WebSpy Live 2.2
Getting Started Guide

This document is intended to help you get started using *WebSpy Live 2.2*. For more detailed information, please see the *Live* user guide or online help.

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

Copyright WebSpy Ltd. 2007

© WebSpy Ltd. 2001 - 2007

All rights reserved. No part of this document may be photocopied, reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical or otherwise, without the prior written permission of WebSpy Ltd.

No warranty of accuracy is given concerning the contents of the information contained in this publication. To the extent permitted by law no liability (including liability to any person by reason of negligence) will be accepted by WebSpy Ltd, its subsidiaries or employees for any direct or indirect loss or damage caused by omissions from or inaccuracies in this document.

WebSpy Ltd. reserves the right to change details in this publication without notice.

Windows is a trademark and Microsoft, MS-DOS, and Windows NT are registered trademarks of Microsoft Corporation. Other product and company names herein may be the trademarks of their respective owners.

Overview of *Live*

WebSpy Live monitors your proxy server or firewall's current log files to provide a real-time picture of what people using your network are doing. *Live* enables you to:

- Find out as soon as unacceptable Internet or email activity occurs
- Configure the types of activity you want to be alerted to
- Identify the users that are browsing at any time
- Discover users who spend too long browsing, while they are still browsing
- Identify users that are downloading or sending large or unacceptable files
- Find out what your users are doing and the sites they are visiting
- Attend to Internet and email misuse when it happens

You can configure *Live* so that an alert is generated whenever one of your users browses in a way that you consider inappropriate. You can specify exactly what is inappropriate for your organization using as many triggers as necessary. See Adding Triggers on page 7.

There are three main parts to *Live*:

- **Live Status**
  Live Status is a small, unobtrusive dialog that lists all current alerts, as well as all active and idle users of your network. You can access Live Status by clicking the Live icon in your system tray. It is the dialog you use most frequently to monitor your network and Internet traffic.
- **Live Configuration**
  Live Configuration is where you configure the way *Live* behaves and operates. Using this dialog, you can choose which proxy logs to monitor, when to produce alerts, configure profiles to categorize types of browsing, and define aliases to represent information more meaningfully.
- **Live Summary**
  Live Summary collates information about the Internet activity of all users being monitored. Using Live Summary, you can browse all network activity categorized by user and user sessions.

Your Internet Gateway or Proxy Server creates log files that contain information about Internet and network traffic (hits). *Live* monitors these log and imports new hits. If these hits match any of your configured triggers, an alert is raised and displayed in Live Status. *Live* supports over 60 log formats, however if you use a format that is not supported, please contact support@webspy.com.

Information captured by *Live* is kept for 24 hours before it is deleted. You can change this time in **Tools | Options | General**, by specifying a different figure for the 'Purge data older than' option. *Live* displays this information even if you close and reopen the application.

When you open *Live,* your log files are checked for new browsing since *Live* was shut down. It may take a short while for *Live* to catch up to the present time, depending on how long ago *Live* was shut down, and the amount of browsing that has occurred since

New in Live 2.2

- ***Windows® Vista Support***
  Installs and runs on Microsoft® Windows Vista.

- ***Purge data older than today***
  New purge option in Tools | Options | General ensures only information for today is shown in Live.
- ***Port Triggers***
  Ports is now an option in Single Hit Triggers. You now be alerted when hits made on a certain Source and/or Destination Port, or for a range of Ports.
- ***Keyword Triggers***
  Keywords is now an option in Single Hit Triggers. You can now be alerted when specific keywords occur at any point in a URL, including the query string where search terms are recorded. (Triggers based Profiles only use site name and resource).
- ***Time Range Triggers***
  There is a new trigger type that allows you to specify a sliding time window (e.g. 10 minutes) or a fixed time window (e.g. 12:00pm to 1:00pm), in combination with all the criteria available in Single Hit Triggers (Size, User names, Site names, File types, Departments, Profiles, Protocols, Keywords, Ports). Sliding window triggers also provide the ability to specify a hit count (e.g alert me when there are 5000 hits within 2 minutes)

Before you start...

