



WebSpy Live 2.1
User Guide



© WebSpy Ltd. 2001 - 2004

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.



Table Of Contents

1. Overview	1
<i>About WebSpy Live 2.1</i>	<i>1</i>
<i>Minimum Requirements</i>	<i>1</i>
<i>Getting Started.....</i>	<i>2</i>
<i>Automatic Updates.....</i>	<i>2</i>
2. Live Configuration.....	5
<i>About Live Configuration</i>	<i>5</i>
<i>Navigating Live Configuration</i>	<i>5</i>
<i>Inputs</i>	
About Inputs.....	6
Adding Inputs	7
Inputs Wizard	7
Using the Input Wizard.....	7
Folder Page	8
Advanced Settings Page	10
Filters Page	11
Additional Filters Page.....	11
Protocol Filter Page.....	12
Profile Filter Page	12
Department Filter Page	13
Final Page	13
Editing an Input	13
Deleting Inputs	13
Enabling Inputs	14
Disabling Inputs	14
Input Issues	14
<i>Triggers.....</i>	<i>15</i>
About Triggers	15
Adding Triggers	16
Trigger Wizard	17
Using the Trigger Wizard	17
Trigger Type Page	18
Single Hit Triggers.....	19
Session & Cumulative Triggers	23
Trigger Properties page	25
Email Notification page.....	26
Final Page	27
Single Hit Trigger Example	27
Session Trigger Example.....	28
Cumulative Trigger Example.....	29
Editing Triggers	29
Deleting Triggers	30
Deleting All Triggers.....	30
Saving Triggers	30
Creating Triggers Lists.....	31
Opening Triggers	31
Disabling Triggers.....	31
Enabling Triggers.....	32
Changing a Trigger's Priority	32
<i>Profiles.....</i>	<i>33</i>
About Profiles.....	33
Adding Profiles	33
Adding Keywords.....	34



Keyword Tips	35
Editing Keywords	35
Deleting Keywords	36
Editing Profiles	36
Deleting Profiles	37
Deleting All Profiles	37
Saving Profiles Lists	38
Creating Profiles Lists	38
Opening Profiles Lists	38
Exporting Profiles Lists	39
Importing Profiles Lists	39
The Miscellaneous Profile	40
<i>Aliases</i>	<i>40</i>
About Aliases	40
User Names	42
About User Names	42
About User Names	42
Adding User Names	43
Using the Unassigned List	43
Resolving IP Addresses	44
Editing User Names	44
Deleting User Names	45
Deleting All User Names	45
Creating User Names Lists	46
Saving User Names	46
Opening User Names	46
Exporting User Names to CSV	47
Importing User Names from CSV	47
Site Names	48
About Site Names	48
Adding Site Names	48
Editing Site Names	49
Deleting Site Names	50
Deleting All Site Names	50
Creating Site Names Lists	50
Saving Site Names	51
Opening Site Names	51
Exporting Site Names to CSV	52
Importing Site Names from CSV	52
File types	53
About File types	53
Adding File Types	53
Editing File Types	54
Deleting File Types	54
Deleting All File Types	55
Creating File Types Lists	55
Saving File Types	55
Opening File Types	56
Exporting File Types to CSV	56
Importing File Types from CSV	57
About Departments	57
About Departments	57
Adding Departments	58
Using the Unassigned List	59
Editing Departments	59
Deleting Departments	60
Deleting All Departments	60



Creating Departments Lists	60
Saving Departments	61
Opening Departments	61
Exporting Departments to CSV	62
Importing Departments from CSV	62
Using Default Departments	63
Importing Windows Users	63
Department Wizard.....	63
Using Wildcards in Aliases.....	66
3. Live Status	67
<i>About Live Status.....</i>	<i>67</i>
Alerts 68	
Protocol Icons	68
Collapsing and Expanding Groups.....	69
Displaying Alert Details	69
Alert Details Dialog.....	70
Dismissing Alerts	72
Marking Alerts as Read	73
Displaying User Details	73
User Details Dialog.....	73
Emailing Users in Live Status.....	74
Adding Users to User names.....	75
Adding Users to Departments	75
Disabling Triggers from Live Status	76
Enabling Triggers from Live Status	76
Suspending Live	77
Resetting Live	77
Shutting Down Live	77
4. Live Summary	79
<i>About Live Summary</i>	<i>79</i>
<i>Navigating Between Summary Levels.....</i>	<i>80</i>
Users Level	80
User Sessions Level	80
Site Level	81
Sorting Data.....	81
Emailing Users in Live Summary	81
Browsing to a URL.....	82
Adding Users or Sites to Aliases	83
Adding Keywords to Profiles	83
5. Live Options	85
Live Options.....	85
General Options.....	85
Display Options	86
Sound Options.....	87
Location Options	87
Email Options.....	89
Extensions Options.....	89
Appearance Options	90
6. Glossary	93
7. Index	100



1. Overview

About WebSpy Live 2.1

WebSpy Live provides you with a real-time picture of what people using your Internet resources are doing. *Live* works in the background while you work, and raises alerts when someone in your organization uses network resources inappropriately. *Live* can also notify you when appropriate or productive browsing occurs.

Live monitors your Internet and network traffic by monitoring log files produced by a logging device, such as an Internet Gateway, Email or Proxy Server. These log files contain information about the traffic on your network.

The type of network activity that *Live* can monitor is limited to the number of protocols that your logging device captures. Common protocols that you may want to monitor include web (HTTP) email (SMTP) and file transfer (FTP).

Live constantly checks your monitored log files and imports new hits. If these hits match any of the triggers you have set up, an alert is triggered and displayed in Live Status.

There are three main parts to *Live*:

- Live Configuration
- Live Status
- Live Summary

The Live Status window is automatically displayed when an alert is triggered. You can also access this dialog at any time by clicking the *Live* icon in the system tray. For information on using Live Status, see Live Status on page 67.

You can customize what you want to be alerted to using Triggers. Triggers, as well as Inputs, Profiles and Aliases are configured using the Live Configuration dialog. For information on using Live Configuration, see Live Configuration on page 5.

The Live Summary dialog presents an overview of all users that have been using your organization's network resources. This includes external users that have sent information to your organization (such as email). For information on using Live Summary, see Live Summary on page 79.

Minimum Requirements

WebSpy Live can be installed on any computer on your network that is running Windows® 98, or above. *Live* runs best on a computer using Windows® 2000 or XP 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 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 support@webspy.com.



Getting Started

The first time you open *WebSpy Live*, Live Configuration and Live Status is displayed. Live Status will be flashing an input issue (black alert) because no inputs are configured.

To start using *Live*:

1. Set up your Inputs. This step configures *Live* to monitor the location that contains your log files. For information on adding inputs, see Adding Inputs on page 7.
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. When an alert is triggered, double-click the alert to see its detail in the Alert Details dialog. Use the buttons on the Alert Details dialog to dismiss the alert or email it's details to a user. For more information on using Live Status, see Live Status on page 67.
3. Use Live Summary to get an overview of the Internet and email activity of all users. For information on using Live Summary, see Live Summary on page 79.

To use *Live* more effectively, you can:

- Create new triggers to alert you to specific Internet or email usage (see Triggers on page 15)
- Create and refine your aliases to represent users, site names, file extensions, and departments (see Aliases on page 40)
- Create and refine your profiles to categorize your data more effectively (see Profiles on page 33)
- Customize Live Options to change how data is displayed and where it is saved (see Live Options on page 85).

If you would like more information on any *Live* functionality, press F1. This launches the appropriate help topic for the screen or dialog you are currently on.

For more information on getting started with *Live*, see the *Live* Getting Started Guide available for download from www.webspy.com.

Automatic Updates

Improvements to WebSpy Live are constantly being made and updates are issued regularly. When you start WebSpy Live, the application checks the Internet for updates and notifies you if updates are available.

You can also check for updates manually by selecting Tools | Check for updates from the main menu.

Please note:

You need to have an active Internet connection to check for updates.

If updates are available, you can simply install the latest updates by clicking the **Install Latest** button on the Update dialog.

Updates to WebSpy Live and updates to the list of supported log formats are made frequently. You may therefore want to update the list of supported log formats, but not update the program. You can do this by clicking the Select Updates... button on the update dialog. This launches the Available Updates dialog.



The Available Updates dialog displays all available updates and downgrades. A plus symbol indicates updates and a minus symbol represents downgrades. A zero represents the version you currently have. A description of the selected update is displayed at the bottom of the list.

Select the updates you want to download and install and click the **Install** button.

The progress of the download and installation is displayed. You can cancel the process at any time.



2. Live Configuration

About Live Configuration

Live Configuration is automatically displayed the first time you run *WebSpy Live*. In order to use *Live* effectively you will need to use Live Configuration to set up inputs, triggers, profiles, and aliases.

To launch Live Configuration, right-click the Live icon in your system tray and select 'Configuration' from the pop-up menu.

OR

If you already have Live Status open, click on the Live icon in the top left hand corner and select 'Configuration' from the menu that is displayed.

Live Configuration provides access to the following areas:

- Inputs - where you can specify the log files you want to monitor
- Triggers - where you can specify the conditions you want to be alerted to
- Profiles - where you can categorize types of browsing using keyword matching
- Aliases - where you can configure user names, site names, file types and departments
- Options - where you can customize the way you want *Live* to behave

Navigating Live Configuration

Live Configuration is launched by right-clicking the Live icon in your system tray and selecting 'Configuration' from the pop-up menu.

Live Configuration consists of four components:

- Sidebar
- main menu
- Task pads
- data screen

The Sidebar is located down the left side of Live Configuration, and provides access to the various areas of Live Configuration. You can also access these areas via the **Views** main menu item.

If using the **Views** main menu item is your preferred method of navigation, you can hide the Sidebar by selecting **Views | Show Sidebar** from the main menu. Repeat this to display the Sidebar again. Both the Views main menu item and the Sidebar provide access to Inputs, Triggers, Profiles and Aliases.

The main menu is located at the top of Live Configuration, and provides additional access to other views and functions of *Live*.

Task pads are located next to the Sidebar or, if the Sidebar is hidden, on the left hand side of the screen. Each task pad contains hyperlinks that, when clicked, perform a certain function.

To the right of the task pads is the data screen. This displays the current configuration for each view.



Each screen in Live Configuration has an information page that you can access using the **Information** button at the top of each data screen. These information pages provide an overview of the functionality of the screen you are currently on.

Inputs

About Inputs

The first step in using *Live* is configuring your inputs to monitor your particular Internet gateway, firewall, or mail server's log files.

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. You can monitor log files stored on a local or network drive. Inputs are configured using the Input Wizard.

To access Inputs, select **Views | Inputs** from the main menu of Live Configuration, or click the Inputs Sidebar icon.

On the Inputs screen, you can:

- Add, edit and delete inputs
- Enable or disable inputs

If your proxy server produces 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 ensure *Live* only monitors the correct files.

If you use Microsoft® Proxy Server, you might use W3*.log as your file mask to only monitor the logs beginning with W3, and not the logs beginning with WS (WS*.log).

For example, if you use Microsoft® Proxy Server, you might use W3*.log as your file mask to only monitor the logs beginning with W3, and not the logs beginning with WS (WS*.log).

Once you have defined an input, *Live* monitors the specified log files and alert you to activity that breaches any triggers you have defined.

Note:

When you close and re-open Live, the hits made since the time Live was shut down are imported and any alerts are raised. These alerts may be triggered in quick succession. You can reset Live to begin monitoring from the current time.

If your log files are moved or deleted, or if your input can no longer read your log files, you will receive an input issue alert in Live Status.

Log files older than the purge time specified in General Options are not monitored.

If this is the first time you have run *Live*, monitoring begins from the end of each log file. Hits recorded prior to that time are not imported.



Adding Inputs

Before *WebSpy Live* can start monitoring your log files, you need to add an input. An input tells *Live* which of your Internet gateway, firewall or mail server's log files need to be monitored.

To add an input:

1. In Live Configuration, go to Inputs by selecting **Views | Inputs** from the main menu or by clicking on the Inputs Sidebar icon
2. Click on the **Add new input** link in the Inputs task pad to launch the Input Wizard

The Input Wizard guides you through the process of specifying the folder that contains the log files you want to monitor, as well as their format, and any filters you want to use.

Inputs Wizard

Using the Input Wizard

The Input Wizard guides you through the process of choosing log files for *WebSpy Live* to monitor. You can also specify the formats of your files, and define any filters you wish to use for that input.

You can use the Input Wizard to add further inputs or edit any of your existing inputs.

To launch the Input Wizard:

1. In Live Configuration, go to Inputs by selecting **Views | Inputs** from the main menu, or by clicking on the Inputs Sidebar icon
2. Click the **Add new input** link in the Inputs task pad

The Input Wizard has the following pages:

- **Welcome Page**
On this page, click **Next** to proceed to the Folder page
- **Folder Page**
On this page, specify the location of the log files you want to monitor
- **Advanced Settings Page**
On this page, specify the time interval for checking updates to the log files you are monitoring, and what to do when a problem occurs with the log file format
- **Filters Page**
On this page, specify filters to reduce the amount of data *Live* is monitoring
- **Final Page**
On this page, read the summary of the input details and click **back** to make any necessary changes

Depending on the choices made on the Filter Page, the following pages may also be displayed:

- **Additional Filters Page**
On this page of the Input Wizard, you can select whether to filter your inputs by protocols, profiles or departments.
- **Protocol Filter page**
On this page of the Input Wizard, you can select the protocols you are interested in monitoring. If you do not filter your protocols, all protocols will be monitored by default.



- **Profile Filter page**
This page of the Input Wizard enables you to select the profiles you are interested in monitoring. If you do not filter your profiles, all profiles will be monitored by default.
- **Department Filter page**
This page of the Input Wizard enables you to select the departments you are interested in monitoring. If you do not filter by department, all departments will be monitored by default.

You can return to any previous page in the wizard to change any of your selections by clicking the **Back** button.

Folder Page

On this page of the wizard you specify the location of the folder that contains the log files you want to monitor. You also need to select the logging device that was used to produce your log files. A file mask can also be defined on this page to avoid monitoring unnecessary files.

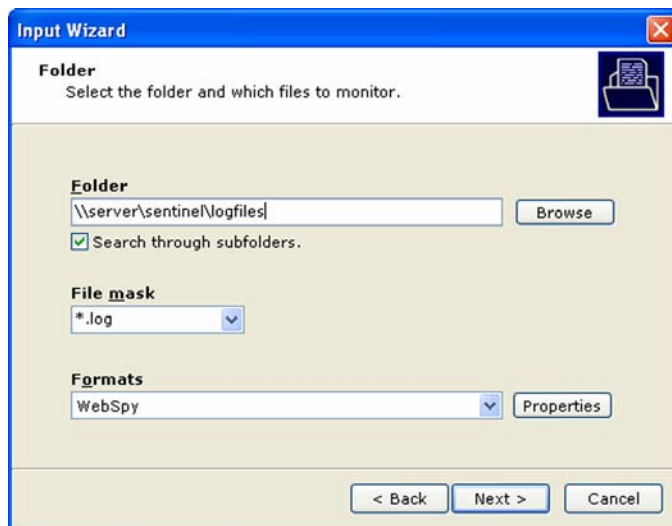


Figure 1: Input Wizard - Folder Page

On the Folder page:

1. Type the location of the folder that contains the log files you want *Live* to monitor directly into the 'Folder' edit box. Alternatively, navigate to the folder by clicking the **Browse** button to launch the Browse for Folder dialog. Navigate to the folder, then click **OK**.

For example, to instruct *Live* to monitor the log files in the 'Logs' folder on the computer with the IP address of 192.168.0.1, type: `\\192.168.0.1\logs` into the 'Folder' edit box.

2. To monitor the log files in any existing subfolders, check the 'Search through subfolders' checkbox. You may want to do this if your proxy server creates sub-folders to store different types of log files in separate locations.
3. Select an appropriate file mask from the drop down list, or enter a custom file mask of your own. If you want *Live* to monitor all files in the folder, select * from the drop down list.
4. Select the format of the log files you are monitoring from the 'Formats' drop-down list. *Live* supports over 80 different log file formats, however if you are using a format that is not supported, please send a sample log file to WebSpy Support, and they will endeavour to assist you.



Sometimes, log files of the same format can have slightly different properties, such as a different date format. For this reason, you may need to edit the properties of your log format.

To edit the properties of your log format:

1. Select your the name of your logging device the 'Formats' drop down list
2. Click the **Properties** button to launch the Format Properties dialog
3. Make the necessary changes on this dialog and click **OK**

Note:

Live will monitor all log files including any new logs added to the folder you specified. If you limit the number of files in this folder, *Live* will use fewer resources. Use file masks and delete/move the files that you do not want *Live* to monitor to ensure that only the relevant log files are monitored.

Once you have made your selections, click **Next** to continue.

Format Properties

Sometimes, log files of the same format can have slightly different properties, such as a different date format.

For example, *Live* may interpret the date format of your log file as dd/mm/yyyy. However, you may actually be recording your date format as yyyy/mm/dd.

WebSpy Live enables you to edit the properties of your log format to change the way log files are imported. You may need to do this if you are Input issues when monitoring your log files.

Format properties are pre-configured so that you should not need to change them if you select the correct format for your log files, however if you have customized the way your proxy server or gateway logs information, then you may need to change the format properties of your storage.

Format properties are edited using the Format Properties dialog which is launched from the Folder page of the Input Wizard (see Folder Page on page 8).

The following Format properties may be available for editing, depending on the format you currently have selected:

- **Formats**

When importing log files into a storage, you are only required to select the generic log file format, and *Live* will detect the version number automatically. If you are experiencing issues when importing your log files, you can specify the version number of the format you are using.

