WebSpy Product Integration Guide

This document illustrates how WebSpy products work together to provide a complete Internet monitoring solution.

The information and procedures described in this guide apply to the following product versions:

- *WebSpy Analyzer Standard 4.0*
- *WebSpy Analyzer Premium 4.0*
- *WebSpy Analyzer Giga 2.0*
- *WebSpy Sentinel 3.2*
- *WebSpy Live 2.0*

Table of Contents

Introduction

Sentinel, *Analyzer Standard, Analyzer Premium, Analyzer Giga* and *Live* work together to provide a complete Internet monitoring solution. *Sentinel* captures your Internet web, mail, telnet, FTP and news traffic, *Analyzer* products create useful summaries and comprehensive reports using *Sentinel* log files, while *Live* monitors *Sentinel's* log files in real time to alert on unacceptable browsing. Unlike most Internet monitoring applications or proxy server software, *Sentinel* can actually capture and store all the web, mail, telnet, ftp and news resources downloaded by each user, and *Analyzer* enables you to view this content captured by *Sentinel*.

Getting Help

This guide is intended to help you start using *Sentinel*, *Analyzer Standard, Analyzer Premium*, *Analyzer Giga* and *Live* together as a complete monitoring solution.

If you require more information on using *Sentinel*, please consult the Sentinel 3.2 Getting Started Guide or Planning and Installation Guide. You can also access Sentinel Management's help by selecting **Help | WebSpy Sentinel Help** from the management console.

For more information about using *Analyzer Standard*, *Analyzer Premium*, *Analyzer Giga* or *Live*, see their respective getting started guides or help. Context sensitive help is available for each product by pressing F1 to launch the help window

Resources:

- For all product documentation: http://www.webspy.com/downloads/manuals.asp
- FAQs, useful hints and tips: http://www.webspy.com
- For WebSpy Support, contact support@webspy.com or go to http://www.webspy.com/contact/support.asp.

Using Sentinel Log Files In Analyzer and Live

Sentinel's log files are similar to other types of proxy server or firewall log files, with the extended ability to capture the actual content of the items accessed over the Internet. Each Sentinel Server that you set up can store data files of the content it captures. You can find the location of each server's log files by accessing the Data Logs view for each server in Sentinel Management. The location listed in the Data Logs view is local to that Sentinel Server.

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 the Sentinel Service (Windows NT® and Windows® 2000) 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.

You can import Sentinel log files *into Analyzer Standard*, *Premium* or *Giga*. There are some things you will need to consider if you choose to import content into *Analyzer* – see Importing Content into Analyzer on page 4 for more information.

Sentinel logs can also be used in with *Live* for real-time Internet monitoring. Unlike some third-party proxy log files, these logs can be immediately read by *Live*, so you will always be up to date with what your network users are doing. See Monitoring Sentinel Log Files with Live on page 7.

Capturing Content Using *Sentinel*

Sentinel logs the details of all Internet resources accessed by users on your network. The log information includes:

- The date and time the resource was accessed
- The name of the user that accessed it (assuming that your network software enables this)
- The URL of the resource, or the subject of the message
- The size of the resource, and
- How long the resource took to download.

Sentinel can also capture and store each individual resource downloaded. So, instead of just knowing that one of your users sent an email at 11:30 am to a friend, you can read the body of that email and view any attachments as well.

You can change your content capture settings on a server-by-server basis. So, if you have more than one computer running *Sentinel* Service, you can set the services to capture different content. Content capture settings can be changed from the Protocols view of *Sentinel Management*. See *Sentinel*'s Help for more information.

Note:
Sentinel does not log failed web hits. Failed hits are requests that failed to generate a successful response. This might happen if the user spelt the URL incorrectly, or the page was no longer available, or the proxy server (on either end) was unable to fulfill the request.