WebSpy Live can be installed on any computer on your network that is running Windows® 2000 or above, with at least 256 MB of RAM and a 1 GHz or faster processor. Naturally, the more users you have, and the more active they are, the more memory and CPU resources *Live* will use.

If your proxy server or firewall's log files are stored on a network drive, the user of *Live* must have permission to access them and will need to know the format of these log files. If you don't know the format, send a sample of the log file to WebSpy Support (support@webspy.com).

Installing and Uninstalling Live

If you downloaded *WebSpy Live* from the WebSpy web site, double-click the downloaded zip file, and extract its contents to a location on your hard drive (you will need WinZip to open the zip file, which can be downloaded from www.winzip.com). Then run Live21.exe and follow the onscreen instructions to install *Live*.

If you are installing *Live* from a WebSpy CD, insert the CD into your computer's CD drive and follow the onscreen instructions.

To uninstall *Live* use Add/Remove Programs in your computer's Control Panel. You also need to delete any folders remaining in the location where *Live* was installed.

Upgrading from Live 2.1

The installation process will install *Live 2.2* to a different folder to *Live 2.1*; therefore you can run both *Live 2.1* and *Live 2.2* at the same time.

When you run Live 2.2 it will detect that another version of Live is installed and ask you if you want to upgrade your files for use in Live 2.2. The upgrade will not delete your old files. It will simply copy them to the new locations for Live 2.2.

All Live 2.1 files such as aliases, profiles and triggers are compatible with Live 2.2.

Getting Started

The first time you open *Live*, Live Configuration and Live Status is displayed. A black alert flashes in Live Status indicating there is an input issue because no inputs are yet configured.

Follow these steps to start using *Live*:

1. Add your inputs. This step configures *Live* to monitor the location that contains your log files (see Adding Inputs on page 5).
2. Click the *Live* icon in your system tray to display Live Status. Active and idle users are displayed in Live Status along with any alerts that are triggered.
3. When an alert is triggered, double-click the alert to view its details in the Alert Details dialog. Use the buttons on the Alert Details dialog to dismiss the alert or email its details to a user (see Using Triggers, Alerts and Live Status on page 6).
4. Use Live Summary to get an overview of the Internet and email activity of all users (see Using Live Summary on page 7).

To use *Live* more effectively, you can:

- Create new triggers to alert you to specific Internet or network usage (see Adding Triggers on page 7)
- Create and refine aliases to represent users, site names, file extensions, and departments (see About Aliases on page 8)
- Create and refine profiles to categorize Internet and network activity more effectively (see About Profiles on page 8)
- Customize *Live* Options to change the way *Live* behaves, how data is displayed and where it is saved

Adding Inputs

Live uses inputs to import data from your log files. When creating inputs, you can specify folders of log files that you want to monitor, and define filters to prevent certain information from being monitored.

To add an input:

1. Open Live Configuration by right-clicking the Live icon in your computer's system tray and selecting 'Configuration' from the menu.
2. Open Inputs by clicking the **Inputs** Sidebar icon or selecting **Views | Inputs** from the main menu.
3. Click the **Add new input** link in the Inputs task pad to launch the Input Wizard. This wizard guides you through the process of choosing the location of the log files you want to monitor, and their format.

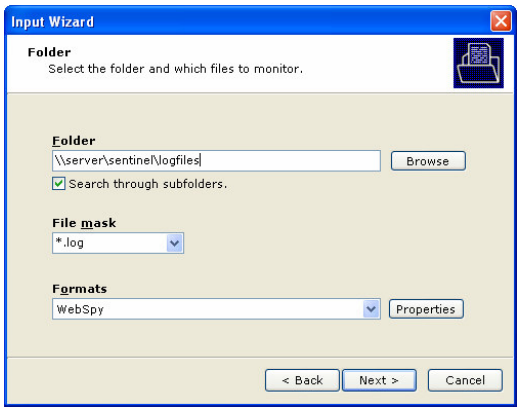


Figure 1: Folder page of the Input Wizard

For more information on adding inputs, please see the online help or user guide.

Using Triggers, Alerts and Live Status

Triggers enable you to set up scenarios that you want to be alerted to, such as users visiting unacceptable web sites, or downloading large files. Triggers can be based on a variety of conditions, such as the types of web sites visited, the length of time users have been browsing, and the size and type of downloaded resources.