To specify a version number:

1. Check the choose format checkbox
2. Select the version number from the drop down list

- **Date Format**

You may be using a log format with a customized date format. For example, your log format may represent dates using the format Day:Month:Year, however *Live* may be expecting the format Year:Day:Month

To change the date format, select another format from the drop down list.

- **Time Zone**

If you proxy server or gateway records times in GMT, you can add an offset to this time in order to customize the time zone you are in. It is also useful if



you have changed to daylight saving time, or if your proxy server or gateway has consistently recorded incorrect times.

To add a time offset, select the appropriate offset from the drop down list.

For example, an offset of +08:00 will add eight hours to the times recorded in your log files.

- **Field Indexes**

If you know the order of data fields in your log file, you can manually specify the order to minimize the chances of *Live* incorrectly importing information.

For example, you may know that the date is the first field in the log file, IP address is the second, and user name is the third. You can specify these field indexes manually.

To specify the order of data fields:

1. Click the **Properties** button next to Field Indexes
 2. Select a field where the index in the log file is known
 3. Click the **Edit** button on the toolbar
 4. Enter the index value into the edit box. The value you enter must be one less than the index number of the field in the log file. For example, if the field is the eighth field in the log file, enter the number '7'. For the first field in the log file, enter the number '0'. A value of '-1' indicates that *Live* should automatically detect the field number.
 5. Click **OK**
 6. Repeat steps 2 - 4 until all the required known fields indexes have been edited
 7. Click **OK**
- **Separator**
If your log format uses a customized character to separate data fields, you can select whether that character is a comma, tab, space, colon, semicolon, or another character that you can type into the Separator edit box.
 - **Content**
This option is only available for the WebSpy Sentinel format. It enables you to select whether to import content.

You can set all the options back to the original values by clicking the **Defaults** button at the bottom of the dialog.

If you require assistance in changing the format properties of a storage, send WebSpy Support a copy of your log file, and they will advise you of any necessary changes that need to be made to the format properties.

Advanced Settings Page

On this page of the Input Wizard you can specify how often *Live* checks the log files being monitored and imports new hits. You can also specify what to do when a problem occurs when importing hits from your log files. In most situations, you will not need to change these settings, and can safely click **Next** to proceed to the next page of the wizard.

Live checks your log files to ensure that all hits are recorded and monitored in a timely manner. The default time interval between checks is set to one second and this value is suitable for most environments. This means that *Live* will check your log files for updates once every second.



In most cases you will not need to change this default time interval, however if you have a lower specification computer you may want to make this time interval longer in order to reduce CPU utilization.

You may also want to specify a longer time interval if your organization does not experience heavy Internet traffic, because fewer hits will be added to your log files each second. You may also specify a longer time if the logging device you are using takes a long time to record hits.

To specify a longer time interval, simply type the time interval in seconds into the appropriate edit box on this page of the wizard.

Check the 'Ignore all log file format issues' checkbox to ignore any issues arising from an incorrect log file format for the log file *Live* is monitoring. Input issues may still arise if problems relating to network availability occur.

For example, if your proxy server was rebooted, *Live* may experience problems accessing the folder containing the log files it was monitoring, and an input issue would be displayed in Live Status.

Click **Next** to proceed to the Filters Page.

Filters Page

On the Filters page, you can choose whether or not to monitor failed hits, resolve IP addresses, or further filter the data from the log files you are monitoring.

To filter out failed hits, un-check the 'Include failed hits' checkbox so that these hits are not monitored by *WebSpy Live*. If you do not un-check this box, all failed hits will be monitored, and they will be displayed in red in the Alert Details dialogs (see Alert Details Dialog on page 70) and the Site level of Live Summary (see Navigating Between Summary Levels on page 80).

If you want *Live* to automatically resolve user and site IP addresses into meaningful names, check the 'Resolve IPs' checkbox.

On the Filters page, you can choose whether or not you want to further filter your log files by protocol, profile or department. To further filter your log files, select the 'Yes' radio button. This includes the Additional Filters page in the wizard (see Additional Filters Page on page 11).

Hint:

If you apply profile filtering, it is a good idea to check the 'resolve IPs' checkbox so that *Live* can check the real names of visited web sites for keywords.

If you do not want to filter your log files by protocol, profile or department, select 'No' and proceed to the final page of the wizard.

Once you have made your selections, click **Next** to continue.

Additional Filters Page

The Additional Filters page enables you to select the types of additional filters you want to apply to your input.



There are three types of additional filters available:

- **Filter by Protocols**
If your log files contain information about more than one protocol, you can filter your inputs so that only selected protocols are monitored.
- **Filter by Profiles**
Filtering your inputs by profiles is useful if you do not want to monitor information that belongs to a specific category.
- **Filter by Departments**
You can filter your inputs by departments to exclude groups of users from being monitored. You first need to configure your departments in Aliases.

Check the checkbox next to the additional filter you want to apply. Each checkbox includes the appropriate filter page in the wizard, where you can configure the filters.

Protocol Filter Page

If your log files contain information about more than one protocol the Protocol Filters page enables you to select the protocols you are interested in monitoring. Filtering your inputs by profiles is useful if you do not want to view any information belonging to a certain protocol.

The Protocol Filter page is only displayed if you selected 'Filter by Protocols' on the Additional Filters page (see Additional Filters Page on page 11).

If your log files contain information about more than one protocol the Protocol Filters page enables you to select the protocols you are interested in monitoring.

On the Protocol Filter page, check the checkbox next to the name of the protocol you want to monitor. Leave unchecked the protocols that you want to filter out. Use the **Select all** and **Clear Selection** buttons as necessary.

Once you have made your selections, click **Next** to continue.

Profile Filter Page

The Profile Filter page enables you to select the profiles you want *Live* to monitor. Filtering your inputs by profiles is useful if you do not want to view any information of a certain category type.

For example, by filtering out information that belongs to the 'Advertising' profile, you can avoid receiving alerts due to pop-up messages and advertising banners.

The Profile Filter page is only displayed if you selected 'Filter by Profiles' on the Additional Filters page (see Additional Filters Page on page 11).

On the Profile Filter page, check the checkbox next to the name of the profiles you want to monitor. Leave unchecked the profiles that you want to filter out. Use the **Select all** and **Clear Selection** buttons as necessary.

Once you have made your selections, click **Next** to continue.



Department Filter Page

The Department Filter page enables you to select the departments you want *Live* to monitor. You can use department filtering to monitor a certain group of users, or all users except a certain group of users.

For example, department filtering can enable you to monitor everyone in your organization except for high-level management.

The Department Filter page is only displayed if you selected 'Filter by Departments' on the Additional Filters page (see Additional Filters Page on page 11).

Before you can select a department to monitor, you need to have configured some departments in Aliases (see About Departments on page 57).

On the Department Filter page, check the checkbox next to the name of the department you want to monitor. Leave unchecked the departments that you want to filter out. Use the **Select all** and **Clear Selection** buttons as necessary.

Note:

Only departments currently set up in Aliases are can be selected on the Department Filter page. Users that are not assigned to a department are automatically assigned to the 'Miscellaneous' Department.

Once you have made your selections, click **Next** to continue.

Final Page

The last page of the Input Wizard provides a summary of the input details you have specified, including any filters you have applied to the log files.

Click **Finish** to start monitoring, or click **Back** to change your selections. Clicking **Cancel** will return you to the Inputs screen without adding a new input.

Editing an Input

You can easily change the details of an existing input.

For example, if the IP address of your proxy server is changed, you can change the location that the input is monitoring.

To edit an input:

1. In Live Configuration, go to Inputs by selecting **Views | Inputs** from the main menu, or by clicking on the Inputs Sidebar icon
2. Select the input you want to edit
3. Click the **Edit selected input** link on the Inputs task pad to launch the Input Wizard (see Using the Input Wizard on page 7)
4. Navigate through the pages of the Input Wizard to make all required changes

Your input will now use the new configuration when monitoring your log files.

Deleting Inputs

WebSpy Live enables you to delete any inputs that you no longer require. Once an input is deleted, it cannot be recovered without recreating the input.



To delete an input:

1. In Live Configuration, go to Inputs by selecting **Views | Inputs** from the main menu, or by clicking on the Inputs Sidebar icon.
2. Select the input in the list that you want to delete
3. Click on the **Delete selected input** link in the Inputs task pad.
4. Click **Yes** on the confirmation dialog to delete the input. If you do not want to delete the input, click **No** to return to Inputs without deleting.

Hint:

You can also delete an input by right-clicking on the input and choosing the 'Delete' option from the pop-up menu.

If you need to change an input, such as if your proxy server changes its IP address, you can simply edit an existing input rather than deleting the existing input and adding a new one with the new IP address.

Enabling Inputs

You can enable and disable any inputs you have added. This enables you to stop and start *Live* monitoring the log files in a specified location without deleting inputs.

To disable an Input:

1. In Live Configuration, go to Inputs by selecting **Views | Inputs** from the main menu or by clicking on the Inputs Sidebar icon
2. Select the disabled input in the list that you want to enable
3. Click the **Enable selected input** link on the Inputs task pad

The status of the input will change to 'Enabled'. *Live* will start monitoring the log files specified in the newly enabled input.

To disable the input, see Disabling Inputs on page 14.

Disabling Inputs

You can enable and disable any inputs you have added. This enables you to stop and start *Live* monitoring the log files in a specified location without deleting inputs.

To disable an input:

1. In Live Configuration, go to Inputs by selecting **Views | Inputs** from the main menu or by clicking on the Inputs Sidebar icon.
2. Select the enabled input in the list that you want to disable.
3. Click on the **Disable selected input** on the Inputs task pad.

The status of the input will change to 'Disabled'. *Live* will stop monitoring the log files specified in the disabled input.

To enable the input, see Enabling Inputs on page 14.

Input Issues

If *WebSpy Live* has difficulties reading the log files you are currently monitoring, the black input issues alert icon is displayed in your system tray (See Alerts).



Input issues may occur because of a corrupted log file, an incorrect date format or a change in format of a log file. Issues relating to network availability will also raise input issues.

For example, if your proxy server is rebooted, *Live* will experience problems accessing the folder containing the log files it was monitoring.

When an input issue is encountered, *Live* will stop monitoring the log files involved.

If you receive an input issues alert in Live Status, right-click on the alert and select the 'Display' option from the pop-up menu. This launches the Input Issues dialog describing the problem *Live* has encountered while monitoring the input.

When input issues occur you can:

- **Resume monitoring your input**
Click on the **Resume** link in the dialog to resume monitoring. This is most appropriate if the last item read from your log file is corrupt. *Live* will skip that item and start monitoring again, and the input issues alert will be removed from Live Status.
- **Edit your input and then resume monitoring**
You may need to edit your input because you selected an incorrect format for your log files. Go back and edit your input using the Input Wizard in Live Configuration. You can then resume monitoring by enabling the input.
- **Email support with any queries**
If you cannot resolve any input issues, you can email WebSpy Support by clicking on the **Email** link in the Input Issues dialog. This may be necessary particularly if your log file format is not supported by *Live*, or if you do not know the format of your log files.

Live will launch your default email program and export the subject heading and input issue details to the body of the email. Add any additional comments and, if possible, attach a sample of your log files to ensure our support team can assist you as quickly as possible.

If you have any input issues that you cannot resolve please contact support@webspy.com.

Hint:

You can also resume monitoring an input from Live Status. Right-click on the input issues alert and select the 'Resume' option from the pop-up menu.

Triggers

About Triggers

WebSpy Live generates alerts when browsing activity matches the conditions specified in a trigger.

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. You can specify conditions based on the types of web sites visited, as well as the length of time users have been browsing, and size and types of downloaded resources.

For example, you can specify a trigger to alert you when users download resources greater than 100Kb from web sites that belong to the unacceptable content profile.



When a trigger is breached, *Live* displays the alert in Live Status. You can assign a priority to each trigger, and depending on this priority level, a different colored alert icon is displayed in Live Status.

There are three different types of triggers:

- **Single Hit triggers**

Single Hit triggers enable you to specify alert conditions based on individual hits in your log files. Using a Single Hit trigger, you can set up *Live* to raise alerts based on any or all of the following conditions; Size, Users, Site names, File types, Departments, Profiles, and Protocols.

For more information, see the Single Hit Trigger Page of the Trigger Wizard on page 19. See also Single Hit Trigger Example on page 27.

- **Session triggers**

A Session trigger alerts you users that are browsing excessively, and/or downloading large amounts within the one session.

For more information, see the Session Trigger Page of the Trigger Wizard on page 23. See also Session Trigger Example on page 28.

- **Cumulative triggers**

Cumulative triggers enable you to set up alerts based on the total activity of your users. Cumulative triggers can be based on the total amount of time users have spent browsing, or the total size of resources they have downloaded.

For more information, see the Cumulative Trigger Page of the Trigger Wizard on page 23. See also Cumulative Trigger Example on page 29.

You can configure Triggers using the Triggers view of Live Configuration (see Live Configuration on page 5), which is accessed by selecting **Views | Triggers** from the main menu, or clicking the Triggers Sidebar icon.

Live comes with a list of common triggers, such as 'Unacceptable Content' and 'Large Downloads'. You can use these existing triggers and add your own custom triggers to suit your organization (see Adding Triggers on page 16). You can also edit and delete any of your triggers (see Editing Triggers on page 29, and Deleting Triggers on page 30).

The triggers listed in the Triggers screen can be saved (see Saving Triggers on page 30) to a file with the extension *.Triggers. These files can then be opened at any time (see Opening Triggers on page 31)

You can also enable and disable any triggers if you want to stop them from raising alerts (see Enabling Triggers on page 32, and Disabling Triggers on page 31).

Adding Triggers

WebSpy Live enables you to set up specific triggers that generate alerts when their conditions are breached.

To add a trigger:

1. In Live Configuration, select **Views | Triggers** from the main menu, or click the Triggers Sidebar icon
2. Click the **Add new trigger** link on the Triggers task pad to launch the Trigger Wizard (see Using the Input Wizard on page 7).



The Trigger Wizard guides you through the process of selecting the conditions of the trigger, and assigning it a priority.

Trigger Wizard

Using the Trigger Wizard

The Trigger Wizard enables you to specify triggers that generate alerts when their conditions are breached. These alerts are displayed in Live Status.

The Trigger Wizard is launched when you add or edit a Trigger (see Adding Triggers on page 16, and Editing Triggers on page 29). You can also launch the Trigger Wizard by selecting **Tools | Trigger Wizard** from the main menu of Live Configuration.

The Trigger Wizard consists of the following main pages:

- Welcome page
- Trigger Type page
- Trigger Properties page
- Final page

Depending on the selections made on the Trigger Type page, the following pages may also be displayed:

- Single Hit Trigger page
- Session Trigger page
- Cumulative Trigger page
- Size page
- Time page
- User names page
- Site names page
- File types page
- Departments page
- Profile page
- Protocol page
- Email Page

When you launch the Trigger Wizard, click **Next** to proceed to the Trigger Type page.

You can create as many triggers as required. If you add more than one trigger with the same name, the alerts for these triggers are grouped under the one trigger heading in Live Status. This can be useful for assigning different priority levels to varying extremes of the same type of alert.

For example, you can create a trigger called 'Large Downloads' and configure it to raise an alert for downloaded files over 1MB. You can then assign it the priority 'Medium' so that any alerts are displayed with a yellow alert icon. You can then create another trigger still called 'Large Downloads', but configure it to raise alerts for downloaded files over 5MB, and assign it the priority 'High'. Alerts for both triggers are displayed under the 'Large Download' trigger heading in Live Status, with files over 1MB displayed in yellow, and files over 5MB displayed in red.



Trigger Type Page

The Trigger Type page of the Trigger Wizard enables you to select the type of trigger you want to create.

You can choose from three types of triggers:

- **Single Hit**

Single Hit triggers enable you to specify alert conditions based on individual hits in your log files. Using Single Hit triggers, you can set up *Live* to raise alerts based on any or all of the following conditions; Size, Users, Site names, File types, Departments, Profiles, and Protocols.

To create a Single Hit trigger, select the 'Single Hit trigger' radio button and click **Next** to proceed to the Single Hit Trigger page of the Trigger Wizard.

See Single Hit Trigger Example on page 27 for an example of creating a Single Hit Trigger.

- **Session**

Session triggers enable you to set up alerts based on the time users have spent browsing and the amount of resources they have downloaded in the one session.

Using Session triggers, you can set up *Live* to raise alerts based on the time users have spent browsing during the one session and/or the amount of resources they have downloaded in the session.

You can set up Session triggers for individual users or departments.

For example, you can set up a Session trigger to alert you to an individual user spending longer than 20 minutes browsing the web in the one session.

To create a Session trigger, select the 'Session trigger' radio button and click **Next** to proceed to the Session Trigger page of the Trigger Wizard.

See Session Trigger Example on page 28 for an example of creating a Session trigger.

- **Cumulative**

Cumulative triggers enable you to set up alerts based on the total activity of your users. Cumulative triggers can be based on the total amount of time users have spent browsing, or the total size of resources they have downloaded.

You can set up Cumulative triggers for individual users or departments.

For example, you can set up a Cumulative trigger to alert you to members of a department downloading more than 100MB in 12 hours.

To create a Cumulative trigger, select the 'Cumulative trigger' radio button and click **Next** to proceed to the Cumulative Trigger page of the Trigger Wizard.

See Cumulative Trigger Example on page 29 for an example of creating a Cumulative trigger.

Select the type of trigger you want to create, and click **Next** to continue.



Single Hit Triggers

Single Hit Trigger Page

The Single Hit Trigger page of the Trigger Wizard enables you to specify alert conditions based on individual hits in your log files.

