



WebSpy Live 1.0

Getting Started Guide

The aim of this document is to provide you with a broad understanding of *WebSpy Live* and enable you to 'get started'. *Live* has lots of useful functionality that is not outlined in this document. To fully understand the power of the application, please use the online help.

You can press F1 at any time to open the most relevant help topic for the task you are performing.



Overview of *Live*

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

- See who is browsing at any moment
- Find out as soon as unacceptable browsing occurs
- Identify any users who spend too long browsing, while they are still browsing
- Discover what your users are doing and what sites they are visiting

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 About Alerts, Triggers, Profiles and Sessions on page 3.

There are three main parts to *Live*:

Live Status – an unobtrusive list where you can see which alerts have been generated, and which of your users are currently browsing. You can select any alert or user to see a summary of the behavior that generated the alert.

Live Summary – an overview window where you can see what each of your users is currently doing, and has been doing for the time *Live* has been monitoring

Live Configuration – a configuration window where you can choose which proxy logs to monitor, and when to produce alerts

Live will keep details of all your users' browsing sessions, including the sites that were visited, until you shut down *Live* or your computer, or until you reset *Live* to clear your accumulated summaries.

Live can be installed on any computer on your network.

Before you start...

WebSpy *Live* can be installed on any computer on your network that is running Windows® 95, 98, ME, NT or 2000. *Live* runs best on a computer using Windows® 2000 with at least 64 MB of RAM and a 200 MHz or faster processor. Naturally, the more users you have, and the more active they are, the more memory and CPU resources *Live* will take up.

Your proxy server needs to support Windows networking, and your computer needs to be set at the same date and time as your proxy server e.g. both at 9:06 am. 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).

A list of supported log files is included at the end of this document.



Installing and Uninstalling Live

To install *WebSpy Live 1.0*, simply double-click the file you downloaded, or insert your *Live CD* into your computer's CD drive.

You can uninstall *WebSpy Live* using Add/Remove Programs in your computer's Control Panel. Then, you will need to delete any folders remaining in the location you originally installed *Live*.

Adding Inputs

An input is a folder of log files that you want to monitor. For example, you may choose the folder that stores your proxy server's log files as one of your inputs.

To add an input, you will need to open Live Configuration, by right-clicking on the Live icon in your computer's system tray (next to the clock) and selecting 'Configuration' from the menu. Then, open Inputs by clicking on the **Inputs** sidebar icon or selecting **Views | Inputs** from the main menu. Click on the **Add** button to launch the Input Wizard. You will need to choose the location of the log files you want to monitor, and their format.

WebSpy Live enables you to specify a file mask for your inputs. File masks are similar to file extensions, except they can include characters before the dot. For example, 'a*.log' is a file mask that will match any log files with names starting with 'a' and ending with '.log'.

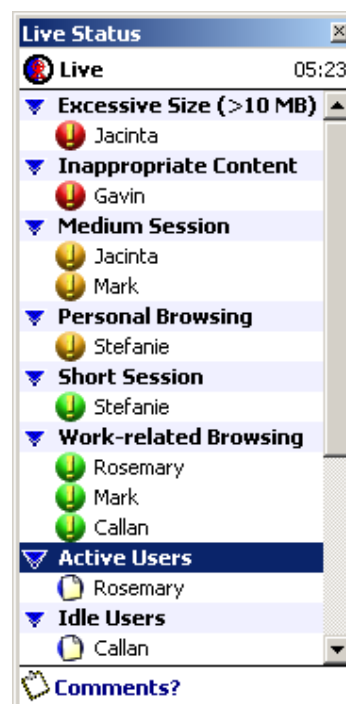
If your proxy server provides more than one type of log file, or if you have other types of files stored in your proxy log file folder, you can use an appropriate file mask to make sure *Live* only monitors the correct files. For example, if you use Microsoft® Proxy Server, you might use W3*.log as your file mask, to only monitor the web logs with the most complete information.

Monitoring Users and Alerts

All active alerts and users are displayed in Live Status. You can double-click on any alert to see the details of the activity that triggered the alert in a Details dialog. Then, you can choose to act on that alert by sending an email, or to dismiss the alert. You can dismiss an alert from Live Status by right-clicking on the alert and selecting 'Dismiss' from the pop-up menu.

From a 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. You can even reassign the site to a different profile, if you wish.

If you want to contact a user about their browsing, you can click on the **Email** button on the Details dialog, and *WebSpy Live* will launch a new email containing the activity details displayed in the Details dialog. You can then edit the email if necessary, and send it to the user.





If you double-click on an active or idle user, you can see the current browsing session for that user, and what sites they browsed in it.

To get a better overall picture of what users in your organization are browsing, you can open Live Summary from the Live menu at the top of Live Status. It lists the number of sessions, total number of hits, total size downloaded and current browsing activity for each user. If you click on an individual user, you can drill-down to see more detailed information about that user's sessions.

If you don't want Live Status showing all the time, you can close it, and watch the *WebSpy Live* icon in your system tray. It will change to a different colored, flashing icon whenever you have new alerts.

About Alerts, Triggers, Profiles and Sessions

WebSpy Live produces an alert when someone browses the Internet inappropriately. You can specify inappropriate browsing conditions in a trigger. When a trigger is breached, *Live* will display the alert in the Status List.

The Trigger Wizard enables you to set up specific triggers based on:

- Profile
- Size
- File extension
- Time

A profile trigger is based on the content of the material, a size trigger is based on the size of the items downloaded, an extension trigger is based on the type of file downloaded and a time trigger is based on the time a user spent browsing.