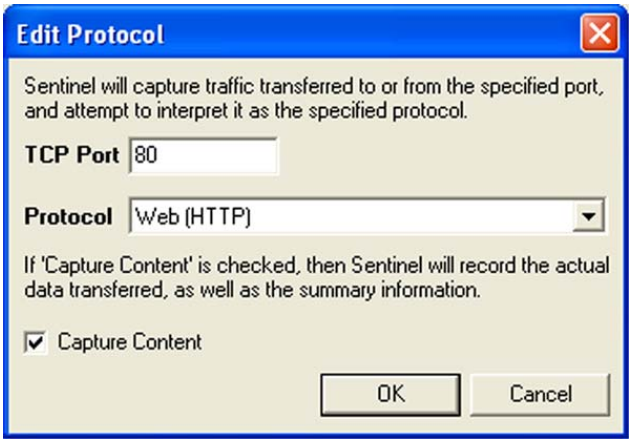

Figure 1: Capturing Web Content in Sentinel

Capturing Mail (SMTP) Content

Since the body of email messages cannot reliably be captured by any other means, it is suggested that you choose to capture mail content. Even if your mail server stores your users' email messages, each user can delete their own messages.

Capturing News (NNTP) Content

Most news messages are quite adequately described by their site and subject name, however if you wish you can choose to capture news content as well.

Capturing Web (HTTP) Content

Capturing web content is not recommended in standard installations, for two reasons. Firstly, it does not supply you with information you cannot easily obtain from another source, such as the web sites themselves. Analyzer enables you to browse to a site using *Analyzer Standard*, *Premium* or *Giga* (see Web Previews on page 6). Secondly, capturing all web content may have a detrimental effect on the performance of the computer running Sentinel Service, due to the sheer volume of web traffic each day.

If you are concerned about the web usage of a particular user, you could install Sentinel Service onto that user's computer to capture full web content for that user. As comparatively little traffic is generated by a single user, this will provide you with content capture without affecting the performance of that computer.

Capturing Remote Login (Telnet) Content

Telnet enables you to use another computer across the Internet. Some uses for telnet are to play Internet games, check private email, or perform administration tasks. Users can run and use any application available to them on the remote computer they have logged in to.

If your organization's users have unrestricted telnet access, telnet content may be worth capturing. However, the content of these telnet sessions may not be clear and easy to follow.

Capturing File Transfer Protocol (FTP) Content

FTP is a communications protocol, which controls the transfer of files from one computer to another over a network. *Sentinel* enables you to capture information on FTP sessions such as the date, time, user and names of files accessed.

Sentinel will not capture the actual content of any files transferred and like Telnet sessions the data captured from FTP sessions may not be clear and easy to follow.

Importing Content into *Analyzer*

When importing *Sentinel* log files with content into *Analyzer Standard* or *Premium*, there are two issues to be aware of:

1 The size of the log files
2 The time they will take to load

Analyzer Standard and *Premium* are able to load up to 2GB of log file data. *Analyzer Giga* can import an unlimited amount of log file data. The more data you import, the longer Analyzer will take to perform certain tasks such as creating reports, and performing drilldowns.

Importing content takes longer than importing normal log file information. For this reason, loading content can noticeably slow the importing process. You can create scheduled tasks for *Analyzer* to import data at a convenient time such as overnight or on the weekend.

Hint:
You don't need to import every protocol *Sentinel* captured at once. You can filter your log files and only import the protocols you are interested in. For example, you could import web and news log information, but only mail content.

Once *Analyzer* has imported your *Sentinel* log files, it stores the hits, contents and information used to generate content previews in *Analyzer*'s Temp folder. Therefore, you will need sufficient available disk space for all of this data. All of the files in this folder are cleared when you exit *Analyzer*.

To import content for *WebSpy Sentinel* log files:

1 Open Analyzer and select **Views | Storages** from the main menu, or click the Storages Sidebar icon.
2 Start a new storage by clicking the **Start a new storage** link on the Management task pad.
3 Once a new storage has been created click the **Import log files** link on the Files task pad. This launches the Import Wizard
4 On the Import Format page, ensure 'WebSpy' is selected as your log file format, and click the **Format Properties** button on the toolbar.
5 Check the Import Content checkbox on the WebSpy Properties dialog and click **OK**.
6 Click **Next** and progress through the remaining pages of the Wizard, ensuring you select your Sentinel log files on the Input Location page.

If you want to import the log files at a later time, uncheck the 'Import hits from selected files or folders' checkbox on the final page of the Import Wizard. You can then create a Task to import hits into this storage at a more convenient time such as overnight or on a weekend (see Creating a Task to Import Sentinel Log Files with content on page 5).

Note:
Sentinel creates .log and .dat files. You will only need to import the .log file into *Analyzer*.