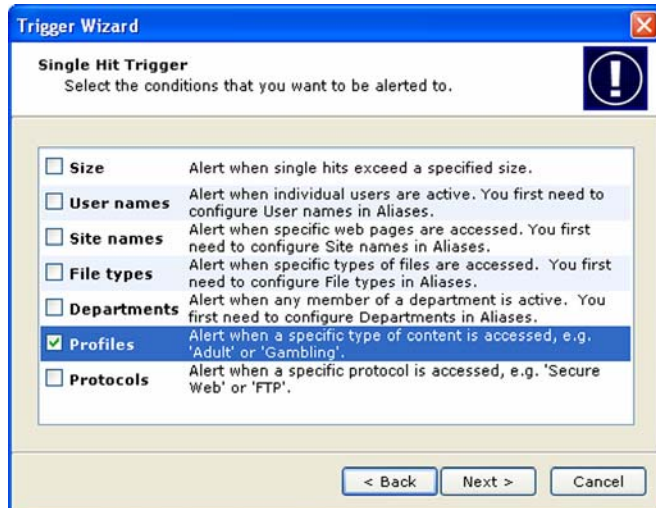


Figure 2: Trigger Wizard - Single Hit Trigger Page

The Single Hit Trigger page of the Trigger Wizard is only displayed if you select 'Single hit trigger' on the Trigger Type page of the wizard (see Trigger Type Page on page 18)

Using Single Hit triggers, you can set up *Live* to raise alerts based on any or all of the following conditions:

- **Size**
Choosing 'Size' enables you to set up alerts based on incoming, outgoing and total size of individual hits. Checking this option includes the Size page in the Trigger Wizard.
- **User names**
Choosing 'Users names' enables you to set up alerts based on individual users. You first need to set up user names in Aliases (see About User Names on page 42). Checking this option includes the User names page in the Trigger Wizard (see User Names Page on page 21).
- **Site names**
Choosing 'Site names' enables you to set up alerts based on individual web sites. You first need to set up site names in Aliases (see Site Names on page 48). Checking this option includes the Site names page in the Trigger Wizard (see Site Names Page on page 21).
- **File types**
Choosing 'File types' enables you to set up alerts based on the types of files accessed by users. For example, you can create a trigger to alert you when a user is downloading multimedia files such as .mp3 and .mpg files. You first need to set up file types in Aliases (see File types on page 53). Checking this option includes the File Types page in the Trigger Wizard (see File Types Page on page 21).
- **Departments**
Choosing 'Departments' enables you to set up alerts based on groups of users. You first need to set up departments in Aliases (see File types on page 53). Checking this option includes the Departments page in the Trigger Wizard (see Departments Page on page 22).



- **Profiles**
Choosing 'Profiles' enables you to set up alerts based on users accessing content that belongs to a specified profile (see About Profiles on page 33). For example, you may set a trigger to alert you when a user is accessing content that belongs to the 'Adult' profile. Checking this option includes the Profiles page in the Trigger Wizard (see Profiles Page on page 22).
- **Protocols**
Choosing 'Protocols' enables you to set up alerts based on individual protocols such as Secure Web or FTP. Checking this option includes the Protocols page in the Trigger Wizard.

For example, you can set up a trigger that alerts you when a particular user browses to a certain site, or when members of a department download files greater than 30KB belonging to the 'Adult' or 'Gambling' profiles.

Note

If you want to set up a trigger that includes user names, site names, file types, or departments, you first need to set these up in Aliases (see About Aliases on page 40).

On the Single Hit Trigger page, select the conditions that you want to be alerted to, by checking the checkbox next to the names of the conditions in the list.

Once you have made your selections, click **Next**. The appropriate pages for the selections you made will be displayed.

Size Page - (Single Hit Triggers)

This page is only displayed if you select 'Size' on the Single Hit Trigger page of the Trigger Wizard (see Single Hit Trigger Page on page 19).

This page enables you to specify the maximum size of an individual resource before an alert is raised. You can specify either an incoming or an outgoing size to differentiate between downloaded and sent resources.

You can also choose to ignore the direction the resource is coming from and simply specify a maximum size for any transferred resource before an alert is raised.

To specify the maximum size a resource must be before an alert is raised:

1. Select either the 'Incoming', 'Outgoing', or 'Total' checkboxes, depending on the direction of transferred resources you want to be alerted about

For example, if you only want to be alerted about downloaded resources, select 'Outgoing size'. If you do not care which direction the resource is coming from, select 'Size'.

2. Type a size into the edit box next to the option you selected, such as '100'
3. Change the unit of size, if necessary, from the drop down list at the top of the dialog.

You can also create Session and Cumulative triggers based on size, to raise alerts for when the sum of downloaded or sent resources exceed a specified size (see Size Page - (Session & Cumulative Triggers) on page 24).

Once you have made your selections, click **Next** to continue.



User Names Page

The User names page enables apply the trigger to certain users.

The User names page of the Trigger Wizard is displayed if you select 'User names' on the Single Hit Trigger page (see Single Hit Trigger Page on page 19), or if you choose 'User names' as an advanced filter on the Session Trigger or Cumulative Trigger pages (see Session Trigger Page on page 23, and Cumulative Trigger Page on page 23).

For example, you can set up a trigger called 'Watch List', and add users that you want to keep an eye on.

All the User names that you have set up in Aliases are displayed on this page (see User Names on page 42)

Check the checkbox next to the name of each user you want to include in the trigger. Use the **Select all**, **Clear selection** and **Invert selection** buttons as required.

Click **Next** once you have made your selections.

Site Names Page

This page enables you apply the trigger to certain web sites.

The Site names page of the Trigger Wizard is only displayed if you select 'Site names' on the Single Hit Trigger page (see Single Hit Trigger Page on page 19).

For example, you can set up a trigger called 'Banned Sites', and add all the specific web sites that you do not want members of your organization to visit. If one of your uses visits the site, you will be alerted.

All the Site names that you have set up in Aliases are displayed on this page (see Site Names on page 48)

Check the checkbox next to the name of each site you want to include in the trigger. Use the **Select all**, **Clear selection** and **Invert selection** buttons as required.

Click **Next** once you have made your selections.

File Types Page

This page enables you set up alerts for when users download specific types of files.

The Files types page of the Trigger Wizard is only displayed if you select 'File types' on the Single Hit Trigger page (see Single Hit Trigger Page on page 19).

For example, you can create a trigger to alert you when a user is downloading multimedia files such as .mp3 and .mpg files.

All the File types that you have set up in Aliases are displayed on this page (see File types on page 53)

Check the checkbox next to the name of each File Type you want to be alerted to. Use the **Select all**, **Clear selection** and **Invert selection** buttons as required.

Click **Next** once you have made your selections.



Departments Page

This page enables you apply the trigger to specific groups of users.

The Departments page of the Trigger Wizard is displayed if you select 'Departments' on the Single Hit Trigger page (see Single Hit Trigger Page on page 19), or if you choose 'Departments' as an advanced filter on the Session Trigger or Cumulative Trigger pages (Session Trigger Page on page 23, and Cumulative Trigger Page on page 23).

For example, you can create triggers that only apply to the members of your 'Marketing' or 'Accounts' department.

All the Departments that you have set up in Aliases are displayed on this page (see About Departments on page 57).

Check the checkbox next to the name of each Department you want to include in the trigger. Use the **Select all**, **Clear selection** and **Invert selection** buttons as required.

Click **Next** once you have made your selections.

Profiles Page

This page enables you set up alerts based on users accessing content that belongs to a specified profile.

The Profiles page of the Trigger Wizard is only displayed if you select 'Profiles' on the Single Hit Trigger page (see Single Hit Trigger Page on page 19).

For example, you can set up a trigger to alert you when a user is accessing content that belongs to the 'Adult' profile.

All the profiles that you have set up are displayed on this page (see About Profiles on page 33)

Check the checkbox next to the name of each Profile you want to include in the trigger. Use the **Select all**, **Clear selection** and **Invert selection** buttons as required.

Click **Next** once you have made your selections.

Protocol Page

The Protocol page of the Trigger Wizard page enables you set up alerts based on individual protocols.

This page is only displayed if you select 'Protocol' on the Single Hit Trigger page (Single Hit Trigger Page on page 19).

For example, you can set up a trigger to alert you to when certain protocols are being used, such as Secure Web or File Transfer Protocol (FTP).

WebSpy Live Supports the following Protocols:

- Domain Name lookup
- File Transfer
- Gopher
- Mail
- News
- Secure Web



- Socks
- Streaming Media
- Telnet
- Web

Live is only able to monitor the protocols that your logging device is configured to record. If your logging device does not support the protocol you want to monitor, you may consider using *WebSpy Sentinel* as your logging device.

Check the checkbox next to the name of the protocols you want to include in the trigger. Use the **Select all**, **Clear selection** and **Invert selection** buttons as required.

Click **Next** once you have made your selections.

Session & Cumulative Triggers

Session Trigger Page

On the Session Trigger page, you can select whether you want to receive alerts based on time and/or size.

You can also choose to apply the trigger only to specific users or departments.

The Session Trigger page is only displayed if you select 'Session Trigger' on the Trigger Type page of the Trigger Wizard (see Trigger Type Page on page 18).

On the Session Trigger page, check the checkbox next to either 'Size' 'Time', or both, depending on the type of information you want to be alerted to.

For example, if you want to be alerted to long sessions, select 'Time'. If you want to be alerted to large amounts of data being downloaded during a session, select 'Size'.

If you want to apply the trigger only to a specific user or department, check the appropriate checkbox under 'Advanced filtering'.

For example, if you want to be alerted to a particular user browsing for too long or downloading too much in the one session, check 'User names'. If you want to be alerted to any member of a department browsing too long or downloading too much, check 'Departments'.

Note:

If you choose to apply the trigger to specific users or departments, these users or departments first need to be specified in Aliases (see About Aliases on page 40).

Once you have made your selections, click **Next** to continue with the Trigger Wizard.

Cumulative Trigger Page

On the Cumulative Trigger page, you can select whether you want to receive alerts based on time and/or size.

You can also apply the trigger to specific users or departments.



The Cumulative Trigger page is only displayed if you selected 'Cumulative Trigger' on the Trigger Type page of the Trigger Wizard (see Trigger Type Page on page 18).

On the Cumulative Trigger page, check the checkbox next to either 'Size', 'Time', or both, depending on the type of information you want to be alerted to.

For example, if you want to be alerted to users that have browsed for too long in total, select 'Time'. If you want to be alerted to users downloading too much data in total, select 'Size'.

If you want to apply the trigger only to a specific user or department, check the appropriate checkbox under 'Advanced filtering'.

For example, if you want to be alerted if a particular user browses for too long or downloads too much, check 'User names'. If you want to be alerted if any member of a department browses too long or downloads too much, check 'Departments'.

Note:

If you choose to apply the trigger to specific users or departments, these users or departments first need to be specified in Aliases (see Aliases on page 40).

Once you have made your selections, click **Next** to continue with the Trigger Wizard.

Size Page - (Session & Cumulative Triggers)

This page enables you to specify the combined size of accessed resources before an alert is raised. You can specify either incoming or outgoing size to differentiate between downloaded and sent resources.

This page is only displayed if you select 'Size' on either the Session Trigger or Cumulative Trigger pages of the Trigger Wizard (see Session Trigger Page on page 23, and Cumulative Trigger Page on page 23).

For example, you can set up an alert for when the total size of downloaded (incoming) resources reaches 100MB.

You can also set up alerts based on the combined size of incoming and outgoing resources.

For example, you can set up an alert for when the total size of both downloaded (incoming) and sent (outgoing) resources reaches 100MB.

To specify the maximum size of transferred resources before an alert is raised:

1. Select either the 'Incoming', 'Outgoing' or 'Total' checkboxes, depending on the direction of transferred resources you want to be alerted about.

For example, if you only want to be alerted about downloaded resources, select 'Incoming'. If you want to be alerted when the combined total of both incoming and outgoing resources reaches a certain size, select 'Total'.

2. Type a size into the edit box next to the option you selected, such as '100'.
3. Change the unit of size, if necessary, from the drop down list at the top of the dialog.

You can also create a Single Hit trigger based on size, to raise alerts when individual downloaded or sent resources exceed a specified size (see Size Page - (Single Hit Triggers) on page 20).



Once you have made your selections, click **Next** to continue.

Time Page

If you are creating a Session Trigger, this page enables you to specify the maximum length of a user's session before an alert is raised.

The Time page of the Trigger Wizard is only displayed if you select 'Time' on either the Session Trigger or Cumulative Trigger pages (see Session Trigger Page on page 23, and Cumulative Trigger Page on page 23).

If you are creating a Cumulative Trigger, this page enables you to specify the total time a user can spend browsing before an alert is raised.

To specify a time, type a maximum time into the edit box at the bottom of the dialog, using the format Hours:Minutes:Seconds.

For example, the time '00:20:15' represents a maximum browsing time of 20 minutes and 15 seconds before the trigger generates an alert.

Once you have entered a time, click **Next** to continue.

Trigger Properties page

The Trigger Properties page of the Trigger Wizard enables you to specify the name and priority level of the trigger. You can also specify whether the trigger should be enabled once you have finished configuring it, and whether the trigger should send emails to specified email addresses each time it raises an alert.

The screenshot shows a dialog box titled "Trigger Wizard" with a sub-header "Trigger Properties" and the instruction "Give this trigger a name and a priority." The "Name" field contains "Watch List". The "Priority" dropdown is set to "High". The "Trigger is enabled" checkbox is checked, and the "Send an email when this trigger generates an Alert" checkbox is unchecked. Navigation buttons at the bottom include "< Back", "Next >", and "Cancel".

Figure 3: Trigger Wizard - Trigger Properties Page

On the Trigger Properties page:

- Enter a name for the trigger in the 'Name' edit box. A default name is provided, however it is recommended you provide a name that meaningfully identifies the trigger.
- Select a priority for the trigger from the 'Priority' drop down list.
- Check the 'Trigger is enabled' checkbox to ensure the trigger is enabled immediately. If you do not want to enable the trigger, un-check this box. Only enabled triggers generate alerts.
- If you want *Live* to automatically send emails to specific users each time an alert is raised, check the 'Send an email when this trigger generates an Alert' checkbox. The Email Notification page is then included in the wizard to specify the email details (see Email Notification page on page 26).



If you are creating a single hit trigger, can also:

- **Set the trigger to raise a new alert each time a hit is made:**

Setting the option to raise new alerts each time a single hit is made, enables more than one alert for the same user to be displayed in Live Status. A new alert is triggered for the same user each time they make single hits that breach the triggers criteria. This option should be set when hits that match the triggers criteria do not have a high frequency of occurring. Such situations include each time a user sends an email, or each time a file greater than 10MB is downloaded.

To set the trigger to raise a new alert each time a hit is made, click the 'Trigger new alert for each hit' radio button.

- **Set the trigger to add new hits to an existing alert:**

Setting the option to add new hits to an existing alert only triggers one alert for each user. Any subsequent hits that also match the triggers criteria are added to this alert. This option should be set when there is a high frequency of hits that could match the triggers criteria. This is useful when alerting on web browsing behaviour as many hits are made each time a user visits a web site (html files, images, script files etc.), and you do not want new alerts generated for each of these hits.

To set the trigger to add new hits to an existing alert, click the 'Add new hit to existing alert' radio button.

If you have selected this option, you can also specify whether the existing alert should be re-triggered when new hits are made. This is useful if you have dismissed or displayed the alert, but you want the alert to be triggered again when new hits are made. Check the 'Re-trigger alert for each new hit' checkbox if you want the alert to be re-triggered when new hits are made. If you do not want the alert to be re-triggered after you have dismissed or displayed it, leave this checkbox un-checked.

Hint:

If you add more than one trigger with the same name, the alerts for these triggers are grouped under the one trigger heading in Live Status. This can be useful for assigning different priorities to varying extremes of the same type of alert.

Email Notification page

You can configure triggers to automatically send emails to specific users each time it raises an alert. The Email Notification page of the Trigger Wizard enables you to configure the details of these emails.

The Email Notification page is only displayed if you checked the 'Send an email when this trigger generates an Alert' checkbox on the Trigger Properties page (see Trigger Properties page on page 25).

On the Email Notification page:

- Enter the email address of the person *Live* should automatically email when the trigger generates an alert into the **To** field
- Enter other email addresses if necessary into the **Cc** and **Bcc** fields
- Enter the subject to be used for each email. A default subject is provided, but it is a good idea to enter a subject that accurately describes the alert

**Hint:**

You can enter multiple email addresses, as long as each address is separated by a comma (,).

Live uses SMTP (Simple Mail Transport Protocol) to automatically send emails. For this to work correctly, you need tell *Live* which SMTP server to use. This is usually the same server you use to send and receive your own emails. You can configure *Live* to use your SMTP server in Email Options, which you can launch by clicking the **Settings...** button on the Email Notification page (see Email Options on page 89).

Note:

Emails are sent in plain text format. If the recipients of the emails use an email client that applies a default font to plain text emails, this can effect the alignment of the alert detail information. To fix this, change the font on the email client to a monospaced font type such as Courier or Lucida Console.

Once you have entered all the email details, click **Next**.

Final Page

The Final page of the Trigger Wizard displays a summary of the selections you have made. Review this summary to ensure the trigger's settings are correct.

If you need to make any changes to the trigger, click **Back** to return to any page in the wizard.

Once you have finished configuring the trigger, click **Finish** to save the trigger. The trigger will be listed in the Triggers view. When the conditions specified in the trigger are breached, an alert will be raised and displayed in Live Status (see Live Status on page 67).

Single Hit Trigger Example

Monitoring requirement: Trigger an alert a particular user downloads multimedia files greater than 1 MB.

