** buttons. This does not start or stop Sentinel Service, but just instructs Sentinel Service to start or stop capturing data. See Starting Sentinel Service Manually on page 22 and Stopping Sentinel Service Manually on page 23 to find out how to start or stop Sentinel Service.

In Sentinel Management, the network device that Sentinel Service is currently capturing data from is displayed under Network Device in the **Home** view. You can also choose which Network Device data is being captured from, if the computer you are connected to has more than one Network Device installed. See Changing the Network Device for Data Capture on page 11.

Hint: There is no relationship between the number of hits (files or items downloaded from an Internet site) and the number of packets that are logged by *Sentinel*.

Adding a Sentinel Server Manually

You can manually add a server using its name or IP address. You may need to do this if you accidentally delete a server.

To manually add a Sentinel Server:

1. Click on 'Sentinel Management' in the server list
2. From the main menu select **Action | Add Server**
3. Type in a new host name for your server then click **OK**. The new Server will be displayed in the server list.
4. You can then connect to this server by clicking on the **Connect** button on the toolbar and entering your user name and password into the Connect to dialog

Connecting to a Sentinel Server

Before you can configure Sentinel Service on a given Sentinel Server on your network, you will need to connect to Sentinel Service on that server.

To connect to a server:

1. Start Sentinel Management
2. From the server list in Sentinel Management, select the server you wish to connect to
3. Click on the **Connect** button on the toolbar if necessary
4. If the Connect to dialog appears, enter your user name and password, then click **OK**

Once you have connected to a server, that connection will remain active until you disconnect, or until you close Sentinel Management. Maintaining any connection over a network requires resources; for this reason, it is recommended that you limit the number of active connections to less than ten. However, repeatedly connecting to or disconnecting from a Sentinel Service may also place an undesirable load on your network, so if you are going to be reusing a connection (for example, to compare packets logged), it is recommended that you leave that connection in place.

Disconnecting from a Sentinel Server

You may want to disconnect from a Sentinel Server, perhaps to minimize the number of active connections you are maintaining across your network. There are two ways you can do this.

To disconnect from a single server:

1. From the server list in Sentinel management, select the Sentinel Server that you wish to disconnect from
2. Click on the **Disconnect** button on the toolbar.

To disconnect from all Sentinel Servers at once, close Sentinel Management.

Changing the Network Device for Data Capture

Some servers may have more than one network device installed and you may need to change which device Sentinel Service captures data from. You will need to do this using Sentinel Management.

To change the network device:

1. Start Sentinel Management
2. From the server list in Sentinel Management, select the Sentinel Server you want to change the network device for
3. Click on the **Connect** button on the toolbar if necessary
4. If the Connect to dialog appears, enter your user name and password, then click **OK**
5. If necessary, go to the Home view by clicking on the navigation link at the top of Sentinel Management
6. Click on the Network Device link to open the Select Network Device dialog
7. Select the appropriate network device from the dialog then click **OK**

Click on the **Start** button on the toolbar of Sentinel Management. *Sentinel* will now start capturing data on the network device currently listed next to Network Device in the Home view.

Starting Data Capture

To start capturing data using Sentinel Service on a single computer:

1. Start Sentinel Management
2. From the server list in Sentinel Management, select the Sentinel Server you want to start capturing data from
3. Click on the **Connect** button on the toolbar if necessary
4. If the Connect to dialog appears, enter your user name and password, then click **OK**
5. Click the **Start** button on the toolbar

Hint: If the Start button on the toolbar of Sentinel Management is disabled you may need to specify a network device for data capture. See Changing the Network Device for Data Capture on page 11 for more information on adding or specifying a new network device.

Stopping Data Capture

If you are capturing data from several Sentinel Servers on your network, you can choose to stop data capture on any particular server if necessary.