WebSpy Live comes with a list of default triggers for common monitoring requirements; however you also can add your own custom triggers (see Adding Triggers on page 7).

When conditions the specified in a trigger are breached, an alert is raised. These alerts are displayed in your computer's system tray, and in Live Status (see Figure 2).

You can assign a priority to each trigger, and depending on this priority level, a different colored alert is displayed in Live Status.

Black alert - input issue

Green alert - low priority

Yellow alert - medium priority

Red alert - high priority

Figure 2: Live Status dialog

You can double-click to launch the Alert Details dialog (see Figure 3) which displays the details of the activity that triggered the alert. You can then act on the alert immediately by sending an email, or dismissing the alert using the buttons on the toolbar.

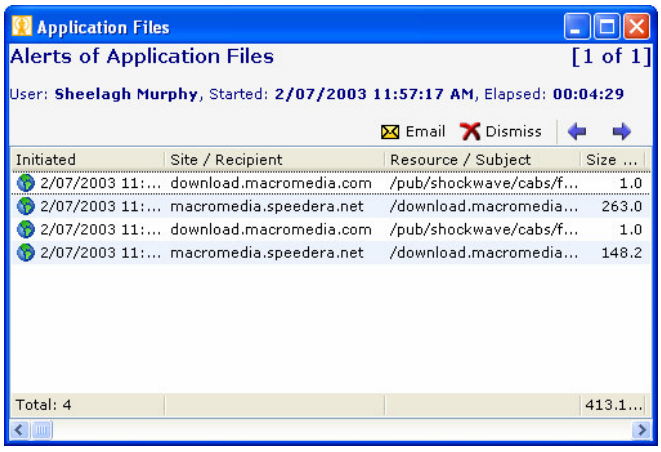


Figure 3: Alert Details dialog

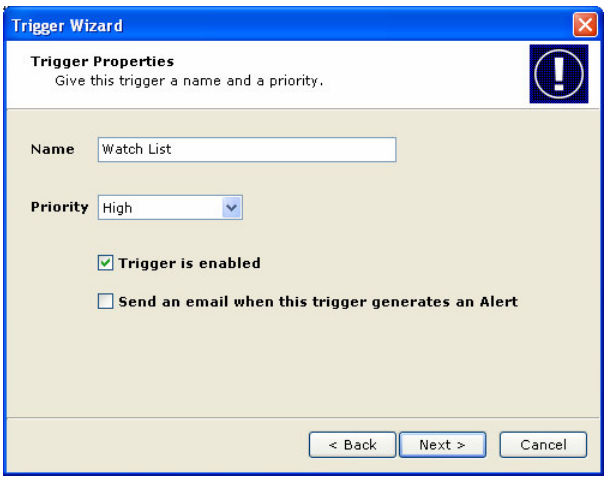
You can also open any listed sites in your default Internet browser by right-clicking on the site's name and selecting **Browse to:** from the pop-up menu.

In addition to alerts, Live Status also displays all active and idle users. You can double-click an active or idle user to view the details of their activity.

Adding Triggers

WebSpy Live comes with a list of common triggers, such as 'Unacceptable Content' and 'Large Downloads', however you may want to set up your own custom triggers.

The Trigger Wizard guides you through the process of setting up triggers to alert you to specific types of Internet and network activity.



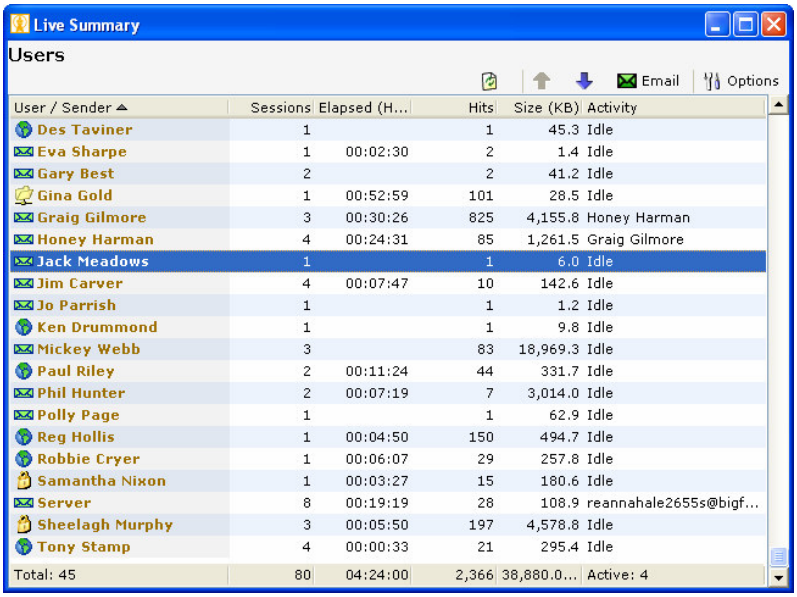
To launch the Trigger Wizard:

1. Open Live Configuration by right-clicking the Live icon in your computer's system tray and selecting **Configuration** from the popup menu
2. Open Triggers by selecting **Views | Triggers** from the main menu, or clicking the Triggers Sidebar icon
3. Click the **Add new trigger** link in the Triggers task pad. This launches the Trigger Wizard that guides you through the process of configuring the trigger.

Figure 4: Trigger Wizard - Trigger Properties Page

For more information on defining triggers, please see the online help or user guide.

Using Live Summary



To get an overall picture of what users in your organization are browsing, you can use Live Summary. Live Summary lists all users of your Internet and email resources.

You can click an individual user, to view a list of the user's sessions. You can then click on any of these sessions to view the user's activity during that session. You can also launch an email to any user using the **Email** button on the toolbar.

To launch Live Summary, click the **Summary** Button at the top of Live Status.

Figure 5: Live Summary

About Profiles

Profiles use keywords to categorize the types of sites and resources users have accessed. For example, you can use 'shop' as a keyword to find out whether a web site or resource is related to shopping or not.

Triggers can be configured to raise an alert when a user accesses content that belongs to a certain profile. For example, you can set up a trigger that generates alerts when users access material belonging to the Adult profile.

Live comes with several profiles already defined, with common keywords. You can also create your own custom profiles to suit your organization.

For information on creating your own profiles, please see the online help or user guide.

About Aliases

WebSpy Live uses Aliases to define alternative names for data items or groups of data items. They are used to represent raw data items with understandable names, and group common information in your log files into one representative name.

For example, you can group the file types 'mpg', 'avi', and 'mov', into a file type alias called 'Video Clips'. You can also represent an IP address such as 192.168.0.15 by a user name alias like 'John'. Aliases also enable you to group a range of IP addresses and user names into a department alias called 'Marketing' or 'Accounts'.

There are four types of Aliases:

- **User names**
  User name aliases enable you to represent IP addresses, email addresses and computer names, by an actual user name such as 'John Citizen'. This user name is then used to represent all the Internet and network activity of this user in Live Status and Live Summary. You can also use user names when defining triggers to alert you when a particular user is active, or browses inappropriately.
- **Site names**
  Site names enable you to represent IP addresses and URLs, such as 'http://www.webspy.com', by simplified site names, such as 'WebSpy'. Site names can then be used when defining triggers based to alert you when users browse to specific sites.
- **File types**
  File types enable you to group file extensions, such as 'htm', 'xml', 'css', into a representative name, such as 'Web Document'. File types can then be used when defining triggers to alert you when specific types of files are being downloaded or sent.
- **Departments**
  Users of your Internet and email resources can be grouped into departments such as 'Accounts', or 'Management'. You can filter your inputs by departments to prevent Live from monitoring particular groups of users. You can also use departments when defining triggers to alert you when a member of a department is active, or browses inappropriately.

Live comes with a list of default file type aliases, however you can create your own custom user names, site names, file types and departments suit your

organization. For information on adding Aliases, see the online help or user guide.

Contact Information

If you would like further assistance with any WebSpy product, you can email your query to support@webspy.com. If you have any comments or suggestions, please feel free to send them to suggestions@webspy.com.

For sales information, please contact the WebSpy Ltd. office in your region:

- Australia: sales@webspy.com.au
- Europe: europesales@webspy.com
- USA: sales@webspy.com