Before you add this trigger, you need to ensure that the user you want to monitor has a User name alias and that all their computer names and email addresses have been added to this alias. You set up User names on the User names tab in Aliases.

WebSpy Live comes with a list of File type aliases already defined, including a 'Multimedia' alias with common file extensions such as MP3 and AVI added to it. If you are not using this File Type alias list, you need to ensure that an appropriate alias has been set up with all the file extensions you want to be alerted about added to it. You set up File Types on the File Types tab in Aliases.

To add this trigger:

1. Launch the Trigger Wizard, by selecting **Views | Triggers** from the main menu, and click the **Add new trigger** link in the Triggers task pad.
2. Proceed to the Trigger Type page. Select 'Single hit trigger' and click **Next**.
3. On the Single Hit Trigger page, select check the checkboxes next to 'Size', 'User names' and 'File types'. Click **Next**.
4. On the Size page, check the checkbox next to 'Incoming', and enter the value '1' into the edit box. Select 'Megabytes' from the drop down list. Click **Next**.



5. On the User names page, check the check box next to the user you want to monitor. Only users already defined on the User names tab in Aliases are displayed here. For this example, we will call the user 'XYZ'. Click **Next**.
6. On the File Types page, check the checkbox next to the 'Multimedia' File type alias. Only File Types already defined on the File Types tab in Aliases are displayed here. Click **Next**.
7. On the Trigger Properties page, give the trigger a descriptive name such as 'XYZ multimedia > 1MB'. Select a priority level from the drop down list, and ensure the 'Trigger is enabled' checkbox is checked. Leave the 'Send an email when this trigger generates an Alert' checkbox un-checked unless you want to *Live* to email a user each time an alert is raised. Click **Next**.
8. On the final page of the wizard, check the summary. It should read 'Incoming greater than 1 MB; users: XYZ; files: Multimedia.' Click **Finish**.

The new trigger is displayed in the trigger list. When user XYZ downloads a multimedia file greater than 1MB, an alert will be generated and displayed under the 'XYZ multimedia > 1MB' trigger in Live Status (see Live Status on page 67).

Session Trigger Example

Monitoring requirement: Trigger an alert when members of a particular department conduct a browsing session longer than 15 minutes.

Before you add this trigger, you need to ensure that the department you want to monitor has a department alias, and that all the members of the department have been added to it. You set up departments on the departments tab in Aliases (see About Departments on page 57).

To add this trigger:

1. Launch the Trigger Wizard, by selecting **Views | Triggers** from the main menu, and click the **Add new trigger** link in the Triggers task pad.
2. Proceed to the Trigger Type page. Select 'Session trigger' and click **Next**.
3. On the Session Trigger page, select check the checkbox next to 'Time'. Under 'Advanced Filtering', check the 'Departments' checkbox. Click **Next**.
4. On the Time page, enter '00:15:00' into the edit box. Click **Next**.
5. On the Departments page, check the checkbox next to the departments you want to monitor. Only departments already defined on the Departments tab in Aliases are displayed here. For this example, we will call the department 'XYZ'. Click **Next**.
6. On the Trigger Properties page, give the trigger a descriptive name such as 'XYZ sessions > 15 mins'. Select a priority level from the drop down list, and ensure the 'Trigger is enabled' checkbox is checked. Leave the 'Send an email when this trigger generates an Alert' checkbox un-checked unless you want to *Live* to email a user each time an alert is raised. Click **Next**.
7. On the final page of the wizard, check the summary. It should read 'Sessions longer than 00:15:00; departments: XYZ.' Click **Finish**.

The new trigger is displayed in the trigger list. When a member of the XYZ department browses for longer than 15 minutes without a break, an alert will be generated and displayed under the 'XYZ sessions > 15 mins' trigger in Live Status (see Live Status on page 67).



Cumulative Trigger Example

Monitoring requirement: Trigger an alert when members of a particular department have downloaded more than 5 MB of data in total, regardless of whether the downloaded resources are part of the same session.

Before you add this trigger, you need to ensure that the department you want to monitor has a department alias, and that all the members of the department have been added to it. You set up departments on the Departments tab in Aliases (About Departments on page 57).

To add this trigger:

1. Launch the Trigger Wizard, by selecting **Views | Triggers** from the main menu, and click the **Add new trigger** link in the Triggers task pad.
2. Proceed to the Trigger Type page. Select 'Cumulative trigger' and click **Next**.
3. On the Cumulative Trigger page, select check the checkbox next to 'Size'. Under 'Advanced Filtering', check the 'Departments' checkbox. Click **Next**.
4. On the Size page, check the checkbox next to 'Incoming', and enter the value '5' into the edit box. Select 'Megabytes' from the drop down list. Click **Next**.
5. On the Departments page, check the checkbox next to the departments you want to monitor. Only departments already defined on the Departments tab in Aliases are displayed here. For this example, we will call the department 'XYZ'. Click **Next**.
6. On the Trigger Properties page, give the trigger a descriptive name such as 'XYZ total downloads > 5MB'. Select a priority level from the drop down list, and ensure the 'Trigger is enabled' checkbox is checked. Leave the 'Send an email when this trigger generates an Alert' checkbox un-checked unless you want to *Live* to email a user each time an alert is raised. Click **Next**.
7. On the final page of the wizard, check the summary. It should read 'Incoming greater than 5 MB; departments: XYZ'. Click **Finish**.

The new trigger is displayed in the trigger list. When a member of the XYZ department downloads more than 5 MB of data, an alert will be generated and displayed under the 'XYZ total downloads > 5MB' trigger in Live Status (see Live Status on page 67).

Editing Triggers

You may need to edit an existing trigger to refine or expand the criteria for generating alerts.

For example, if a trigger is generating too many alerts, you may want to edit it so that it only applies to certain users or departments, or refine its criteria in some other way.

To edit a trigger:

1. In Live Configuration, select **View | Triggers** from the main menu, or select the Triggers Sidebar icon
2. Select the trigger that you want to edit from the list
3. Click the **Edit selected trigger** link in the Triggers task pad. This launches the Trigger Wizard, which guides you through the process of editing your trigger (see Using the Trigger Wizard on page 17).

The edited trigger is displayed in the triggers list. You can also delete any triggers that are no longer required (see Deleting Triggers on page 30).

Note:

You cannot change the 'type' of trigger by editing it, such as changing it from



a Single Hit trigger to a Session trigger. If you want to do this, you will need to add a new trigger of the type you want and delete the old one.

Deleting Triggers

You may need to delete triggers when they are no longer required.

For example, if a trigger is not raising any useful alerts, you can delete it from the list.

To delete a trigger:

1. In Live Configuration, select **View | Triggers** from the main menu, or select the Triggers Sidebar icon
2. Select the trigger that you want to delete in the list
3. Click the **Delete selected trigger** link in the Triggers task pad
4. Click **Yes** on the confirmation dialog to delete the Trigger

The trigger is no longer displayed in the triggers list.

It is recommended that you save your triggers before deleting, in case you need to recover them later (see Saving Triggers on page 30).

If you do not want to see the alerts generated by a specific trigger, but you do not want to delete the trigger, you can disable the trigger as an alternative. Any disabled triggers will not generate any alerts until they are enabled (see Disabling Triggers on page 31).

Deleting All Triggers

WebSpy Live enables you to delete all your triggers at the one time.

To delete all your triggers:

1. In Live Configuration, select **Views | Triggers** from the main menu or click the Triggers Sidebar icon
2. Click the **Delete all triggers** link on the Triggers task pad. A confirmation dialog is displayed
3. Click **Yes** on the confirmation dialog to delete all your trigger

It is recommended that you save your Triggers before deleting, in case you need to recover them later (see Saving Triggers on page 30). You can also delete individual triggers one at a time.(see Deleting Triggers on page 30)

Saving Triggers

Triggers are automatically saved each time you exit *Live*, however you can manually save your triggers at any time. By default, triggers are saved in the location specified in Location Options (see Location Options on page 87).

To save your triggers:

1. In Live Configuration, select **Views | Triggers** from the main menu, or click the Triggers Sidebar icon
2. Click the **Save current triggers** link on the Management task pad
3. Type a name for the Triggers list in the 'File name' edit box
4. Click the **Save** button



All Triggers lists are saved with the extension *.Triggers. Once you have saved a Triggers list, you can quickly open this list in *Live* when required.

Your Triggers list is automatically saved when you exit *Live*.

Creating Triggers Lists

WebSpy Live comes with a list of default triggers to alert you to common browsing scenarios, however you can set up your own Triggers lists if the default triggers do not meet your organization's monitoring requirements.

To create a new Triggers list:

1. Select **Views | Triggers** from the main menu, or click the Triggers Sidebar icon
2. Click on the **Delete all triggers** link in the Triggers task pad. A confirmation dialog will be displayed.
3. Click **Yes** to clear the existing Triggers list
4. Add triggers to the new list (see Adding Triggers on page 16)

Your Triggers list is automatically saved when you exit *Live*. It is a good idea to save your existing Triggers list before creating a new list, in case you want to recover them later.

Note:

It may be easier to edit your existing Triggers list rather than creating a new list.

Opening Triggers

WebSpy Live enables you to open triggers that have been previously saved (see Saving Triggers on page 30). This is useful if you want to recover a list of triggers you backed up earlier.

To open a Triggers list:

1. In *Live Configuration*, select **Views | Triggers** from the main menu, or click on the Triggers Sidebar icon
2. Click the **Open existing triggers** link on the Triggers task pad to launch the Open dialog
3. Select a Triggers list to open. All Triggers lists have the file extension *.Triggers
4. Click on the **Open** button

Triggers lists are saved with the extension *.Triggers. *Live* stores triggers in the location specified in Locations Options (see Location Options on page 87).

Your Triggers list is automatically saved when you exit *Live*

Disabling Triggers

WebSpy Live enables you to enable and disable your triggers at any time. When triggers are disabled, they do not raise alerts. This is useful when you want to stop alerts from a specific trigger without deleting the trigger.



To disable a trigger:

1. In Live Configuration, select **Views | Triggers** from the main menu, or click the Triggers Sidebar icon
2. Select the enabled trigger you want to disable. Enabled triggers show 'Enabled' in the status column.
3. Click the **Disable selected trigger** link in the Triggers task pad

The trigger is displayed as 'Disabled' in the status column and its color turns to light gray. You can also enable and disable triggers from Live Status (see Enabling Triggers from Live Status on page 76, and Disabling Triggers from Live Status on page 76).

Enabling Triggers

WebSpy Live enables you to enable and disable your triggers at any time. When triggers are disabled, they do not raise alerts (see Disabling Triggers on page 31). You can manually enable any disabled triggers.

To enable a trigger:

1. In Live Configuration, select **Views | Triggers** from the main menu, or click the Triggers Sidebar icon
2. Select the disabled trigger you want to enable. Disabled triggers are displayed in light gray, and show 'Disabled' in the status column
3. Click the **Enable selected trigger** link in the Triggers task pad

The trigger is displayed as 'Enabled' in the status column. You can also enable and disable triggers from Live Status (see Enabling Triggers from Live Status on page 76, and Disabling Triggers from Live Status on page 76).

Changing a Trigger's Priority

Each trigger is assigned a priority level, to indicate the importance of the alert. You can change this priority level at any time.

To change a trigger's priority level:

1. In Live Configuration, select **View | Triggers** from the main menu, or select the Triggers Sidebar icon
2. Select the trigger that you want to change the priority for
3. Click the **Edit selected trigger** link in the Triggers task pad. This launches the Trigger Wizard, which guides you through the process of editing your trigger (see Using the Trigger Wizard on page 17)
4. Proceed to the Trigger Properties page of the Trigger Wizard without making any selections, by clicking the **Next** button on each page
5. On the Trigger Properties page, select the desired priority of the trigger from the 'Priority' drop down list
6. Proceed to the final page of the Trigger Wizard and click **Finish**

The trigger's new priority is displayed in the Priority column, and any new alerts that the trigger raises will be displayed in the color of that priority (see Alerts on page 68).



Profiles

About Profiles

Profiles are used to categorize the Internet resources accessed by members of your organization.

A profile is collection of keywords that are matched against the names of sites and downloaded resources. *WebSpy Live* looks along the length of each hit for any include keywords. As soon as it finds a keyword, it will check if the hit matches any exclude keywords for that profile. If there are no exclude keywords, then the hit is assigned to that profile. If there is an exclude keyword, the hit is checked for keywords in the next profile.

For example, if a site name contains 'computershop', it will be assigned to the computer profile instead of the shop profile, since the keyword 'computer' comes before the keyword 'shop', assuming that the rest of the URL has no exclude keywords from the computer profile.

A hit that does not contain any include keywords will be assigned to the Miscellaneous profile. Approximately 20-35% of hits will be assigned to this profile using the default profiles that come with *Live*. Fewer hits are assigned to the Miscellaneous profile as you develop and refine your own profiles.

Profiles can be used when defining triggers to alert you to specific types of Internet or email activity (see About Triggers on page 15).

For example, if you want to be alerted when someone in your organization sends email to a particular client, or visits their web site, you can set up a profile called 'Client' with the client's name as an 'include' keyword, then set up a trigger based on the 'Client' profile.

Live comes with a list of profiles already defined with common keywords. You can add, edit or delete profiles and include and exclude keywords to suit your organization's Internet usage patterns (see Adding Profiles on page 33, Editing Profiles on page 36, and Deleting Profiles on page 37).

Profiles are grouped together in a Profiles list that is saved with the extension *.Profiles (see Saving Profiles Lists on page 38). You can create your own lists, and you can import and export them to a CSV file using the options in the Special task pad (see Importing Profiles Lists on page 39, and Exporting Profiles Lists on page 39).

Adding Profiles

You can add profiles and keywords to suit your organization's Internet usage patterns. You can add profiles to an existing Profiles list such as the default list that comes with *WebSpy Live*, or add them to a new blank list (see Deleting All Profiles).

You can then use these profiles when creating triggers to alert you of certain types of Internet browsing or network activity (see About Triggers on page 15).

To add a new profile:

1. In Live Configuration, select **Views | Profiles** from the main menu, or click the Profiles Sidebar icon



2. Click the **Add a new profile** link in the Profiles task pad. This launches the Profile dialog.
3. Enter a name and description for the new profile into the appropriate edit boxes
4. Use the 'Include' or 'Exclude' tabs of the dialog to add keywords to the profile, so that hits containing the keywords are either assigned to or excluded from the profile. For more information on adding keywords, see Adding Keywords on page 34.
5. When you have finished adding keywords, click **OK**

You can edit any of your profiles at any time, and add, edit and delete keywords (see Editing Profiles on page 36). You can use the 'Add to profile' function in Live Summary to add keywords to profiles and create new profiles (see Adding Keywords to Profiles on page 83).

Adding Keywords

You need to maintain and update your profiles on a regular basis so that they accurately reflect Internet and email activity. This involves adding keywords as you come across them to the appropriate profile.

For example, if you notice that a user has browsed to a site called `www.computerproducts4you.com`, you can add the keyword 'computerproducts4you' to the Information Technology profile, or the Finance and Shopping profile. Alternatively, you could simply add the keyword 'computer' to the Information Technology profile.

Each of your defined Profiles has an 'include' keywords list. If a hit contains a word that matches any keywords in a profile's include keyword list, the hit will be assigned to that profile. If a hit contains a word that matches any keywords in a profile's exclude keyword list, the hit will not be placed in the profile, even if it matches one of the profiles include keywords

You can add include or exclude keywords to any profile from the Profile dialog.

To add keywords using the Profile dialog:

1. Launch the Profile dialog either by adding a new profile or editing an existing profile (see Adding Profiles on page 33, and Editing Profiles on page 36)
2. Click the appropriate tab depending on whether you wish to add the keyword(s) to the profile's include or exclude list
3. Click the **Add** button on the toolbar
4. Enter the name of the keyword and click **OK**. The new keyword will be displayed in the list
5. Repeat steps 3 and 4 until all necessary keywords have been added
6. Click **OK**

Hint:

To add a number of keywords at once, from another source such as a text document, copy the list of keywords (each on a separate line), click either the 'Include' or 'Exclude' tabs on the Profile dialog, and click the **Paste** button on the toolbar. For tips on defining your keywords, see Keyword Tips.

You can also add keywords to profiles, and create new profiles using the 'Add to profile' function in Live Summary.

Note:

Changes to your profiles are only applied to the new hits coming in from your log files. Hits that have already been processed by *Live* do not trigger alerts if they match the keywords of a recently updated profile.



Keyword Tips

Adding keywords to your profiles is an important part of ensuring that they accurately reflect your organization's browsing behaviour.

Here are some tips to help you define keywords that efficiently assign hits to the correct profile:

- **Review hits that are not assigned to a profile**

It is a good idea to set up a trigger based on the Miscellaneous profile. This trigger is likely to create many alerts, however it will alert you to browsing activity that does not get assigned to a profile. You can then use this information to update your profiles.

You can also use *WebSpy Analyzer* to drilldown into the Miscellaneous profile and add keywords to the appropriate profiles. If the 'Keep Profiles and Aliases synchronized between WebSpy applications' checkbox in General Options is checked in both *Analyzer* and *Live*, the changes made to your profiles in *Analyzer* will also be reflected in *Live*.

- **Choose your keywords wisely**

The more keywords you have defined, the more time it takes for *Live* process each hit. It is therefore a good idea to keep your keywords general enough to capture the appropriate sites, and specific enough not include the wrong sites. You should try and define your keywords so that you achieve a desirable balance between performance and accurate reporting.

For example, instead of adding `www.webspy.com` as a keyword, just add the keyword `webspy`, as 'webspy' is specific enough to capture all the desired web sites. This way other sites such as `www.webspy.co.uk` will also be assigned to the profile.