To stop Sentinel Service from capturing data on a single computer:

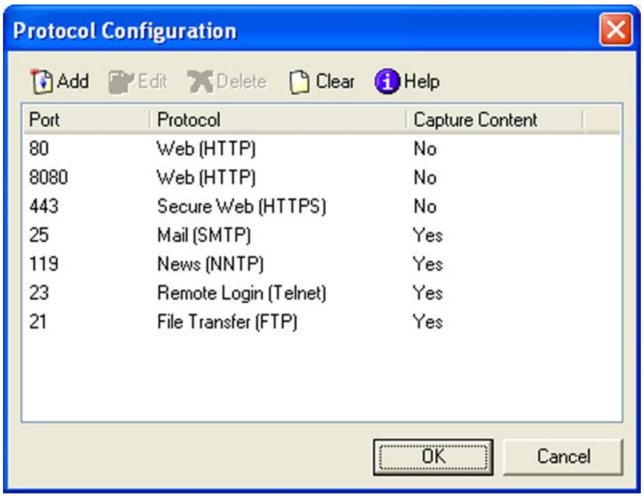
1. Start Sentinel Management
2. From the server list in Sentinel Management, select the Sentinel Server that you wish to stop capturing data from
3. Click on the **Connect** button on the toolbar if necessary
4. If the Connect to dialog appears, enter your user name and password, then click **OK**
5. Click the **Stop** button on the toolbar

Protocol Configuration

The Protocols view displays the names of the protocols currently being captured on the Sentinel Server you are connected to.

To open this view:

1. Start Sentinel Management
2. From the server list in Sentinel Management, select the Sentinel Server that you want to view the Protocol configuration for
3. Click on the **Connect** button on the toolbar if necessary
4. If the Connect to dialog appears, enter your user name and password, then click **OK**
5. Access the Protocols view by either clicking the Protocol navigation link or by clicking the Protocols link on the Home view



Port	Protocol	Capture Content
80	Web (HTTP)	No
8080	Web (HTTP)	No
443	Secure Web (HTTPS)	No
25	Mail (SMTP)	Yes
119	News (NNTP)	Yes
23	Remote Login (Telnet)	Yes
21	File Transfer (FTP)	Yes

Figure 2 - Sentinel Management - Protocols View

Figure 2 above shows the Protocols view in Sentinel Management. In this view you can configure which protocols are captured, whether content is captured, and what port the content is captured from.

For mail, telnet, newsgroup and FTP traffic, Sentinel Service is configured to capture the content of the e-mail, posting or file transfer. For Web traffic the default is to not capture the content. If you wish to change any of these defaults, use the Capture Content checkbox on the Protocol dialog, which enables you to specify whether or not to capture all the details of the currently selected protocol. See Changing Content Capture Settings on page 13.

For example, the content of an email includes the sender, the recipient, the subject and the body of the email. The content of a web page includes any text, images, sound files or style sheets that are contained within the page.

Start Capturing Data from a Port

Sentinel can capture Web, mail, newsgroup, telnet and FTP traffic on your network. Each of these protocols have associated port numbers and a computer running Sentinel Service can be configured to monitor any data passing from this port to your network.

Sentinel enables you to specify the protocols and the port you wish to capture data from. For example, you may want to capture file transfers using the FTP protocol on port 21. Sentinel will monitor this port and capture information relating to any transfers, as well as capture the full content of any files transferred.

The following is a list of protocols and the port numbers typically associated with them:

- Web (HTTP), port 80, 8080
- Secure Web (HTTPS), port 443
- Mail (SMTP), port 25
- News (NNTP), port 119
- Remote Login (Telnet), port 23
- File Transfer (FTP), port 21
- POP3, port 110

Although *Sentinel* is configured to monitor the above protocols with their typical port numbers, protocol transfers can occur over a variety of other ports. Therefore Sentinel Management provides you with the option of configuring your server to capture protocols from different ports.

To configure Sentinel to capture protocols from different ports:

1. From the server list in Sentinel Management, select the Sentinel Server you wish to change the port number for
2. Click on the **Connect** button on the toolbar if necessary
3. If the Connect to dialog appears, enter your user name and password, then click **OK**
4. Open the **Protocols** view by clicking on the **Protocols** navigation link
5. Click on the **Add** button to open the Protocol dialog
6. Type in the new TCP Port Number
7. Select the protocol to capture from the drop-down list
8. Choose whether or not to capture content for that protocol by checking or unchecking the 'Capture Content' checkbox
9. Click **OK** close the Protocol dialog
10. Click **OK** button at the bottom of the Protocols view to update Sentinel Service on that server

Stop Capturing Data from a Port

To stop capturing data from a particular port:

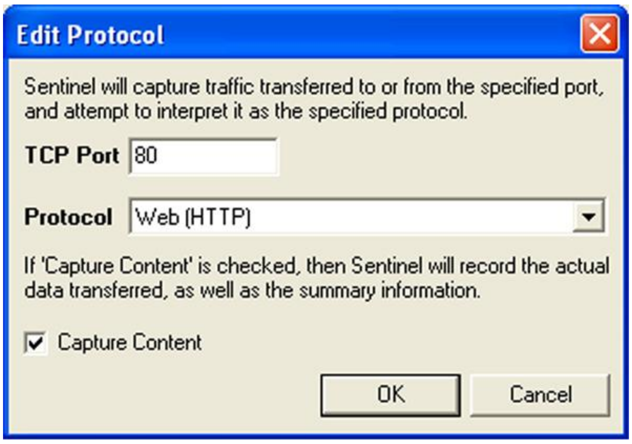
1. From the server list in Sentinel Management, select the Sentinel Server you want to remove the port number for
2. Click on the **Connect** button on the toolbar if necessary
3. If the Connect to dialog appears, enter your user name and password, then click **OK**
4. Open the Protocols view by clicking on the Protocols navigation link
5. Select the port that you want to stop capturing data from out of the list
6. Click the **Delete** button on the toolbar
7. Click **OK** at the bottom of the Protocols View to update Sentinel Service on that server

Changing Content Capture Settings

To configure Sentinel Service to capture the content of a protocol from a particular port:

1. From the server list in Sentinel Management, select the Sentinel Server you wish to change the content capture settings for
2. Click on the **Connect** button on the toolbar if necessary
3. If the Connect to dialog appears, enter your user name and password, then click **OK**
4. Open the Protocols view by clicking on the Protocols navigation link
5. Select the protocol that you want to change the content capture settings for from the list and click on the **Edit** button to launch the Protocol dialog

6. Make any necessary changes to the Protocol, then choose whether or not to capture content for that protocol by checking or unchecking the 'Capture Content' checkbox
7. Click **OK** to close the Protocol dialog



Edit Protocol

Sentinel will capture traffic transferred to or from the specified port, and attempt to interpret it as the specified protocol.

TCP Port 80

Protocol Web (HTTP)

If 'Capture Content' is checked, then Sentinel will record the actual data transferred, as well as the summary information.

☑ Capture Content

Figure 3: Changing content capture settings

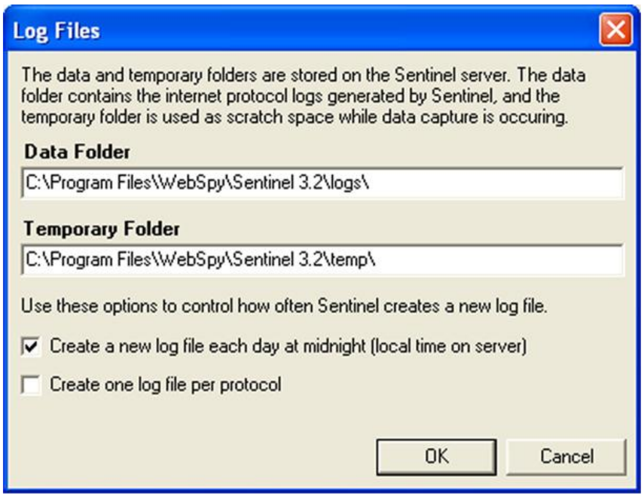
Log Files

This view displays the names and locations of the folders containing log files associated with *WebSpy Sentinel*. This includes the Data Folder and the Temporary folder.

Note: The locations given are local to each Sentinel Server. *Sentinel* enables you to change the log file locations for these folders.

To access the Log Files view:

1. Start Sentinel Management
2. From the server list in Sentinel Management, select the server that you want to view log details for
3. Click on the **Connect** button on the toolbar if necessary
4. If the Connect to dialog appears, enter your user name and password and click **OK**
5. Go to the **Log Files** view by clicking on the **Log Files** navigation link.



The data and temporary folders are stored on the Sentinel server. The data folder contains the internet protocol logs generated by Sentinel, and the temporary folder is used as scratch space while data capture is occuring.

Data Folder: C:\Program Files\WebSpy\Sentinel 3.2\logs\

Temporary Folder: C:\Program Files\WebSpy\Sentinel 3.2\temp\

Use these options to control how often Sentinel creates a new log file.