Creating a Task to Import Sentinel Log Files with content

As importing content can slow the importing process, you may want to set a task for the importing to run at a convenient time such as over night or on a weekend.

To create a task:

1 Follow the steps on page 4 for importing content into Analyzer, and ensure the 'Import hits from selected files or folders' checkbox on the final page of the Import Wizard is NOT checked.
2 Select Views | Tasks from the main menu, or click the Tasks Sidebar icon.
3 Click the Add new task link in the Tasks task pad. This launches the Task Wizard.
4 Proceed through the Task Wizard making the appropriate selections. Ensure that on the Storages page of the wizard, the storage that you want to import data into is selected (Note: this does not apply in Analyzer Standard as only one storage can be open at a time).
5 Proceed through the remaining pages of the Wizard and click **Finish** on the final page.

Note:
The Task Wizard ensures that you also include a report as part of the task. If you do not want to create a report, you can edit the task and delete the report on the Reports tab of the **Task Properties** dialog.

Displaying Content using *Analyzer*

You can display mail, web, news, telnet and FTP content in *Analyzer*'s content preview panel in Summaries.

WARNING:
Analyzer will display the content that *Sentinel* captured exactly as it is. This may mean that offensive material may be displayed.

To view content in *Analyzer*:

1 Make sure you are in Summaries by selecting **Views | Summaries** from the main menu or clicking the **Summaries** Sidebar icon
2 Drill down to the information you wish to display (such as the sites a user has visited)
3 Group the information by Individual Hits by choosing 'Individual Hits' from the Location bar
4 Select the hit that you want to view
5 *Analyzer* will display the content of that hit in the content preview panel at the bottom of the view

Note:
If no content was captured, that will be noted in the content preview panel.

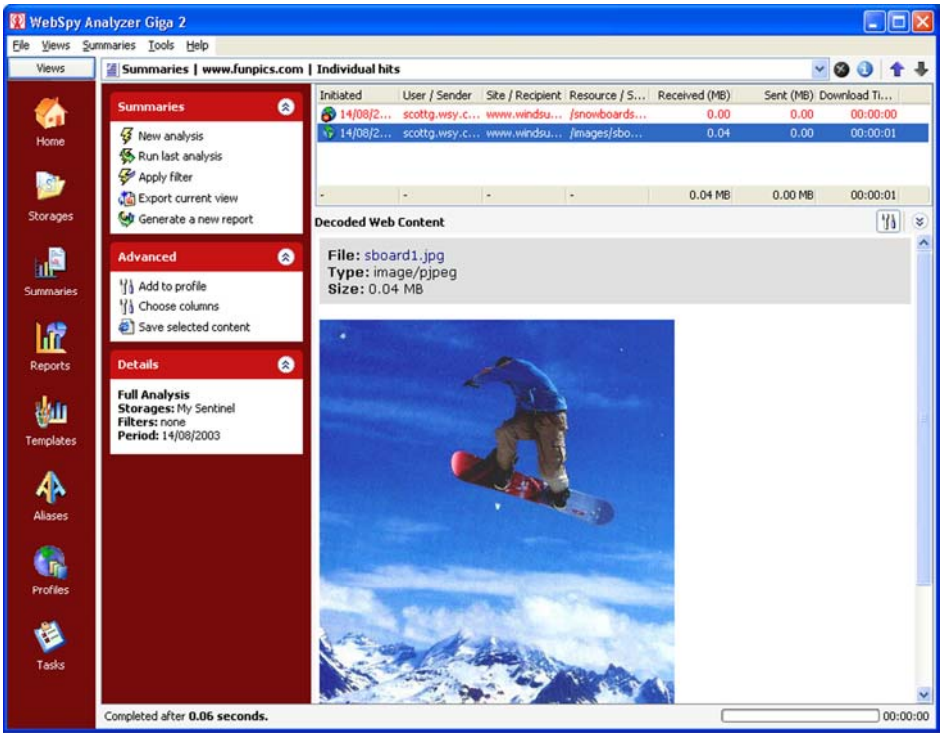

Figure 2: Displaying captured content in Analyzer Giga

Email Previews

The email preview will show you an outline of the email *Sentinel* captured, including the To: and Cc: addressees, subject, message body and any attachments.

You can send emails to the sender or any of the listed recipients, and open or save any attachments.