- **Avoid small keywords**

Be wary of adding small words that may appear within bigger words.

For example, the hit `www.lala.com/smallgun.gif` would be assigned to the profile with `mall` rather than the profile with `gun`.

- **Take language into account**

English keywords will not correctly match hits for non-English web pages. Therefore, when browsing non-english sites, you would expect most web pages to end up in the wrong profile, unless you have specified non-english keywords for your profiles.

Editing Keywords

You need to maintain and update your profiles on a regular basis so that they accurately reflect Internet and email activity. This may involve editing existing include or exclude keywords so that they more efficiently categorize types of browsing.

For example, if you have a keyword `'computerproducts4you'` in the Information Technology profile, you can change the keyword to `'computer'`. This ensures that all hits that contain the word `'computer'` are categorized into the Information Technology profile.

To edit a keyword:

1. Launch the Profile dialog either by adding a new profile or editing an existing profile



2. Click the appropriate tab depending on whether you wish to edit keyword(s) in the profile's include or exclude list
3. Select the keyword that you want to edit from the list
4. Click the **Edit** button on the toolbar
5. Type the desired keyword into the edit box
6. Click **OK**

Hint:

You can edit a keyword quickly by right-clicking the keyword and selecting **Edit** from the pop-up menu.

Note:

Changes to your profiles are only applied to the new hits coming in from your log files. Hits that have already been processed by *Live* do not trigger alerts if they match the keywords of a recently updated profile.

Deleting Keywords

You need to maintain and update your profiles on a regular basis so that they accurately reflect Internet and email activity. This may involve deleting keywords from a profile's include or exclude keyword list if they are inappropriately assigning hits to a profile.

To delete keywords from a profile:

1. Launch the Profile dialog either by adding a new profile or editing an existing profile
2. Click the appropriate tab depending on whether you wish to delete keyword(s) from the profile's include or exclude list
3. Select the keyword that you want to delete from the list
4. Click the **Delete** button on the toolbar
5. Repeat steps 3 and 4 until all necessary keywords have been deleted
6. Click **OK**

Hint:

You can delete a keyword quickly by right-clicking the keyword and selecting **Delete** from the pop-up menu.

Editing Profiles

You can edit the properties and keywords of a profile at any time by following the steps below. It is a good idea to save your Profiles list before you make any major changes in case you need to recover your profiles later (see Saving Profiles Lists on page 38).

To edit the properties of a profile:

1. In Live Configuration, select **Views | Profiles** from the main menu, or click the Profiles Sidebar icon
2. Select the profile you want to edit in the list and click the **Edit selected profile** link in the Profiles task pad. This launches the Profile dialog.
3. On the Profile dialog, you can:
 - Change the profile's name and description by typing the new name or description into the appropriate edit boxes
 - Add, edit, or delete the profile's include or exclude keywords using the appropriate tabs of the dialog.



4. Once you have finished, click **OK**

Note:

Changes to your profiles are only applied to the new hits coming in from your log files. Hits that have already been processed by *Live* do not trigger alerts if they match the keywords of a recently updated profile.

Hint:

You can also add keywords to profiles, and create new profiles using the 'Add to profile' function in Live Summary (see Adding Keywords to Profiles on page 83).

When dealing with large amounts of information, you may prefer to export your profiles to a CSV file, edit the file in a program such as Microsoft® Excel, and then import the edited file back into *Live* (see Exporting Profiles Lists on page 39, and Importing Profiles Lists on page 39).

Deleting Profiles

You can delete individual profiles from your Profiles list when they are no longer required. It is always a good idea to save your Profiles list before deleting any profiles, in case you need to recover them later.

To delete a profile from the Profiles list:

1. In Live Configuration, select **Views | Profiles** from the main menu, or click the Profiles Sidebar icon
2. Select the name of the profile you want to delete and click the **Delete selected profile** link in the Profiles task pad
3. Click **Yes** on the confirmation dialog to delete your profiles

You can also delete all profiles at once (See Deleting All Profiles on page 37).

Hint:

To you can delete a profile quickly by right-clicking the keyword and selecting **Delete** from the pop-up menu.

Deleting All Profiles

You can delete your list of profiles if you want to start a new list. Deleting all profiles essentially closes your active Profiles list and presents you with a blank list to which you can add new profiles.

To delete your profiles:

1. In Live Configuration, select **Views | Profiles** from the main menu, or click the Profiles Sidebar icon
2. Click the **Delete all profiles** link in the Profiles task pad
3. Click **Yes** on the confirmation dialog to delete your profiles

You can then open an existing Profiles list (see Opening Profiles Lists on page 38), or add new profiles to the blank list (see Adding Profiles on page 33).

Your Profiles list is automatically saved each time you exit *Live*.



Saving Profiles Lists

WebSpy Live enables you to save and open Profiles lists so that you can backup and transport your profiles.

For example, if you install Live on another computer, you can save your old Profiles and open them within Live on the other computer.

To save a Profiles list:

1. In Live Configuration, select **Views | Profiles** from the main menu, or click the Profiles Sidebar icon
2. Click the **Save current profiles** link in the Management task pad to open the Save Profiles dialog
3. Select the correct file name from the dialog, or type the new name into the File name box
4. Click **Save**. The file will be saved with an extension of *.Profiles

Your Profiles list is automatically saved each time you exit *Live*.

Creating Profiles Lists

WebSpy Live comes with a list of default profiles to help categorize common Internet browsing, however you can set up your own Profiles Lists if the default profiles do not meet your organization's criteria.

To create a new Profiles list:

1. In Live Configuration, select **Views | Profiles** from the main menu, or click the Profiles Sidebar icon
2. Click on the **Delete all profiles** link in the Profiles task pad. A confirmation dialog will be displayed
3. Click **Yes** to clear the existing Profiles list
4. Add new profiles to the new list (see Adding Profiles on page 33)

Your profiles list is automatically saved when you exit Live. It is a good idea to save your existing profiles list before creating a new list, in case you want to recover them later.

Note:

It may be easier to edit your existing Profiles list rather than creating a new list from scratch.

Opening Profiles Lists

WebSpy Live enables you to save and open Profiles lists so that you can backup and transport your profiles.

For example, if you install Live on another computer, you can save your old Profiles and open them within Live on the other computer.

To open a saved Profiles list:

1. In Live Configuration, select **Views | Profiles** from the main menu, or click the Profiles Sidebar icon
2. Click the **Open existing profiles** link in the Management task pad to open the Open Profiles dialog
3. Select the required *.Profile file from the Open dialog, and click **Open**



4. If you have not cleared the previous Profiles list, a confirmation dialog appears asking if you want to merge the two lists:
 - Click **Yes** to merge the two lists
 - Click **No** to clear the previous list and open the new list
 - Click **Cancel** to revert to the previous list

Note:

You must ensure that the same keyword does not exist in more than one profile, otherwise hits may not be appropriately assigned to the correct profile.

Exporting Profiles Lists

Live enables you to export your Profiles list to a CSV file which can be loaded in Microsoft® Excel or any text editor.

This functionality enables you to view all your profiles and keywords in the one file. It is also useful for editing your profiles and keywords more efficiently when dealing with large amounts of information.

To export a Profiles list:

1. In Live Configuration, select **Views | Profiles** from the main menu, or click the Profiles Sidebar icon
2. Click the **Export to a CSV file** link on the Advanced task pad to open the Save Profiles dialog
3. Select a location and type a file name for the CSV file in the Save As dialog
4. Click **Save**

Once you have exported your Profiles list, you can edit it using Microsoft® Excel, and then import the list back into *Live* (see Importing Profiles Lists on page 39).

Importing Profiles Lists

Once you have exported a Profiles list to a CSV file using the export function (see Exporting Profiles Lists on page 39), you can import the CSV file back into *Live*.

Importing and exporting to a CSV file is useful for efficiently editing profiles and keywords when dealing with large amounts of information.

To import a Profiles list from a CSV file:

1. In Live Configuration, select **Views | Profiles** from the main menu, or click the Profiles Sidebar icon
2. Click the **Import from a CSV file** link on the Advanced task pad to open the Import Profiles dialog
3. Find and select the CSV file
4. Click **Open**

The CSV file needs to be formatted correctly for the import to work. The easiest way to discover how the CSV file should be formatted is to export an existing Profiles list (see Exporting Profiles Lists on page 39) and view the resulting CSV file.

The figure below illustrates how information in a CSV file should be formatted for the import process to work correctly.



	A	B	C	D	E
1	Profile 1 Name				
2	Profile 1 Description				
3	Includes Keyword 1	Includes Keyword 2	Includes Keyword 3	Includes Keyword 4	
4	Excludes Keyword 1	Excludes Keyword 2	Excludes Keyword 3	Excludes Keyword 4	
5	Profile 2 Name				
6	Profile 2 Description				
7	Includes Keyword 1	Includes Keyword 2	Includes Keyword 3	Includes Keyword 4	
8	Excludes Keyword 1	Excludes Keyword 2	Excludes Keyword 3	Excludes Keyword 4	
9					

Layout of a Profiles list in a CSV file, displayed in Microsoft® Excel

The Miscellaneous Profile

If a hit contains no keywords, it is assigned to the Miscellaneous profile. Approximately 25-30% of hits will end up in this profile using *WebSpy Live's* supplied profile keywords.

The actual proportion depends on how members of your organization use your web resources, and whether you have customized your profiles to suit your organization.

Having a large number of hits in the Miscellaneous Profile does not mean that *Live* is not functioning properly. What it does mean is that you need to update your profile keywords, so that hits are assigned to the appropriate profile rather than to the Miscellaneous profile.

One way of reducing the hits in your Miscellaneous profile is by adding a trigger based on the Miscellaneous profile to alert you to sites/recipients that are not being categorized into a defined profile (see About Triggers on page 15). You can then use this information to update your profiles with appropriate keywords.

Note:

Changes to your profiles are only applied to the new hits coming in from your log files. Hits that have already been processed by *Live* do not trigger alerts if they match the keywords of a recently updated profile.

It is important to note that the more keywords you have defined, the longer *Live* takes to process each hit. It is therefore a good idea to keep your keywords general enough to capture the appropriate sites, and specific enough to not include the wrong sites. You should try and define your keywords so that you achieve a desirable balance between performance and accurate reporting. For more information on defining keywords, see Keyword Tips on page 35.

Aliases

About Aliases

WebSpy Live uses Aliases to group and represent data items in your log files such as users, IP addresses, and file types in more meaningful ways.

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'.

Aliases are used to help define triggers (see About Triggers on page 15), and for filtering your inputs (About Inputs on page 6)

For example, you can define a trigger that alerts you when a certain user browses a particular web site. To do this, you need to set up a user name alias that groups all instances of the user, such as IP addresses, email addresses and computer names. You then need to create a site name alias that groups all instances of the web site, such as IP addresses and URLs. Then you can create a single hit trigger and select the user name and site name. For more information on setting up triggers, see Using the Trigger Wizard on page 17.

Aliases are configured using the Aliases screen of Live Configuration, which is accessed by selecting **Views | Aliases** from the main menu, or clicking the Aliases Sidebar icon (see Live Configuration on page 5).

There are four types of Aliases:

- **User names**
User name aliases can represent IP addresses, email addresses and computer names, by an actual user name such as 'Joe Citizen'. This user name is then used to represent all the Internet and network activity of this user in Live Status and Live Summary. For more information, see User Names on page 42.
- **Site names**
Site names enable you to represent IP address and URLs, such as 'http://www.webspy.com', by simplified site names, such as 'WebSpy'. Defined site names can then be used in defining triggers based on the 'Site name' alias. For more information, see Site Names on page 48.
- **File types**
File types enable you to group file extensions, such as 'htm', 'xml', 'css', into a representative name, such as 'Web Document'. Defined File types can then be used in defining triggers based on the 'File type' alias. For more information, see File types on page 53.
- **Departments**
You can group users of your network resources into departments such as 'Accounts', or 'Management'. Department aliases can be selected when defining triggers to alert you to the Internet and network activity of members of a department. Departments is the only alias type available for filtering your inputs. For more information, see About Departments on page 57.

You can configure each type of alias using the appropriate tab on the Aliases screen.

Live comes with a list of default file type aliases, however you need to create your own user names, site names, and departments suit your organization.

The 'User names' and 'Departments' tab have an unassigned list that displays all current users of your network that are not assigned to a User name or Department alias. The unassigned list enables you to drag and drop unassigned users to an appropriate alias.

You can quickly add users to user name and department aliases from Live Status, by right-clicking a user and selecting **Add to alias...** from the pop-up menu (see Adding Users to User names on page 75 and Adding Users to Departments on page 75). You can also add Users to user name and department aliases, and URLs to site name aliases from Live Summary (see Adding Users or Sites to Aliases on page 83).



Each list of aliases can be saved to a file for backup and recovery, as well as for transporting your aliases to other licences of *Live* that you may be running.

You can also export and import aliases to and from a CSV file for efficient editing of large amounts of data. This is also useful for transferring your aliases to *WebSpy Analyzer*.

User Names

About User Names

User name aliases enable you to represent IP addresses, email addresses and computer names, by an actual user name such as 'Joe Citizen'. This user name is then used to represent all the Internet and network activity of this user in Live Status and Live Summary (see Live Status on page 67, and Live Summary on page 79).

You can use user names when defining triggers to alert you to the browsing activity of specific users.

For example, you can create a hit-based trigger called 'Watch List'. When defining this trigger, you can select any of the user names defined on the 'User name' tab of the Aliases screen. You will then be alerted when these users browse the Internet.

You can add, edit and delete user names on the 'User names' tab of the Aliases screen in Live Configuration.

You can also import and export your User name aliases to a CSV file using the links in the Advanced task pad. This is useful for importing and exporting your user name aliases to and from *WebSpy Analyzer*, and for editing large numbers of user names using third party software such as Microsoft® Excel (see Importing User Names from CSV on page 47 and Exporting User Names to CSV on page 47).

Any changes made to your user names are only applied to new log data.

About User Names

User name aliases enable you to represent IP addresses, email addresses and computer names, by an actual user name such as 'Joe 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 use user names when defining triggers to alert you to the browsing activity of specific users (see About Triggers on page 15).

For example, you can create a hit-based trigger called 'Watch List'. When defining this trigger, you can select any of the user names defined on the 'User name' tab of the Aliases screen. You will then be alerted when these users browse the Internet.

You can add, edit and delete user names on the 'User names' tab of the Aliases screen in Live Configuration.

You can also import and export your User name aliases to a CSV file using the links in the Advanced task pad. This is useful for importing and exporting your User name aliases to and from *WebSpy Analyzer*, and for editing a large number



of user names using third party software such as Microsoft® Excel (see Importing User Names from CSV on page 47 and Exporting User Names to CSV on page 47).

Any changes made to your user names are only applied to new log data.

Adding User Names

You can add user name aliases to represent users in Live Status and Live Summary more meaningfully, and they can be used when defining user based triggers (see About Triggers on page 15).

To add a user name:

1. In Live Configuration, select **View | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'User names' tab
3. Click the **Add new user name** link in the User names task pad. This launches the New Name dialog
4. Type the name that you want to represent data into the 'Name' edit box. For example, if you want to represent an IP address with the name 'John', type 'John' into the 'Name' edit box
5. Click the **Add** button on the toolbar to launch the New dialog
6. Type in the name of the item (such as IP and email addresses) that you want to add to the user names alias, then click **OK** to close the dialog
7. Repeat steps 5 and 6 until you have added all necessary items to the user names alias. You can also add items later using the unassigned list, Live Status and Live Summary.
8. Click **OK**

The new user name is displayed in the aliases list. You can edit and delete any user name aliases in this list (see Editing User Names on page 44 and Deleting User Names on page 45).

Hint:

To add a number of users to a user name alias at the one time, you can paste a list of users from another application, like Microsoft® Word. Copy the users (each on a separate line), then right-click in the sites list and select 'Paste' from the pop-up menu that is displayed.

Hint:

You can use wildcards when adding users to a user name alias to reduce the number of items you need to add. For more information, see Using Wildcards in Aliases on page 66.

Using the Unassigned List

To the right of the 'User names' tab is the Unassigned list. It displays all users that are not currently assigned to an alias. You can assign any of these users to the appropriate user name alias.

To add an unassigned user to a user name alias:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'User names' tab
3. Select the user in the Unassigned list. You can use the 'Find' function at the top of the Unassigned list to search for keywords in the list. You can also



select more than one user by holding down the <Ctrl> and <Shift> keys when selecting.

4. Drag the user to the appropriate user name alias in the aliases list

You can also add unassigned users to user names from Live Status and Live Summary (see Adding Users to User names on page 75 and Adding Users or Sites to Aliases on page 83).

You can resolve any IP addresses in your Unassigned list to more meaningful names to help you determine which user name alias they should be assigned to (see Resolving IP Addresses on page 44).

Resolving IP Addresses

WebSpy Live enables you to resolve any user IP addresses that are displayed in the Unassigned List (see Using the Unassigned List on page 43) to more recognizable names that you can then assign to the appropriate user name alias.

To resolve unassigned IP addresses:

1. In Live Configuration, select **Views | Aliases** from the main menu, or click the Aliases sidebar icon
2. Click the 'User names' tab
3. Click the **Resolve IP addresses** link on the Advanced task pad

Live will contact your Domain Name System (DNS) server to attempt to find out the name of each unassigned IP address. This may take some time. If *Live* cannot contact the server, or if the server does not have a record for the IP address, the IP address will remain unchanged in the Unassigned list.

Note:

Your computer must have an active Internet connection for this to work.

Resolving IP addresses may take some time depending on how many unassigned IP addresses you have in the Unassigned list. You can stop the process by clicking the **Stop** button at the top of the Aliases screen.