☑ Create a new log file each day at midnight (local time on server)

☐ Create one log file per protocol

Figure 4 - Sentinel Management - Log Files View

Data logs contain the data and content that Sentinel Service has captured and are stored in the Data Folder.

The Temporary Folder is used to store a copy of large items as they are downloaded, before the item is added to the log file. Once an item has completely downloaded, it is deleted from the temporary folder.

It is recommended that the temporary folder is not a sub folder of the data folder.

You would use the data logs as you would any proxy log files, except that the *WebSpy Sentinel* log files can also contain the content of the files and resources accessed. *WebSpy Analyzer* is perfect for monitoring and analyzing network usage, especially since it can display the content of any emails, newsgroups or web pages that have been downloaded. See Using Sentinel Log Files in *Analyzer* on page 25.

You can also use *Sentinel* log files with *WebSpy Live* for real time Internet monitoring.

Note: The locations given for the data log folder are relative to that server i.e. if the location of the capture log folder for Computer A is given as 'C:\Program Files\WebSpy\Sentinel 3.2\logs\,' to open the log file, you will need to go to C:\Program Files\WebSpy\Sentinel 3.2\logs\ on Computer A **NOT** the computer you are running Sentinel Management on.

Changing Log File Locations

You can change the location of any of the log files kept by a Sentinel Server.

To do this:

1. Start Sentinel Management

2. From the server list in Sentinel Management, select the Sentinel Server that you wish to change the log file location for
3. Click on the **Connect** button on the toolbar if necessary
4. If the Connect to dialog appears, enter your user name and password, then click **OK**
5. Go to the **Log Files** view by clicking the **Log Files** navigation link
6. Type the new file location into the appropriate box and click **OK**

Hint: You can set up each server to store its logs in a central location, however each Sentinel Server must write to a separate folder. Remember that Sentinel Service must be able to write to that central location.

Name Resolution

To resolve user names, *WebSpy Sentinel* uses your Windows NT®, Windows® 2000 or Windows® XP security logs.

Note: (Sentinel Build 3.2.2.3074) There are currently issues preventing the username resolution feature working correctly when your domain controller is running Windows Server 2003 and above. There may also be issues logging usernames for the client machines running Windows Vista and above. This feature will be improved in a future version of Sentinel.

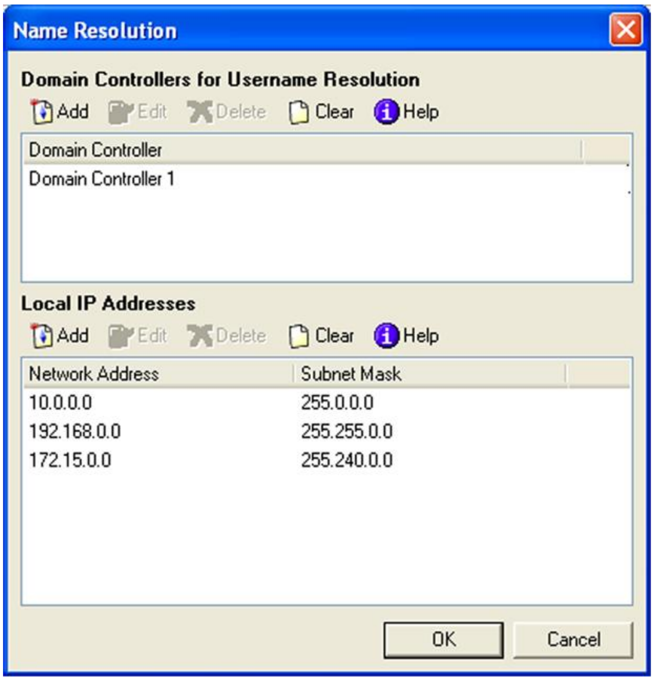
There are a number of conditions that have to be met before *Sentinel* can resolve user names, including:

- *WebSpy Sentinel* must be capturing data from a Windows NT®, Windows® 2000 or Windows® XP domain
- Sentinel Service must be run on a computer using the Windows NT®, Windows® 2000 or Windows® XP operating systems, in the same domain as the users whose user names you wish to resolve
- Sentinel Service must be run as a user with rights to audit the domain security logs
- Sentinel Service must be run as a user with rights to write to the *WebSpy Sentinel* installation and storage locations (since Program Files is write-protected for non-admin users)

For information on configuring the above conditions, please refer to the WebSpy Sentinel Planning and Installation Guide, available from the WebSpy website, http://www.webspy.com.