To open an attachment, click on the attachment's name in the header of the email in the content preview pane. The attachment will be opened by your default browser, if your browser supports the attachment type.

To send email to a sender or recipient, click on the address in the header of the email in the content preview pane. Your default mail program will launch a new message addressed to that person.

Web Previews

The web preview will show you the resource that *Sentinel* captured. Since web pages are often made up of lots of very small parts, like small pictures or pieces of text, the preview may or may not be useful. You may also find that *Analyzer Standard* and *Premium* cannot display resources that your default Internet browser does not support. In this situation, your default browser's standard Open/Save dialog will be launched.

To view the web resources that a user accessed, you can simply right-click on any URL or site name listed in *Analyzer*'s Summaries, and choose 'Browse:' from

the pop-up menu that is displayed. The URL or site will be launched in your default web browser. Note that your computer will need an active Internet connection to view the site.

Telnet Previews

The telnet preview is a direct copy of the information exchanged between the user's computer and the remote computer.

News Previews

The news preview will show you the news item that *Sentinel* captured, including the sender of the item, the subject and the message body. From Individual Hits, you can right-click on any news item and select 'Browse:' from the pop-up menu to open the news item using your default news browser.

Saving Content using *Analyzer*

If necessary, you can save any of the content displayed in *Analyzer Standard* and *Premium* to another location. For example, you may wish to print an email containing offensive content to show the sender, or, if a mail message cannot be displayed, you could open it in a text editor to view the message body.

Remember, though, that all of this content is already stored in the *Sentinel* log file, so there is no need to save content that you have no direct use for.

To save content from *Analyzer*:

1 Make sure you are in Summaries by selecting **Views | Summaries** from the main menu or clicking the **Summaries** sidebar icon
2 Drill down to the information you wish to display
3 Group the information by Individual Hits by choosing 'Individual Hits' from the Location bar
4 Select the hit with the content that you want to save
5 Right-click the hit, and choose **Save...** from the pop-up menu that is displayed
6 *Analyzer* will open a 'Save as' dialog for you to choose the location to save the content to

To save an email attachment, right-click on the name of the attachment in the email preview and select 'Save Target as' from the pop-up menu that appears. A Save dialog will be displayed for you to choose where to save the attachment.

Monitoring Sentinel Log Files with *Live*

You can use WebSpy Live to monitor Sentinel Log files in real-time and generate alerts when certain browsing conditions are breached.

To monitor Sentinel log files:

1 Open *Live's c*onfiguration dialog by right-clicking the *Live* system tray icon and select **Configuration** from the pop-up menu.

2 Go to Inputs by selecting **Views | Inputs** from the main menu or clicking the Inputs Sidebar icon
3 Click the **Add new input** link in the Inputs task pad. This launches the Input Wizard.
4 Proceed to the Folder page of the Input Wizard. Enter the location path where your Sentinel log files are stored. This is the 'Data Folder' location specified on the Data logs\User Filters view in WebSpy Sentinel.
5 Select *.log in the File Mask drop down list
6 Select 'WebSpy' from the Formats dropdown list.
7 Click **Next** to proceed to the Advanced Settings page. WebSpy recommends that you check logs every 1 second and ignore all log file format issues. Make these selections and click **Next**.
8 Proceed through the remaining pages of the Wizard. On the Final Page, ensure the 'Input is enabled' checkbox is checked. Click **Finish**.

Live will start monitoring your Sentinel log files. Active users and alerts will be displayed in Live Status as your log files are updated.

Synchronizing Aliases between *Analyzer* and *Live*

If you are running *WebSpy Live* and *WebSpy Analyzer*, you can synchronize your alias and profiles, so that changes made in one WebSpy application are also made in the other.

To synchronize you profiles and aliases:

1 Open *Live's* Options dialog by right-clicking the Live system tray icon and select **Options** from the pop-up menu.
2 On the General Tab of the dialog, ensure the 'Keep Profiles and Aliases synchronized between WebSpy applications' checkbox is checked.
3 Open WebSpy Analyzer's Options dialog by select **Tools | Options** from the main menu.
4 On the General Tab of the dialog, ensure the 'Keep Profiles and Aliases synchronized between WebSpy applications' checkbox is checked.

More Information

If you would like more information on using any of the WebSpy products visit our website at http://www.webspy.com or contact WebSpy Support at support@webspy.com.