Editing User Names

Once you have added user name aliases (see Adding User Names on page 43), you need to maintain them. The most common maintenance task is adding new instances of a user, such as new email addresses or computer names, to the user name alias. You can also edit and delete items assigned to a user name.

To edit a user name:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'User names' tab
3. Select the user name that you want to edit in the list
4. Click the **Edit selected user name** link in the User names task pad. This launches the Edit dialog. On this dialog you can change the name of the alias, add items, edit existing items, or delete existing items from the alias.
 - To change the name of the alias:
Type the new user name alias into the 'Name' edit box
 - To add items to the alias:
Click the **Add** button, type the name of the new item into the New dialog and click **OK**



- To edit an existing item:
Select the item in the list that you want to edit, click the **Edit** button, type the new item into the New dialog and click **OK**
- To delete an existing item:
Select the item in the list that you want to delete and click the **Delete** button

5. Click **OK**

The edited user name will be displayed in the aliases list. You can also delete any user name aliases that are no longer required (see Deleting User Names on page 45).

Hint:

An easy way of adding an instance of a users (such as an email or IP address) that is not currently assigned to a user name alias is by using the Unassigned list. You can also add items to user name aliases from Live Status and Live Summary (see Adding Users to User names on page 75 and Adding Users or Sites to Aliases on page 83)

Deleting User Names

You may need to delete user names when they are no longer required.

For example, if an employee leaves your organization, you can delete them from the list of user name aliases.

To delete a user name:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'User names' tab
3. Select the user name that you want to delete in the list
4. Click the **Delete selected user name** link in the User names task pad
5. Click **Yes** on the confirmation dialog to delete the user name

The user name is no longer displayed in the aliases list. Any items previously assigned to the user name alias will be represented in their original form in Live Status and Live Summary.

You can also edit any user name aliases in the list (see Editing User Names on page 44).

Deleting All User Names

Deleting all user names closes your active user names list and presents you with a blank list, to which you can add new user names.

To delete all user names:

1. In Live Configuration, select **Views | Aliases** from the main menu, or click the Aliases Sidebar icon
2. Click the 'User names' tab
3. Click the **Delete all user names** link in the User names task pad
4. Click **Yes** on the confirmation dialog to delete all your user names

You can then open an existing user names list (see Opening User Names on page 46), or add new user names (see Adding User Names on page 43).

Your user names list is automatically saved when you exit Live.



Creating User Names Lists

WebSpy Live enables you to create a new list of user names.

To create a new user names list:

1. In Live Configuration, select **Views | Aliases** from the main menu, or click the Aliases Sidebar icon
2. Click the 'User names' tab
3. Click the **Delete all user names** link in the User names task pad. A confirmation dialog will be displayed
4. Click **Yes** to delete the existing user names list
5. Add new user names to the new list (see Adding User Names on page 43)

This user names list is automatically saved when you exit Live. It is a good idea to save your existing user names list before creating a new list, in case you want to recover them later.

Note:

It may be easier to edit your existing user names list rather than creating a new list.

Saving User Names

You can save your list of user names to a file, which you can open in *WebSpy Live* at any time. This enables you to back up your user names, and create separate lists of user names for different purposes. This can be useful if you monitor different log files at separate times.

To save a user names list:

1. In Live Configuration, select **Views | Aliases** from the main menu, or click the Aliases Sidebar icon
2. Click the 'User names' tab
3. Click on the **Save current user names** link on the Management task pad
4. Type a name for the user names list in the 'File name' edit box
5. Click the **Save** button

All user names lists are saved with the extension *.UserNames. Once you have saved a user names list, you can quickly open this list in *Live* when required (see Opening User Names on page 46).

The active user names list is automatically saved whenever you exit *Live* as Default.UserNames (See **Error! Reference source not found.** on page **Error! Bookmark not defined.**).

By default, *Live* stores user names in the location specified in Locations Options (see Location Options on page 87).

Opening User Names

WebSpy Live enables you to open a saved list of user names at any time. This is useful if you want to open a list of user names specific to a log file location you are monitoring.

To open a user names list:

1. In Live Configuration, select **Views | Aliases** from the main menu, or click the Aliases Sidebar icon
2. Click the 'User names' tab



3. Click the **Open existing user names** link on the Management task pad to launch the Open dialog
4. Select a user names list to open. All user names lists have the file extension *.UserNames.
5. Click on the **Open** button. If you have not cleared the previous user names list, a confirmation dialog appears asking if you want to merge your current user names list with the new list:
 - Click **Yes** to merge the two lists
 - Click **No** to clear the existing user names list and open the new list
 - Click **Cancel** to return to the current user names list

Note:

If the list you are opening contains some of the same user names as the current list, the user names are left in their original state. (I.e. the users in the current list will remain unchanged).

User names lists are saved with the extension *.UserNames. *Live* stores user names in the location specified in Locations Options (see Location Options on page 87).

When you exit *Live*, the User Names list you currently have open is saved to Default.UserNames (See **Error! Reference source not found.** on page **Error! Bookmark not defined.**).

Exporting User Names to CSV

WebSpy Live enables you to export your user names to a CSV file, which can be opened in Microsoft® Excel or any text editor.

This functionality enables you to view all user names in the one file. It is also useful for editing your user names more efficiently when dealing with large amounts of information. You can then import the edited CSV file back into *Live*.

To export your user names list:

1. In Live Configuration, select **Views | Aliases** from the main menu, or click the Aliases Sidebar icon
2. Click the 'User names' tab
3. Click on the **Export to a CSV file** link on the Advanced task pad
4. Type a name for the CSV file in the 'File name' edit box
5. Click the **Save** button

You can import CSV files back into *Live* as long as the information within the CSV file is formatted correctly (see Importing User Names from CSV on page 47).

Importing User Names from CSV

Once you have exported user names to a CSV file using the export function, you can import the CSV file back into *WebSpy Live*.

To import user names from a CSV file:

1. In Live Configuration, select **Views | Aliases** from the main menu, or click the Aliases Sidebar icon
2. Click the 'User names' tab
3. Click on the **Import from a CSV file** link on the Advanced task pad
4. Find and select the CSV file to import
5. Click **Open**



The CSV file needs to be formatted correctly for the import to work. The easiest way to discover how the CSV file should be formatted is to export your existing user names (see Exporting User Names to CSV) and view the resulting CSV file.

The figure below illustrates how information in a CSV file should be formatted for the import process to work correctly.

	A	B	C	D	E
1	User name 1	Data item 1	Data item 2	Data item 3	
2	User name 2	Data item 1	Data item 2	Data item 3	
3	User name 3	Data item 1	Data item 2	Data item 3	
4	... etc.				
5					

Figure 4: Layout of user names and their associated data items in CSV format

Site Names

About Site Names

Site name aliases enable you to represent IP addresses, and URLs, by an actual web site name such as 'Hotmail' or 'WebSpy'.

You use site names when defining triggers to alert you when users browse to specific sites (see About Triggers on page 15).

For example, you can create a single hit trigger called 'Black List' that alerts you when users browse to specific sites. When defining this trigger, you can select any of the site names defined on the 'Site name' tab of the Aliases screen. You will then be alerted when users browse to these sites.

You can add, edit and delete site names on the 'Site names' tab of the Aliases screen in Live Configuration.

You can also import and export your site name aliases to a CSV file using the links in the Advanced task pad. This is useful for importing and exporting your site name aliases to and from *WebSpy Analyzer*, and for editing large numbers of site names using third party software such as Microsoft© Excel (see Importing Site Names from CSV on page 52 and Exporting Site Names to CSV on page 52).

Adding Site Names

You need to add site name aliases if you want to define triggers that alert you when specific web sites are being viewed by users (see About Triggers on page 15).

As web sites can have several different addresses, site name aliases can save you time maintaining site based triggers.

For example, you can define the site name alias 'WebSpy' and add to it the items `www.webspy.com`, `www.webspy.co.uk`, and `www.webspy.com.au`. All you need to do when defining a site based trigger is select 'WebSpy' on the appropriate page of the Trigger Wizard.



To add a site name:

1. In Live Configuration, select **Views | Aliases** from the main menu, or click the Aliases Sidebar icon
2. Click the 'Site names' tab
3. Click the **Add new site name** link in the Site names task pad. This launches the New Name dialog
4. Type the site name into the 'Name' edit box. For example, if you want to represent `http://www.webspy.com` by the word 'WebSpy', type 'WebSpy' into the 'Name' edit box
5. Click the **Add** button on the toolbar to launch the New dialog
6. Type in the name of the item (such as an IP address or URL) that you want to add to the site name alias, then click **OK** to close the dialog
7. Repeat steps 5 and 6 until you have added all necessary items to the site name alias
8. Click **OK**

The new site name is displayed in the aliases list. You can edit and delete any site name aliases in this list (see Editing Site Names on page 49 and Deleting Site Names on page 50).

Hint:

To add a number of sites to a site name alias at the one time, you can paste a list of sites from another application, like Microsoft® Word. Copy the sites (each on a separate line), then right-click in the users list and select 'Paste' from the pop-up menu that is displayed.

Hint:

You can use wildcards when adding sites to a site name alias to reduce the number of items you need to add. For more information, see Using Wildcards in Aliases on page 66.

Editing Site Names

Once you have added site name aliases, you need to maintain them. The most common maintenance task is adding new instances of a site, such as URLs, to the site name alias. You can also edit and delete items assigned to a site name.

For example, if the site name alias called 'WebSpy' is used to represent `www.webspy.com`, you may also need to add `www.webspy.co.uk` to the alias.

To edit a site name:

1. In Live Configuration, select **Views | Aliases** from the main menu, or click the Aliases Sidebar icon
2. Click the 'Site names' tab
3. Select the site name that you want to edit in the list
4. Click the **Edit selected site name** link in the site names task pad. This launches the Edit dialog. On this dialog you can change the name of the alias, add items, edit existing items, or delete existing items from the alias.
 - To change the name of the alias:
Type the new site name alias into the 'Name' edit box
 - To add items to the alias:
Click the **Add** button, type the name of the new item into the New dialog and click **OK**
 - To edit an existing item:
Select the item in the list that you want to edit, click the **Edit** button, type the new item into the New dialog and click **OK**



- To delete an existing item:
Select the item in the list that you want to delete and click the **Delete** button

5. Click **OK**

The edited site name will be displayed in the aliases list. You can also delete any site name aliases that are no longer required (see Deleting Site Names on page 50).

You can also add items, such as URLs and IP addresses, to site name aliases from Live Summary (see Adding Users or Sites to Aliases on page 83).

Deleting Site Names

You may need to delete site names when they are no longer required.

For example, if a web site is no longer active you can delete it from the list of site name aliases.

To delete a site name:

1. In Live Configuration, select **Views | Aliases** from the main menu, or click the Aliases Sidebar icon
2. Click the 'Site names' tab
3. Select the site name that you want to delete in the list
4. Click the **Delete selected site name** link in the Site names task pad
5. Click **Yes** on the confirmation dialog to delete the site name.

The site name is no longer displayed in the aliases list. You can also edit any site name aliases in the list (see Editing Site Names on page 49).

Deleting All Site Names

Deleting all site names closes your active site name list and presents you with a new blank list, to which you can add new site names.

To clear your site names:

1. In Live Configuration, select **Views | Aliases** from the main menu, or click the Aliases Sidebar icon
2. Click the 'Site names' tab
3. Click the **Delete all site names** link in the Site names task pad
4. Click **Yes** on the confirmation dialog to delete the site name

You can then open an existing site names list (see Opening Site Names on page 51), or add new site names (see Adding Site Names on page 48).

Your site names list is automatically saved when you exit *Live*

Creating Site Names Lists

WebSpy Live enables you to create a new list of site names.

To create a new site names list:

1. In Live Configuration, select **Views | Aliases** from the main menu, or click the Aliases Sidebar icon
2. Click the 'Site names' tab



3. Click the **Delete all site names** link in the Site names task pad. A confirmation dialog will be displayed (see Deleting All Site Names).
4. Click **Yes** to clear the existing site names list
5. Add new site names to the new list (see Adding Site Names on page 48)

This site names list is automatically saved when you exit Live. It is a good idea to save your existing site names list before creating a new list, in case you want to recover them later.

Note:

It may be easier to edit your existing site names list rather than creating a new list.

Saving Site Names

You can save your list of site names to a file, which you can open in *WebSpy Live* at any time. This enables you to back up your site names.

To save a site names list:

1. In Live Configuration, select **Views | Aliases** from the main menu, or click the Aliases Sidebar icon
2. Click the 'Site names' tab
3. Click the **Save current site names** link in the Management task pad
4. Type a name for the site names list in the 'File name' edit box
5. Click the **Save** button

All site names lists are saved with the extension *.SiteNames. Once you have saved a site names list, you can quickly open this list in *Live* when required (see Opening Site Names on page 51).

Your site names list is automatically saved when you exit *Live*.

By default, *Live* stores site names in the location specified in Locations Options (see Location Options on page 87).

Opening Site Names

WebSpy Live enables you to open a saved list of site names at any time. This is useful if you want to open a backed up list of site names.

To open a site names list:

1. In Live Configuration, select **Views | Aliases** from the main menu, or click on the Aliases Sidebar icon
2. Click the 'Site names' tab
3. Click the **Open existing site name** link in the Management task pad to launch the Open dialog
4. Select a site names list to open. All site names lists have the file extension *.SiteNames.
5. Click the **Open** button. If you have not cleared the previous site names list, a confirmation dialog appears asking if you want to merge your current site names list with the new list:
 - Click **Yes** to merge the two lists
 - Click **No** to clear the existing site names list and open the new list
 - Click **Cancel** to return to the current site names list

Note:

If the list you are opening contains some of the same site names as the



current list, the site names are left in their original state. (I.e. the sites in the current list will remain unchanged).

Site names lists are saved with the extension *.SiteNames. *Live* stores site names in the location specified in Locations Options (see Location Options on page 87).

Your site names list is automatically saved when you exit *Live*

Exporting Site Names to CSV

WebSpy Live enables you to export your site names to a CSV file, which can be opened in Microsoft® Excel or any text editor.

This functionality enables you to view all site names in the one file. It is also useful for editing your site names more efficiently when dealing with large amounts of information. You can then import the edited CSV file back into *Live*.

To export your site names list:

1. In Live Configuration, select **Views | Aliases** from the main menu, or click the Aliases Sidebar icon
2. Click the 'Site names' tab
3. Click on the **Export to a CSV file** link on the Advanced task pad.
4. Type a name for the CSV file in the 'File name' edit box.
5. Click the **Save** button.

CSV files can be imported back into Live as long as the information within the CSV file is formatted correctly (see Importing Site Names from CSV on page 52).

Importing Site Names from CSV

Once you have exported site name to a CSV file using the export function, you can import the CSV file back into *WebSpy Live*.

To import site names from a CSV file:

1. In Live Configuration, select **Views | Aliases** from the main menu, or click the Aliases Sidebar icon
2. Click the site names tab
3. Click the **Import from a CSV file** link on the Advanced task pad.
4. Find and select the CSV file to import
5. Click **Open**

The CSV file needs to be formatted correctly for the import to work. The easiest way to discover how the CSV file should be formatted is to export your existing site names and view the resulting CSV file.

The figure below illustrates how information in a CSV file should be formatted for the import process to work correctly.

	A	B	C	D	E
1	Site name 1	Data item 1	Data item 2	Data item 3	
2	Site name 2	Data item 1	Data item 2	Data item 3	
3	Site name 3	Data item 1	Data item 2	Data item 3	
4	... etc.				
5					

Figure 5: Layout of site names and their associated data items in CSV format



File types

About File types

File type aliases enable you to group common types of downloaded resources by file type names, using file extensions.

For example, you can group the file types 'mpg', 'avi', and 'mov', into a file type alias called 'Video Clips'.

You can use file types when defining triggers to alert you when particular types of files are downloaded (see About Triggers on page 15). This helps you identify users that are downloading potentially harmful application files, or users wasting bandwidth by downloading large video files.

You can add, edit and delete file types using the links in the Aliases task pad.

You can also import and export your File type aliases to a CSV file using the links in the Advanced task pad. This is useful for importing and exporting your file type aliases to and from *WebSpy Analyzer*, and for editing a large number of file types using third party software such as Microsoft© Excel (see Importing File Types from CSV on page 57 and Exporting File Types to CSV on page 56).

Adding File Types

You need to add file types aliases if you want to define triggers that alert you when particular types of files are downloaded (see About Triggers on page 15).

For example, if you want to be alerted when any type of multimedia file is downloaded, you need to add the extensions of all applicable files (such as '.mp3', and '.mov') to an alias, and then choose that alias when you create your trigger.

To add a file type:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'File types' tab
3. Click the **Add new file type** link in the File Types task pad. This launches the New Name dialog
4. Type the name of the new file type into the 'Name' edit box. For example, type 'Multimedia' if this file type is representing files such as '.mp3' and '.mov'.
5. Click the **Add** button on the toolbar to launch the New dialog
6. Type in the extension of one of the file types (such .exe, or .gif) that you want to include in this alias, then click **OK** to close the dialog
7. Repeat steps 5 and 6 until you have added all necessary file extensions to the file type alias
8. Click **OK**

The new file type is displayed in the aliases list. You can edit and delete any file type aliases in this list (see Editing File Types on page 54 and Deleting File Types on page 54).

Hint:

To add a number of extensions to a file type alias at the one time, you can paste a list of extensions from another application, like Microsoft® Word. Copy the extensions (each on a separate line), then right-click in the file name list and select 'Paste' from the pop-up menu that is displayed.



Editing File Types

Once you have added file type aliases (see Adding File Types on page 53), you need to maintain them. The most common maintenance task is adding extensions to the file type alias. You can also edit and delete extensions assigned to a file type.