Configuring Sentinel to log usernames instead of IP addresses requires two steps:

1. Add the domain controller to use for resolving IP addresses to user names
2. Add the networks (Local IP addresses) that you want to include in the username resolution process



Domain Controller
Domain Controller 1

Network Address	Subnet Mask
10.0.0.0	255.0.0.0
192.168.0.0	255.255.0.0
172.15.0.0	255.240.0.0

Figure 5: Sentinel Management - Name Resolution View

Adding a domain controller

To be able to include user names in its log files, each Sentinel Server must have access to the domain controller administering access for the users the Sentinel Server is monitoring.

To ensure that the required information is available, for each Sentinel Server you should add all of the primary or backup domain controllers accessible to that server.

To do this:

1. Start Sentinel Management
2. From the server list in Sentinel Management, select the Sentinel Server that you want to add domain controllers for
3. Click on the **Connect** button on the toolbar if necessary
4. If the Connect to dialog appears, enter your user name and password, then click **OK**
5. Go to the **Name Resolution** view by clicking on the **Name Resolution** navigation link
6. Click on the **Add** button at the top of the view to launch the Add Server dialog
7. Type the name of the new domain controller into the box, and click **OK** to close the dialog
8. Click **OK** on the Name Resolution view.

You will need to repeat steps 6 - 7 for each of your domain controllers.

You also need to add the local IP addresses that you want included in the name resolution process, otherwise Sentinel will not resolve any user names (see Adding Local IP Addresses on page 18).

Note: This explanation is to be used as a guide only. If you have any further problems, you should contact your system administrator or consult your network documentation. Detailed instructions on resolving user names can also be found in the Sentinel Planning and Installation guide.

Adding Local IP Addresses

Resolving usernames, especially on large networks, can degrade Sentinel's performance. For this reason, you can specify the networks that you want to include in the username resolution process and exclude all other addresses from the process.

Important!
If you do not enter any networks, Sentinel will not resolve any usernames.

To add a network:

1. Start Sentinel Management
2. From the server list in Sentinel Management, select the Sentinel Server that you want to add domain controllers for
3. Click on the **Connect** button on the toolbar if necessary
4. If the Connect to dialog appears, enter your user name and password, then click **OK**
5. Go to the **Name Resolution** view by clicking on the **Name Resolution** navigation link
6. Click the **Add** button under the 'Local IP Addresses' section
7. Enter the network address into the network address edit box. For example, a common internal network address is 192.168.0.0.
8. Enter the subnet mask associated with the network you want to resolve usernames for. For example 255.255.255.0.
9. Click **OK**

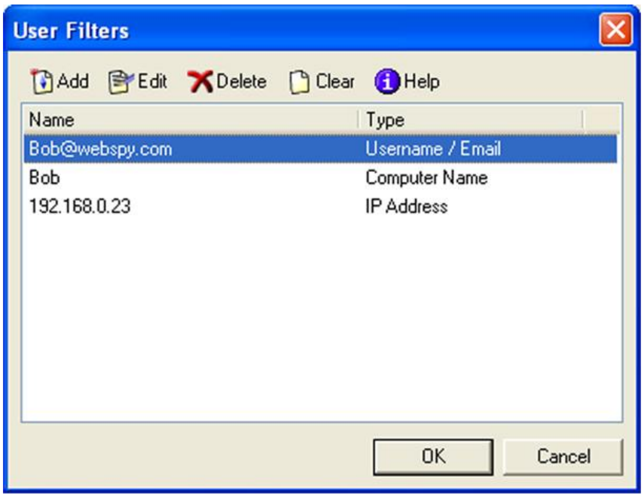
To resolve all usernames, enter the network address 0.0.0.0 and the subnet mask 0.0.0.0. This combination will match all IP addresses and resolve all usernames.

User Filters

In the User Filters view you can exclude specific users from the log files that *WebSpy Sentinel* is creating. For example, you may filter out your Accountant as a user to reduce the risk of capturing confidential accounts information.

To access the User Filters view:

- Start Sentinel Management
- From the server list in Sentinel Management, select the server that you want to view log details for
- Click on the **Connect** button on the toolbar if necessary
- If the Connect to dialog appears, enter your user name and password and click **OK**
- Go to the **User Filters** view by clicking on the **User Filters** navigation link.