A profile trigger generates an alert if someone accesses content that belongs to one of the profiles specified in the trigger. For example, you could set up a profile trigger that will generate an alert if a user accesses material belonging to the Adult profile.

Profiles use keywords to classify the kinds of resources accessed. For example, you can use 'shop' as a keyword to find out whether a website is related to shopping or not. *Live* comes with a set of 11 basic profiles.

A size trigger will generate an alert if someone downloads a single resource larger than the size you specified. For example, you might want to be notified if someone downloads an item larger than 10MB. You can also have combined size triggers that raise alerts if someone downloads more than the specified size during the time *Live* is running.

An extension trigger will generate an alert if someone downloads a file with a particular extension. For example, if you set '.mp3' as one of the file extensions in the trigger, you would be notified if any of your users downloaded mp3 music files.

A time trigger generates an alert if someone's session time is greater than the time specified in the trigger. For example, you could set up a trigger that will alert you if a user spends half an hour browsing. You can also have combined time triggers that raise alerts if someone browses over a number of sessions for longer than the time specified, during the time *Live* is running.



A session is the period of time that one user spent using the Internet, for example browsing the web. If a user downloads two or more Internet resources within a set threshold time, then *Live* groups those resources as part of a user session. You can customize the threshold time via Live Options.

You can edit or add new triggers for *Live* to use, with the Trigger Wizard. To add a trigger, you will need to open Live Configuration, and open Triggers by clicking on the **Triggers** sidebar icon or selecting **Views | Triggers** from the main menu. Then, click on the **Add** button to launch the Trigger Wizard.

Bright Ideas...

Aliases transform cryptic network names or IP addresses into the users' actual names. For example, 192.168.0.51 can be displayed in Live Status and Live Summary as Bob Jones. If a user has more than one network name, you can assign both of these network aliases to the same user's name. To set up aliases, open Aliases by clicking on the **Aliases** sidebar icon in Live Configuration.

Departments are groups of users. You can set up departments, such as Accounts or Sales, to use when filtering your log files. It is easier to set up aliases for your usernames before you set up departments, since departments contain those usernames. To set up departments, open Departments by clicking on the **Departments** sidebar icon in Live Configuration. You can also convert Windows NT® or 2000 user groups into departments using the Department Wizard.

You can customize profiles very easily. For example, you might want to add the addresses for your company's website, or your suppliers' websites to the 'My Organization' profile, so you could identify work-related web browsing. Similarly, if you knew a particular user was accessing an unacceptable website, you could use that site's name as a keyword in a new profile, called 'Unacceptable'. To customize your profiles, open Profiles by clicking on the **Profiles** sidebar icon in Live Configuration.

You can quickly create aliases, departments and customize profiles from Live Status and Live Summary. Simply right-click on any user you want to create an alias for, or add to a department, and select the appropriate item from the pop-up menu. *Live* will open the appropriate dialog for you. You can also assign any site you see in a Details dialog or Live Summary to an appropriate profile by right-clicking on the site or resource name and selecting 'Adjust Profile...' from the pop-up menu. You can add or exclude the site from any profile, or create a new profile.

If you are seeing Internet traffic that you are not interested in, you can always filter the log files you are monitoring to only monitor what you have to. You can filter by protocol, profile or department. To filter your log files, simply edit an existing input using the Input Wizard, making sure you choose to filter your log files on the Filter page.

If some of the sites your users are visiting are listed as IP addresses (e.g. 209.61.214.8), you can get *Live* to translate the IP addresses into real site names. Just use the Input Wizard to edit each of your inputs, making sure you check the 'Resolve site IPs' checkbox on the Folders page of the wizard each time.



To improve *WebSpy Live*'s performance, you should only keep your most recent log files in the folders *Live* monitors. If you archive the older logs in another folder, so *Live* only monitors the most recent log file, you will find that *Live* works faster and more efficiently. You can also modify options on the Advanced Settings Page of the Input Wizard to minimize CPU usage. You will need to do this on a per-input basis.

You can use aliases, departments and profiles from *WebSpy Analyzer 2.0*, and profiles from *WebSpy Analyzer 1.0*.

There are lots of options you can specify to make *Live* easier for you to use. You can play sounds whenever an alert is raised, automatically start *Live* whenever your computer starts, and keep *Live* Status on top of any open windows. You can change any of these settings from *Live* Options, which you can access from *Live* Configuration, *Live* Summary, *Live* Status or the *Live* system tray icon.

Supported Log File Formats

C Proxy	Groupwise Internet Agent	Net Proxy	Syslog Utility
CacheXpress	Kiwi's Syslog Daemon	Netscape Proxy	Trend Interscan Webmanager
Checkpoint Firewall-1	LinkSYS	Netscreen	Vicomsoft Web Cache
Cisco Firewall	Lotus Domino	Novell Border Manager	WebSense
Cisco Pix	Mailgate (RG)	Novell Border Manager Extended	WebSpy Netflow
ConSeal Firewall	Mailtraq	Pro FTP	WebSpy Sentinel
Cyberguard Firewall	MDaemon	ProxyNow!	WebSTAR Proxy Server
CSM Blocking Log	Microsoft Exchange Server	Raptor Firewall	WebSweeper
FT Gate	Microsoft ISA Server	Sendmail	Wingate
FT Gate Webserver	Microsoft Proxy	SonicWall	Winroute Firewall
Gauntlet Firewall	Microsoft IIS	Squid Native	Winroute Pro - Mail
GNATBox	Midpoint	Squid Additional	WT Syslog