For example, you may want to remove the extension `.mov` from the 'Multimedia' alias, and add it to another alias called 'Video clips'.

To edit a file type:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'File types' tab
3. Select the file type that you want to edit in the list
4. Click the **Edit selected file type** link in the file types task pad. This launches the Edit dialog. On this dialog you can change the name of the alias, add items, edit existing items, or delete existing items from the alias
 - To change the name of the alias:
Type the new file type alias name into the 'Name' edit box
 - To add items (extensions) to the alias:
Click the **Add** button, type the name of the new item into the New dialog and click **OK**
 - To edit an existing item (extension):
Select the item in the list that you want to edit, click the **Edit** button, type the new item into the New dialog and click **OK**
 - To delete an existing item (extension):
Select the item in the list that you want to delete and click the **Delete** button
5. Click **OK**

The edited file type is displayed in the aliases list. You can also delete any file type aliases that are no longer required (see Deleting File Types on page 54).

Deleting File Types

You may need to delete file types when they are no longer required.

For example, if you do not need to use one of your defined file types in any trigger, you can delete that file type.

To delete a Files type:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'File types' tab
3. Select the file type that you want to delete in the list
4. Click the **Delete selected file type** link in the File types task pad.
5. Click **Yes** on the confirmation dialog to delete the file type alias

The file type is no longer displayed in the aliases list.

You can also edit any file type alias in the list.



Deleting All File Types

You can delete your list of file types if you want to start a new list. Deleting all file types essentially closes your active file types list and presents you with a blank list, to which you can add new file types.

To delete all file types:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'File types' tab
3. Click the **Delete all file types** link in the file types task pad
4. Click **Yes** on the confirmation dialog to delete the file type

You can then open an existing file types list (see Opening File Types on page 56), or add new file types (see Adding File Types on page 53).

Your file types list is saved automatically when you exit *Live*.

Creating File Types Lists

WebSpy Live enables you to create a new list of file types.

To create a new file types list:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'File types' tab
3. Click the **Delete all file types** link in the File Types task pad. A confirmation dialog will be displayed
4. Click **Yes** to delete the existing file types list
5. Add new file types to the new list (see Adding File Types on page 53).

This file types list is saved automatically when you exit *Live*. It is a good idea to save your existing file types list before creating a new list, in case you want to recover them later.

Note:

It may be easier to edit your existing file types list rather than creating a new list.

Saving File Types

You can save your list of file types, which you can open in *WebSpy Live* at any time. This enables you to back up your file types.

To save a file types list:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'File types' tab
3. Click on the **Save current file types** link on the File Types task pad
4. Type a name for the file types list in the 'File name' edit box
5. Click the **Save** button

All file types lists are saved with the extension *.FileTypes. Once you have saved a file types list, you can quickly open this list in *Live* when required (see Opening File Types on page 56).

By default, *Live* stores file types in the location specified in Locations Options (see Location Options on page 87).



Your file types list is saved automatically when you exit Live.

Opening File Types

WebSpy Live enables you to open a saved list of file types at any time. This is useful if you want to open a backed up list of file types.

To open a file types list:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'File types' tab
3. Click the **Open existing file types** link in the Management task pad to launch the Open dialog
4. Select a file types list to open. All file types lists have the file extension *.FileTypes
5. Click the **Open** button. If you have not cleared the previous file types list, a confirmation dialog appears asking if you want to merge your current file types list with the new list:
 - Click **Yes** to merge the two lists
 - Click **No** to clear the existing file types list and open the new list
 - Click **Cancel** to return to the current file types list

Note:

If the list you are opening contains some of the same file types as the current list, the file types are left in their original state. (I.e. the file types in the current list will remain unchanged).

file types lists are saved with the extension *.FileTypes. *Live* stores file types in the location specified in Locations Options (see Location Options on page 87).

When you exit *Live*, the file types list you currently have open is saved to Default.FileTypes (See **Error! Reference source not found.** on page **Error! Bookmark not defined.**).

Exporting File Types to CSV

WebSpy Live enables you to export your file types to a CSV file, which can be opened in Microsoft® Excel or any text editor.

This functionality enables you to view all file types in the one file. It is also useful for editing your file types more efficiently when dealing with large amounts of information. You can then import the edited CSV file back into *Live*.

To export your file types list:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'File types' tab
3. Click on the **Export to a CSV file** link on the Advanced task pad.
4. Type a name for the CSV file in the 'File name' edit box.
5. Click the **Save** button.

You can import CSV files back into *Live* as long as the information within the CSV file is formatted correctly (see Importing File Types from CSV on page 57)



Importing File Types from CSV

Once you have exported file types to a CSV file using the export function (see Exporting File Types to CSV on page 56), you can import the CSV file back into *WebSpy Live*.

To import file types from a CSV file:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'File types' tab
3. Click on the **Import from a CSV file** link on the Advanced task pad
4. Find and select the CSV file to import
5. Click **Open**

The CSV file needs to be formatted correctly for the import to work. The easiest way to discover how the CSV file should be formatted is to export your existing file types and view the resulting CSV file.

The figure below illustrates how information in a CSV file should be formatted for the import process to work correctly.

	A	B	C	D	E
1	File type 1	Data item 1	Data item 2	Data item 3	
2	File type 2	Data item 1	Data item 2	Data item 3	
3	File type 3	Data item 1	Data item 2	Data item 3	
4	... etc.				
5					

Figure 6: Layout of file types and their associated data items in CSV format

About Departments

About Departments

Departments are logical groups of an organization's personnel. Department aliases enable you to group users into department names such as 'Accounts' or 'Management'.

You can use department aliases when defining triggers to alert you to the Internet and network activity of members of a department (see About Triggers on page 15). You can also use departments to filter your Inputs (see About Inputs on page 6).

For example, if you are not interested in monitoring Management staff, you can create a department called 'Management' that groups all the appropriate users, and filter out this department in your Inputs.

You can add, edit and delete departments using the links in the Departments task pad.

You can also import and export your departments to a CSV file using the links in the Advanced task pad. This is useful for importing and exporting your department aliases to and from *WebSpy Analyzer*, and for editing large numbers of departments using third party software such as Microsoft© Excel (see Importing Departments from CSV on page 62 and Exporting Departments to CSV on page 62).



You can also use the Department Wizard to create departments from your Windows NT® or Windows® 2000 user groups (see Importing Windows Users on page 63).

Any changes made to your departments are only applied to new log data.

Adding Departments

You need to add departments if you want to be alerted to the Internet and email activity of members of a department, or if you want to filter your inputs so that *Live* does not monitor certain groups of users.

For example, departments enable you to monitor the activity of specific groups of users, such as the 'Marketing' department, or exclude groups of users from being monitored such as 'Management'.

To add a department:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'Departments' tab
3. Click the **Add new department** link in the Departments task pad. This launches the New Name dialog
4. Type the name of the department into the 'Name' edit box. For example, if you want to represent a list of users with the name 'Development', type 'Development' into the 'Name' edit box
5. Click the **Add** button on the toolbar to launch the New dialog
6. Type in the name of a user (such as an IP or email address) that you want to add to the department alias, and then click **OK** to close the dialog. You can also type the name of a defined User name alias.
7. Repeat steps 5 and 6 until you have added all necessary users to the department alias. You can also add items later using the Unassigned list (see Using the Unassigned List on page 59), Live Status (see Adding Users to Departments on page 75) and Live Summary (see Adding Users or Sites to Aliases on page 83).

Hint:

To add a number of users to a department at the one time, you can paste a list of user's names from another application, like Microsoft® Word. Copy the names (each on a separate line), then right-click in the users list and select 'Paste' from the pop-up menu that is displayed.

8. Click **OK**

The new department is displayed in the aliases list. You can edit and delete any department aliases in this list.

You can quickly create departments using your Windows NT® or Windows® 2000 user groups by Importing Windows Users (see Importing Windows Users on page 63).

Hint:

You can use wildcards when adding users to a department alias to reduce the number of items you need to add. For more information, see Using Wildcards in Aliases on page 66

Hint:

You can type the name of a defined user name alias when adding users to your department. It is therefore a good idea to set up all your users with a user name alias before you create your departments.



Using the Unassigned List

To the right of the 'Departments' tab is the Unassigned list. It displays all users who are not currently assigned to a department. You can assign any of these users to the appropriate department alias.

To add an unassigned user to a department alias:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'Departments' tabs
3. Select the user in the Unassigned list. You can use the 'Find' function at the top of the Unassigned list to search for keywords in the list. You can also select more than one user by holding down the <Ctrl> and <Shift> keys when selecting.
4. Drag the user to the appropriate department in the aliases list

You can also add users to departments from Live Status (see Adding Users to Departments on page 75) and Live Summary (see Adding Users or Sites to Aliases on page 83).

Editing Departments

Once you have added department aliases (see Adding Departments on page 58), you need to maintain them so that they represent all users belonging to that department. The most common maintenance task is adding new users to the department alias. You can also edit and delete users assigned to a department.

To edit a department:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'Department' tab
3. Select the department that you want to edit in the list
4. Click the **Edit selected department** link in the Departments task pad. This launches the Edit dialog. On this dialog you can change the name of the department, add users, edit existing users, or delete existing users from the department.
 - To change the name of the department:
Type the new department name into the 'Name' edit box
 - To add users to the department:
Click the **Add** button, type the name of the new user into the New dialog and click **OK**
 - To edit an existing user:
Select the user in the list that you want to edit, click the **Edit** button, type the new user into the New dialog and click **OK**
 - To delete an existing user:
Select the user in the list that you want to edit and click the **Delete** button
5. Click **OK**

The edited department will be displayed in the aliases list. You can also delete any departments that are no longer required (see Deleting Departments on page 60).

An easy way of adding users that are not currently assigned to a department alias is by using the Unassigned list (see Using the Unassigned List on page 59). You can also add users to department aliases from Live Status (see Adding Users



to Departments on page 75) and Live Summary (see Emailing Users in Live Summary on page 81).

Deleting Departments

You may need to delete departments when they are no longer required.

For example, if you have created departments to represent users in project-based teams, you may want to delete the departments when the projects have come to an end.

To delete a department:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'Departments' tab
3. Select the department that you want to delete in the list
4. Click the **Delete selected department** link in the departments task pad
5. Click **Yes** on the confirmation dialog to delete the department alias, or click **No** to cancel the deletion

The department is no longer displayed in the aliases list. You can also edit any department aliases in the list (see Editing Departments on page 59).

Deleting All Departments

You can delete your list of departments if you want to start a new list. Deleting all departments essentially closes your active departments list and presents you with a blank list, to which you can add new departments.

To clear your departments:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'Departments' tab
3. Click the **Delete all departments** link in the Departments task pad. Click **Yes** on the confirmation dialog to delete the departments.

You can then open an existing departments list (see Opening Departments on page 61), or add new departments (see Adding Departments on page 58).

Your departments list is automatically saved when you exit *Live*.

Creating Departments Lists

WebSpy Live enables you to create a new list of departments.

To create a new departments list:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'Departments' tab.
3. Click the **Delete all departments** link in the Departments task pad. A confirmation dialog will be displayed
4. Click **Yes** to clear the existing departments list
5. Add new departments to the new list (see Adding Departments on page 58)

When you exit *Live*, this departments list is saved as your default list. It is therefore a good idea to save your existing departments list before creating a



new list, in case you want to recover them later. For more information see Using Default Departments on page 63.

Note:

It may be easier to edit the default departments list rather than creating a new list from scratch.

Saving Departments

You can save your list of departments, which you can open in *WebSpy Live* at any time. This enables you to back up your departments.

To save a departments list:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'Departments' tab
3. Click on the **Save current departments** link on the Departments task pad
4. Type a name for the departments list in the 'File name' edit box
5. Click the **Save** button

All departments lists are saved with the extension *.Departments. Once you have saved a departments list, you can quickly open this list in *Live* when required (see Opening Departments on page 61).

By default, *Live* stores departments lists in the location specified in Locations Options (see Location Options on page 87).

Your departments list is automatically saved to when you exit *Live*.

Opening Departments

WebSpy Live enables you to open a saved list of departments at any time. This is useful if you want to open a backed up list of departments.

To open a departments list:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'Departments' tab
3. Click the **Open existing departments** link on the departments task pad to launch the Open dialog
4. Select a departments list to open. All departments lists have the file extension *.Departments
5. Click the **Open** button. If you have not cleared the previous departments list, a confirmation dialog appears asking if you want to merge your current departments list with the new list:
 - Click **Yes** to merge the two lists
 - Click **No** to clear the existing departments list and open the new list
 - Click **Cancel** to return to the current departments list

Note:

If the list you are opening contains some of the same departments as the current list, the departments are left in their original state. (I.e. the departments in the current list will remain unchanged).

Departments lists are saved with the extension *.Departments. *Live* stores departments in the location specified in Locations Options (see Location Options on page 87).



Your departments list is automatically saved to when you exit *Live*.

Exporting Departments to CSV

WebSpy Live enables you to export your departments to a CSV file, which can be opened in Microsoft® Excel or any text editor.

This functionality enables you to view all departments in the one file. It is also useful for editing your departments more efficiently when dealing with large amounts of information. You can then import the edited CSV file back into *Live*.

To export your departments list:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'Departments' tab
3. Click on the **Export to a CSV file** link on the Advanced task pad.
4. Type a name for the CSV file in the 'File name' edit box.
5. Click the **Save** button.

You can import CSV files back into *Live* as long as the information within the CSV file is formatted correctly (see Importing Departments from CSV on page 62).

Importing Departments from CSV

Once you have exported departments to a CSV file using the export function (see Exporting Departments to CSV on page 62), you can import the CSV file back into *WebSpy Live*.

To import departments from a CSV file:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'Departments' tab
3. Click on the **Import from a CSV file** link on the Advanced task pad
4. Find and select the CSV file to import
5. Click **Open**

The CSV file needs to be formatted correctly for the import to work. The easiest way to discover how the CSV file should be formatted is to export your existing departments and view the resulting CSV file.

The figure below illustrates how information in a CSV file should be formatted for the import process to work correctly.

	A	B	C	D	E
1	Department 1	Data item 1	Data item 2	Data item 3	
2	Department 2	Data item 1	Data item 2	Data item 3	
3	Department 3	Data item 1	Data item 2	Data item 3	
4	... etc.				
5					

Figure 7: Layout of departments and their associated data items in CSV format

Using Default Departments

When you open *WebSpy Live*, your default departments list (Default.Departments) is automatically loaded. You can edit this list as desired



(see Editing Departments on page 59) or create another custom departments list.

If you open another list during your *Live* session, this second list is saved as your default when you exit *Live*. However, if you make any changes to the second list, and do not save it, the changes are only applied to the default list.

Default departments are effectively a snapshot of the list you were using when you last exited *Live*.

Importing Windows Users

If your PC is part of a Windows NT® domain, you can utilize your existing network resources to quickly create alias groups for 'departments' and 'user names' aliases. You can do this by utilizing *Live's* 'Import Windows Users' function.

You can use this function to import user names or departments as they are listed in your Windows NT® domain.

To use the 'Import Windows users' function, you need to be using a Windows NT based authentication server and operating system (Windows NT, 2000 or XP), and have a domain controller correctly configured. 'Importing Windows users' does not work when running a Windows 9.x operating system (Windows 95, 98, ME). For more information on whether you are running the correct system for importing windows users, contact your system administrator or support@webspys.com.

To import Windows users:

1. In Live Configuration, select **Views | Aliases** from the main menu, or select the Aliases Sidebar icon
2. Click the 'Departments' tab
3. Click the **Import Windows Users** link on the Advanced task pad. This launches the Department Wizard which guides you through the process of importing Windows users (see Using the Department Wizard on page 63).

Department Wizard

Using the Department Wizard

The Department Wizard enables you to create departments easily by converting Windows NT® or Windows® 2000 user groups into *WebSpy Live* departments.

To launch the wizard:

1. In Live Configuration, select **Views | Aliases** from the main menu, or click on the Aliases Sidebar icon
2. Click the 'Departments' tab
3. Click the **Import Windows Users** link on the Advanced task pad

You can also launch the Department Wizard by selecting **Tools | Department Wizard** from the main menu of Live Configuration.

The wizard is made up of three main pages:

- Domain Controller page
- Groups page
- Users page



If a user belongs to more than one user group, the Department Conflict page is displayed for you to choose the department you want to assign the user to.

Note:

You can only use the Department Wizard if you use Windows NT® 4.0, 2000 or XP Server as your authentication server.

Domain Controller Page

On this page of the Department Wizard you can select which domain controller on your network stores the information about user groups that *WebSpy Live* requires to convert the groups into Department aliases.

By default, *Live* uses the primary domain controller of the domain you are currently logged in to.

You might want to use a different domain controller because the groups you want to access are not defined on the domain you are logged in to.

To use a different domain controller:

1. Select the 'Enter a Domain Controller' radio button
2. Type the location of the controller into the edit box

Live can append your domain name to the name of your user aliases. Make sure that the 'Add domain name to the user aliases' checkbox is checked to ensure that your domain name is added.

For example, Bob on the domain of WEBSPY\ would appear as WEBSPY\Bob.

Once you have made your selections, click **Next** to continue.

Groups Page

On the Groups page of the Department Wizard, you can select the user groups that you want to use as departments.

To select which groups to use, check the checkbox next to the name of the group you want to use from the list. Use the **Select All**, **Clear Selection** and **Invert Selection** buttons as necessary.

Once you have made your selections, click **Next** to continue.

Users Page

This page of the wizard enables you to select the users you want to include in your departments.

To select which user to use check the checkbox next to the name of the users that you want to use from the list. Use the **Select All**, **Clear Selection** and **Invert Selection** buttons as necessary.