Name	Type
Bob@webspy.com	Username / Email
Bob	Computer Name
192.168.0.23	IP Address

Figure 6: Sentinel Management - User Filters View

Specifying User Filters

You can apply user filters based on a user name, email address, computer name or IP address. To exclude a user by the name of Bob from your data logs you could add the following filters:

- User name - Bob
- Email address - Bob@webspy.com
- Computer name - Bob01
- IP address - 190.132.0.42

To specify user filtering:

1. Start Sentinel Management
2. From the server list in Sentinel Management, select the Sentinel Server that you wish to apply user filtering to
3. Click on the **Connect** button on the toolbar if necessary
4. If the Connect to dialog appears, enter your username and password, then click **OK**
5. Go to the User Filters view by clicking the correct navigation link
6. Click the **Add** button on the toolbar
7. Add a name, email address, computer name or IP address to filter and select the appropriate type from the Type drop down list
8. Click **OK** to add the user to the list
9. Click on the **OK** button at the bottom of the User Filters view

Hint: If user name resolution on your network is not configured, you will not be able to apply user filtering based on IP address. Try filtering by computer name instead.

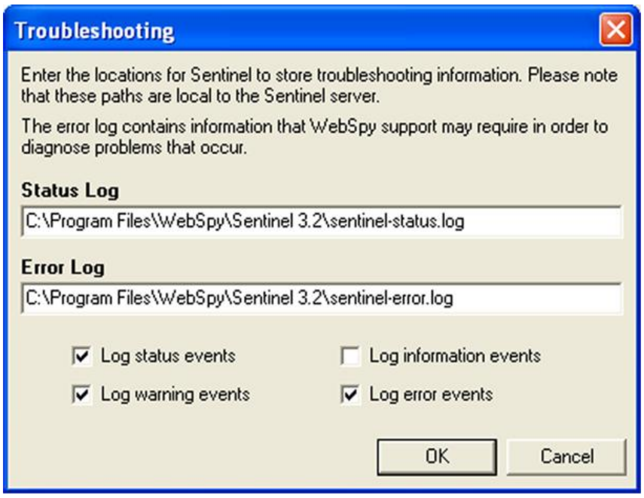
Troubleshooting

This view displays the names and locations of the event log files associated with *WebSpy Sentinel*. The locations given are local to each Sentinel Server. Event log files contain useful troubleshooting information.

You can also use *Sentinel* to resolve user names in this view.

To access the **Troubleshooting** view:

1. Start Sentinel Management
2. From the server list in Sentinel Management, select the server that you want to view log details for
3. Click on the **Connect** button on the toolbar if necessary
4. If the Connect to dialog appears, enter your user name and password and click **OK**
5. Go to the **Troubleshooting** view by clicking the **Troubleshooting** navigation link



Enter the locations for Sentinel to store troubleshooting information. Please note that these paths are local to the Sentinel server.

The error log contains information that WebSpy support may require in order to diagnose problems that occur.

Status Log: C:\Program Files\WebSpy\Sentinel 3.2\sentinel-status.log

Error Log: C:\Program Files\WebSpy\Sentinel 3.2\sentinel-error.log

☑ Log status events ☐ Log information events

☑ Log warning events ☑ Log error events

Figure 7 - Sentinel Management Troubleshooting View

WebSpy Support may be able to use the data contained in the event log files for diagnostic purposes in the event of any issues with *Sentinel*. The Status log provides a record of when the Sentinel Service was started or stopped on that computer. If you found that Sentinel Service had not been capturing data on a particular computer, you could check the status log to determine whether Sentinel Service was simply not started, or if there was a different problem. The Error log contains more detailed information. If you are having problems with *WebSpy Sentinel*, the Error log will be used by WebSpy Support to help identify and solve your problem.

Note: The locations given for the log files are relative to that computer i.e. if the location of the event logs for Computer A is given as ‘C:\Program Files\WebSpy Sentinel\logs\’ to open any of the log files, you will need to go to C:\Program Files\WebSpy Sentinel\logs\ on Computer A **NOT** the computer you are running Sentinel Management on.

Changing Events to be logged

You can change which events are logged in the Event Log. You can log:

- Status events - when Sentinel Service is started or stopped on that Sentinel Server
- Information events - internal status information
- Warning events - non-fatal error information
- Error events - details of issues that caused Sentinel Service to stop

To change the events to be logged for a particular server:

1. Start Sentinel Management
2. From the server list in Sentinel Management, select the Sentinel Server that you want to change the events log for
3. Click on the **Connect** button on the toolbar if necessary

4. If the Connect to dialog appears, enter your user name and password, then click **OK**
5. Go to the **Troubleshooting** view by clicking on the **Troubleshooting** navigation link
6. Check or uncheck the checkboxes at the bottom of the view as appropriate
7. Click **OK**

Changing Log File Locations in Event Logs

You can change the location of any of the log files kept by a Sentinel Server.

To do this:

1. Start Sentinel Management
2. From the server list in Sentinel Management, select the Sentinel Server that you wish to change the log file location for
3. Click on the **Connect** button on the toolbar if necessary
4. If the Connect to dialog appears, enter your user name and password, then click **OK**
5. Go to the **Troubleshooting** view by clicking the **Troubleshooting** navigation link
6. Type the new file location into the appropriate box
7. Click **OK**

Hint: You can set up each server to store its logs in a central location. Remember that Sentinel Service (Windows NT®, Windows® 2000 and Windows® XP) must be able to write to that central location. If you use Windows® 98, you will need to make sure the user that is currently logged on to the Sentinel Server has permission to write to the central location.

Starting Sentinel Service Manually

Sentinel Service may need to be started manually if you have disabled the option to start it up automatically whenever the computer is booted up. Once you have started Sentinel Service using the following instructions, you can start data capture via Sentinel Management (see page 11).

1. Go to Start Menu | Settings | Control Panel | Administrative Tools
2. Double-click Services to open the Services dialog
3. Find ‘Sentinel’ in the list and:
   Either
   Double-click on it to open its Properties dialog and click on the **Start** button on the General tab
   Or
   Select ‘Sentinel’ from the list and use the ► button on the toolbar of the Services dialog

Stopping Sentinel Service Manually

You would normally stop Sentinel Service from capturing data through Sentinel Management (see page 11). If this application is not working for some reason you may need to stop Sentinel Service itself, and therefore data capture, manually. To do this:

1. Go to **Start Menu | Settings | Control Panel | Administrative Tools**
2. Double-click Services to open the Services dialog
3. Find 'Sentinel' in the list and:
   Either
   Double-click on it to open its Properties dialog and click on the **Stop** button on the General tab
   Or
   Select 'Sentinel' from the list and use the ■ button on the toolbar of the Services dialog

Using Passwords

Passwords are used in Sentinel Management to limit access to viewing status information and changing configuration options to authorized users.

Sentinel Management enables you to set a password for a server, change the password for a server and remember the password for a server. Passwords are specific to a Sentinel Server; therefore, a different password will be required to connect to each server.

Note: By default, all servers have the same user name of 'admin' and password of 'webspy'.

Hint: You should change the user name and password for each server as soon as possible after installation.

Using the Connect to Dialog

The Connect to dialog appears whenever you try to connect to a Sentinel Server, unless you have chosen to remember your password by checking the 'Remember Password' checkbox in the Connect to dialog.

To access the server, type your user name and password into the appropriate boxes, and click **OK**.

Changing your Password

Sentinel Management enables you to change the password required to connect to a particular Sentinel Server. Note that you cannot have more than one user name or password for a single server.

To change a password:

1. Start Sentinel Management
2. Select the Sentinel Server from servers list that you wish to change the password for
3. Click on the **Connect** button if necessary
4. If the Connect to dialog appears, enter your user name and password, then click **OK**
5. Go to **Action | Change Password** on the main menu, or right-click on the Sentinel Server and choose 'Change Password' from the pop-up menu that is displayed to open the Connect to dialog
6. Type the name of the user, the user's new password and the confirmation of the new password into the Connect to dialog
7. Click **OK** to close the dialog

Hint: If you do not want to use a password, simply do not enter a new password into the Connect to dialog, and click **OK**. However, this is not recommended.

Remembering your Password

Sentinel Management enables you to save the password required to connect to a particular Sentinel Server, for your current session using Sentinel Management.

To remember a password:

1. Start Sentinel Management
2. Select the Sentinel Server from the servers list that you wish to connect to
3. Click on the **Connect** button if necessary
4. If the Connect to dialog appears, enter your user name and password
5. Check the 'Remember Password' checkbox
6. Click **OK** to close the dialog. Sentinel Management will remember your password for that server until the end of your session.

Using Sentinel Log Files in Analyzer

WebSpy Sentinel 3.2 divides the Internet traffic that it captures into two separate capture log files. One file contains the hits captured while the other contains the content of all protocols accessed. This means that you import both log files into *WebSpy Analyzer* to see all of the traffic that *Sentinel* has captured. The location of these log files is described in the Log Files view on page 15 and the names of these log files are described in Table 1.

Table 1 - Sentinel Log File Names

	Log File Name
Hits	YYYYMMDD.log
Content	YYYYMMDD.dat

Before attempting to import a Sentinel log file into *Analyzer*, you must ensure that you have enough free space on your hard disk to fit in the entire Sentinel log file.

Once you have imported the log files into *Analyzer*, you will be able to view the content that *Sentinel* captured by drilling down to the 'Individual Hits' level in **Summaries**.

For more information, please see *WebSpy Analyzer's* Manual or Help Files.

Definitions

Domain Controller

A domain controller is the computer that logs users on to domain accounts in a Windows NT® Server domain. The primary domain controller keeps track of any changes to the domain accounts, and will log users on to domain accounts. By default, *Sentinel* uses the primary domain controller to resolve user names. A backup domain controller is kept up to date with changes by the primary domain controller, and can be used to provide the information *Sentinel* needs, if the primary domain controller is not available.

LAN

A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building). Usually, the server has applications and data storage that are shared in common by multiple computer users. A local area network may serve as few as two or three users (for example, in a home network) or many thousands of users (for example, in a large corporation).

Mail

For *WebSpy Sentinel's* purposes, this is Internet traffic received via SMTP (Simple Mail Transfer Protocol). POP3 and IMAP protocols are not captured. SMTP is a TCP/IP protocol used in sending and receiving e-mail. POP3 or IMAP are protocols that let the user save messages in a server mailbox and download them periodically from the server. Users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving messages that have been stored for them at their local server.

Newsgroups

A newsgroup is a discussion about a particular subject consisting of e-mails or notes written to a central Internet site and redistributed through Usenet, a worldwide network of news discussion groups. The protocol used is Network News Transfer Protocol (NNTP).

Packet

A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file (e-mail message, HTML file, GIF file, URL request, and so forth) is sent from one place to another on the Internet, the file is divided into "chunks" or packets of a suitable size for efficient routing. Each of these packets is separately numbered and includes the Internet address of the destination.

Protocol

A protocol is a special set of rules or conventions for communication between two computers, both of which must recognize and observe the protocol. Different types of Internet traffic use different protocols. Protocols are often described in an industry or international standard.

Telnet

Telnet enables you to access another computer across the Internet, assuming they have given you permission. Such a computer is known as a 'host' computer. With Telnet, you log on as a regular user with whatever privileges you may have been granted to the specific application on that computer.

Web

For *WebSpy Sentinel's* purposes, this is any Internet traffic received via HTTP (Hypertext Transfer Protocol). HTTP is the set of rules for exchanging files (text, graphics, and other multimedia files) on the World Wide Web (WWW).

Contact WebSpy

WebSpy North America

(Servicing North and South America)

Columbia Center
701 5th Ave, Suite 4200
Seattle, Washington 98104

Toll free: 888-862-4403
Phone: +1 206-575-7763
Fax: +1 206-575-7809
Email: sales@webspy.com

WebSpy Europe

(Servicing Europe, Middle East and Africa)

3rd Floor, Unit 19
Angel Gate
326 City Road
London, EC1V 2PT

Phone: +44 (0) 207 239 7500
Fax: +44 (0) 207 239 7539
Email: europesales@webspy.com

WebSpy Australia

(Servicing Australia, Asia and the Pacific)

Level 3
9 Colin Street
West Perth, Western Australia 6005

Toll Free: 1800 801 121
Phone: +61 8 9321 3322
Fax: +61 8 9321 3377
Email: sales@webspy.com.au

WebSpy Support

To contact WebSpy Support, please visit our support page at http://www.webspy.com.au/contact/support.aspx