Once you have made your selections, click **Next** to continue.

If a user belongs to more than one user group, the Department Conflict page is displayed for you to choose the Department you want to assign the user to.



Department Conflict Page

The Department Conflict page is only displayed if one of your chosen users belongs to more than one user group. If there are no conflicts, the final page of the Department Wizard is displayed.

Conflicts occur when a single user is assigned to one or more User Groups. While this is possible in Windows® user groups, you cannot have a user in more than one Department alias.

When this happens, you need to choose which department to assign the user to.

On the Department Conflict page, the name of the user that belongs to more than one user group is displayed. The page will appear for as many users as necessary.

There are four ways of resolving the conflict.

- Assign the user to one of the departments that will be created from the chosen user groups
 1. Select the first radio button, 'Assign from available groups'
 2. Click on the arrow in the drop down list just below the radio button and select the name of the department to assign the user to
 3. Click **Next**
- Assign the user to an existing department
 1. Select the second radio button, 'Assign to existing department'
 2. Click on the arrow in the drop down list just below the radio button and select the name of the department to assign the user to
 3. Click **Next**
- Assign the user to a new department
 1. Select the third radio button, 'Assign to new department'
 2. Type the name of the new department to assign the user to into the edit box just below the radio button
 3. Click **Next**
- Ignore the user
 1. Select the fourth radio button, 'Ignore this user'
 2. Click **Next**

Once all the conflicts have been resolved, the final page of the Department Wizard is displayed.

Final Page

On the final page of the Department Wizard, click **Finish** to begin the import process. Your imported departments and associated users will be displayed on the Departments tab of the Aliases screen. You can edit these departments as required (see Editing Departments on page 59).

You can use these departments when defining triggers (see About Triggers on page 15), or when filtering your inputs (see About Inputs on page 6).



Using Wildcards in Aliases

A data item needs to exactly match an alias item for it to be associated with the corresponding alias. Defining your aliases can therefore be a time consuming task.

For example, if you are trying to alias all hits to your organization's website, you need to add an item to your alias for every page, and every resource that belongs to your website.

Fortunately, you can utilize 'wildcards' when [adding items to alias groups](#), to make the task of defining your aliases much easier.

A wildcard is a special character or group of characters that represents information that is allowed to change from hit to hit.

For example, if you want to alias all hits to your companies website, you can specify the item `www.yourcompany.*`. The asterisk character is the wildcard. It represents all information that follows `www.yourcompany`. Every page associated with your website will therefore be associated with the alias you are defining.

There are three types of wildcards:

- **The asterisk character (*)**

You generally use the asterisk character in place of characters that you want to ignore. The asterisk can be used to represent many characters and is generally placed at the beginning or end of a phrase that you want included in the alias.

For example, `*@webspy.com` represents all company email addresses at WebSpy Ltd. Anything that precedes `@webspy.com` is ignored. Alternatively, you could use `*@webspy.co*` to include all company email addresses at both the `webspy.com` and `webspy.co.uk` domains.

- **The question mark character (?)**

The question mark character can be used to represent single characters that can change from hit to hit.

`170.158.1.???` can represent an IP address in one of your companies sub-networks. `john?webspy` can represent `john@webspy` and `john.webspy`

- **The square bracket characters ([])**

You can specify acceptable ranges using the square bracket characters.

`[0-9][0-9][0-9].[0-9][0-9][0-9].[0-9][0-9][0-9].[0-9][0-9][0-9]` can represent any IP address with three digits in each part. `[A-Z]` can represent any alpha character.

You can use wildcards when adding items such as users and URLs to your user name (see Adding User Names on page 43), site name (see Adding Site Names on page 48), file types (see Adding File Types on page 53), or department (see Adding Departments on page 58) aliases. Simply type the desired wildcard characters into the item name when adding the item to the alias.



3. Live Status

About Live Status

Live Status displays a list of all current alerts. *WebSpy Live* raises an alert when a hit breaches a defined trigger (see About Triggers on page 15). Live Status is therefore the dialog you use most frequently to monitor your Internet and email traffic.

To launch Live Status, click the Live icon in the system tray.



A **Live** button is displayed at the top of Live Status. Clicking this button displays a menu that provides access to other areas of *Live*.

This menu also enables you to:

- Reset *Live* (see Resetting Live on page 77)
- Dismiss all alerts (see Dismissing Alerts on page 72)
- Mark all alerts as read (see Marking Alerts as Read on page 73)
- Suspend and un-suspend *Live* (see Suspending Live on page 77)
- Shutdown *Live* (see Shutting Down Live on page 77)

There is also a **Summary** button at the top of Live Status that provides quick access to the Live Summary dialog (see About Live Summary on page 79).

Live Status groups alerts by trigger name. It also displays all active and idle users. An icon representing the most recently accessed protocol is displayed next each active user's name. For more information see Protocol Icons on page 68.

Figure 8: Live Status

Any new alerts that are triggered are represented by alert icons in Live Status and the system tray. The color of the icon in the system tray depends on the priority level of the current alerts (see Alerts on page 68).

For example, if the highest priority alert is 'medium', the icon in the system tray will be yellow. If you have any unread high priority alerts, the icon in the system tray will be red.

If you do not want to view the alerts for a particular trigger, or if you are not interested in viewing either active or idle users, you can collapse that particular group of Live Status (see Collapsing and Expanding Groups on page 69).

Using Live Status, you can also:

- Display alert details (see Displaying Alert Details on page 69)
- Display user details (see Displaying User Details on page 73)
- Dismiss alerts (see Dismissing Alerts on page 72)
- Enable triggers (see Enabling Triggers from Live Status on page 76)
- Disable triggers (see Disabling Triggers from Live Status on page 76)
- Add users to user name or department aliases (see Adding Users to User names on page 75 and Adding Users to Departments on page 75).



Alerts

Alerts are represented by icons in Live Status and the system tray.

When no alert have been triggered, or if 'Flash when there are unseen alerts' is un-checked in Display Options (see Display Options on page 86), the default Live icon is displayed in the system tray.

 **Figure 9: Default system tray icon.**

You can assign a priority level to a trigger to indicate how important the trigger is. This priority is indicated by the colour of the alert.

A trigger assigned a low priority generates green alerts. Triggers assigned medium and high priorities generate yellow and red alerts respectively. Black alerts are raised when an issue occurs with one or more of your configured inputs.



Black alert - input issue

This icon is displayed in Live Status and the system tray when there is an input issue.



Green alert - low priority

This icon is displayed in the system tray when a low priority alert has been triggered, and there are no unseen alerts of a higher priority (yellow or red).



Yellow alert - medium priority

This icon is displayed in the system tray when a medium priority alert has been triggered, and there are no unseen high priority (red) alerts.



Red alert - high priority

This icon is displayed in the system tray when a high priority alert has been triggered.

Once an alert has been displayed in the Alert Details dialog, it's associated alert icon stops flashing in Live Status. This is to differentiate between read and unread alerts.

Note:

Alert icons are not displayed in the system tray, and do not flash in Live Status if 'Flash when there are unseen alerts' is un-checked in Display Options (see Display Options on page 86).

Protocol Icons

Some *WebSpy Live* dialogs display icons that represent the protocols being monitored. These dialogs include Alert Details, User Details and Live Summary dialogs. The active and idle users lists in Live Status also display the associated protocol icon representing each users latest activity.

The following is a list of the protocols *Live* is capable of monitoring, and their associated protocol icon:



Web



Email



Telnet



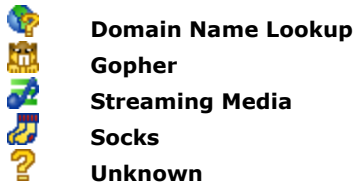
File Transfer Protocol (FTP)



News



Secure Web



Live Summary displays failed hits by displaying a red cross in the bottom left hand corner of the protocol icon.



Note:

Your log files must first be capable of monitoring the above protocols for Live to display them. If your current log format does not support the above protocols, you may consider WebSpy Sentinel as your logging tool.

Collapsing and Expanding Groups





The Live Status dialog groups alerts by trigger name (see About Triggers on page 15). It also displays all active and idle users.

If you do not want to view the alerts for a particular trigger, or you are not interested in viewing either active or idle users, you can collapse that particular group of the Live Status dialog.

To collapse a group, click the minus sign  to the left of the group heading. The minus sign is replaced with a plus sign . If there are any unread alerts within a collapsed group, the plus sign will be the color corresponding to the priority level of the unread alert (see Alerts on page 68).

For example, if there is an unread medium priority alert within a collapsed group of Live Status, the plus sign is displayed in yellow.

Unread alert icons:

-  Unread input issue alert
-  Unread low priority alert
-  Unread medium priority alert
-  Unread high priority alert

To expand a group, simply click the plus sign to the left of the group heading.

Displaying Alert Details

Live Status displays all alerts that have been raised based on the defined triggers *WebSpy Live* (see Displaying Alert Details on page 69). All the alerts are grouped by trigger name. The user name of the person who breached the conditions of the trigger is displayed next to the alert icon.

To view the details of an alert, right-click on the alert and select the **Display** option from the pop-up menu that is displayed. Alternatively, double-click the alert in Live Status. The appropriate Alert Details dialog is displayed.

To view the details of other alerts generated by the same trigger, click the **Next** and **Previous** arrows on the toolbar.

Hint:

You can also right-click a trigger group and select **Display** from the pop-up menu. This displays the details of the first alert in the trigger group.



Double-clicking the system tray icon when an alert is triggered displays the most recent unseen alert in the Alert Details dialog.

Once an alert is displayed in the Alert Details dialog, its associated alert icon stops flashing in Live Status. This is to differentiate between read and unread alerts (see also Marking Alerts as Read on page 73)

Note:

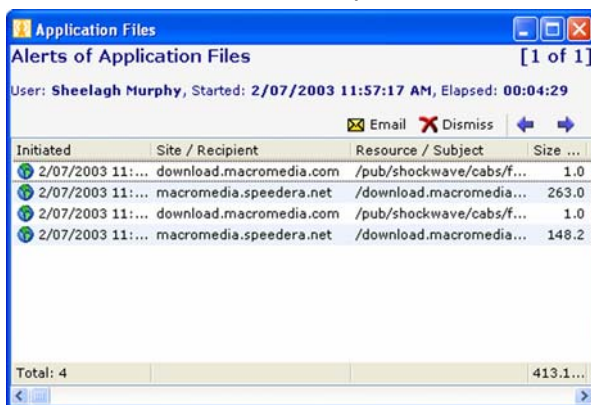
Alert icons do not flash in the Live Status dialog or in the system tray if you have 'flash when there are unseen alerts' unchecked in Display Options (see Display Options on page 86).

Alert Details Dialog

The Alert Details dialog displays information about the hits that triggered the alert.

From this dialog, you can:

- Email a user the details of an alert (see Emailing Users in Live Status on page 74)
- Dismiss an alert (see Dismissing Alerts on page 72)
- Add sites or recipients to aliases or profiles keywords lists.
- Navigate between alerts using the next and previous arrows on the toolbar



To launch the Alert Details dialog, double click an alert in the Live Status dialog. Alternatively, right-click the alert and select **Display** from the pop-up menu.

The summary information displayed in the Alert Details dialog varies depending on whether the alert was raised by a Single Hit, Session, or Cumulative trigger.

Figure 10: Alert Details Dialog

The following summary information is displayed in the Alert Details dialog:

Single Hit alerts

- **User:**
The name of the user responsible for triggering the alert
- **Started:**
The time when the first hit was made
- **Elapsed:**
The total time from when the user first started browsing
- **Initiated:**
The time the single hit that triggered the alert occurred, displayed with an associated protocol icon
- **Site/Recipient:**
The names of web addresses, email addresses or other Internet servers accessed.
- **Resource/Subject:**
The individual files that the user downloaded from the Internet sites, or the subject line of emails



- **Size:**
The size of each hit
- **Profile:**
The Profile that each hit belongs to. See About Profiles

Session alerts

- **User:**
The name of the user responsible for triggering the alert
- **Started:**
The time the session started
- **Elapsed:**
The total time of the session, from the first hit to the last hit
- **Site/Recipient:**
The names of web addresses, email addresses or other Internet servers accessed during the session, displayed with an associated protocol icon
- **Hits:**
The total number of hits the user has made to each site or recipient during the session
- **Size:**
The total size of all the hits to each site or recipient
- **Last Accessed:**
The time when a user last visited the site or last sent email to the recipient during the session

Cumulative alert

- **User:**
The name of the user responsible for triggering the alert
- **Elapsed:**
The total time the user has been browsing. This is the combined time of all of the users session
- **Session Start:**
The time each session began
- **Sites:**
The number of sites visited in each session
- **Elapsed:**
The total length of each session
- **Hits:**
The total number of hits made in each session
- **Size:**
The total size for each session

Totals for each column are displayed at the bottom of each column.

On the Alert Details dialogs for Single Hit and Session alerts, you can add any site or recipient to an alias or to any profiles keyword list.

To add a site or recipient to an alias:

1. Right-click on the site or recipient in the Alert Details dialog
2. Select **Add to alias...** from the pop-up menu to launch the Quick Alias dialog
3. The site or recipient name appears in the 'Item' edit box. Edit this name if necessary
4. Select the type of alias, such as user names or site names from the 'In' drop down list.
5. Select an item that you want to assign the site or recipient to from the 'As' drop down list, or type a new value into the drop down list.
6. Click **OK** to assign the site or recipient to the alias



To add a site or recipient to a profiles keyword list:

1. Right-click a site or recipient and select **Add to profile...** from the pop-up menu. This launches the Quick Profile dialog
2. The site or recipient you selected appears automatically in the 'Keyword' drop down list. You can edit this keyword as desired.

For example, if you select the keyword `www.webspay.com`, you can edit this so that only 'webspay' is added to the profile.

3. Select whether you want to add the keyword to the profile's includes or excludes list using the appropriate radio buttons
4. Select the profile that you wish to add the keyword to from the Profile drop down list, or type a new profile into the list
5. Click **OK**

Dismissing Alerts

In Live Status you can dismiss alerts that you no longer want displayed. You can dismiss individual alerts, all the alerts raised by a particular trigger, or all your alerts.

For example, if you receive an 'Unacceptable Content' alert for web browsing that is legitimate, you may want to dismiss the alert so that it is no longer displayed in the Live Status dialog.

To dismiss an alert:

1. Double-click the alert you want to dismiss. This launches the Alert Details dialog for that alert.
2. Click the **Dismiss** button on the toolbar. The alert is no longer displayed in the Live Status dialog, and the next alert is displayed the Alert Details dialog.
3. Repeat step 2 until you have finished dismissing all necessary alerts

Hint:

Right-click on an alert to dismiss or display details for the alert. Just select the appropriate options from the pop-up menu.

You can also dismiss all alerts for a trigger at the one time.

To dismiss all alerts for a trigger:

1. Right-click on the trigger group heading
2. Select **Dismiss** from the pop-up menu.

All alerts for this trigger are no longer displayed in Live Status.

You can also dismiss all alerts in Live Status at the one time.

To dismiss all alerts:

1. Click the Live menu button at the top of Live Status
2. Select **Dismiss All** from the menu

Live Status will be cleared of all alerts. Your list of active and idle users will remain in Live Status. If you also want to clear your list of active and idle users, you can reset *Live* (see Resetting Live on page 77).



Marking Alerts as Read

When an alert is triggered, it is displayed in Live Status as a flashing alert icon (see Alerts on page 68). If you do not want any existing alerts to flash, but still want new alerts to flash, you can use *Live's* 'Mark as read' feature.

For example, if you start *Live* for the first time in the morning, and Live Status displays 30 alerts that have occurred during the night, you can mark all these alerts as read in order to stop them from flashing. This differentiates the overnight alerts from any new alerts coming in, giving you time to go through them before looking at the new alerts.

You can mark all the alerts in Live Status, all alerts for a particular trigger, or just a single alert as read.

To mark all alerts in Live Status as read:

1. Click the **Live** button at the top of Live Status
2. Select **Mark all as Read** from the menu

To mark all the alerts for a particular trigger as read:

1. Right-click the trigger heading in Live Status
2. Select **Mark <trigger name> as read** from the pop-up menu

To mark an individual alert as read:

1. Right-click the alert in Live Status
2. Select **Mark <user name> as read** from the pop-up menu

Alerts are automatically marked as read once they have been displayed (see Displaying Alert Details on page 69).

Displaying User Details

Live Status displays a list of all active and idle users, but does not display the details of their activity.

To view the activity of a user:

1. Right-click the user's name in either the active or idle group in Live Status, and select **Display** from the pop-up menu. Alternatively, double-click the user's name in Live Status. The appropriate User Details dialog is displayed.
2. Click the **Next** and **Previous** arrows on the toolbar to view the details of other users.

You can also right-click the Active or Idle group heading in Live Status and select **Display** from the pop-up menu. This displays the details of the first user in the group. You can view other users by clicking the **Next** and **Previous** arrows on the toolbar.

Hint:

If you do not want to view any active or idle users you can collapse the lists.

User Details Dialog

Live Status displays all active and idle users of your network. You can display the activity of each of these users using the User Details dialog.



To launch the User Details dialog, double-click a user under the Active or Idle groups of Live Status. Alternatively, right-click the alert and select **Display** from the pop-up menu.

The following summary information is displayed in the User Details dialog for each active or idle user:

- **User name:**
The name of the user accessing your Internet resources
- **Started:**
The time when the user first started browsing or when the user session began
- **Elapsed:**
The total accumulated time for the current user session
- **Site/Recipient:**
The names of web addresses, email addresses or other Internet servers that the user accessed, displayed with an associated protocol image
- **Hits:**
The total number of hits a user has accessed for the session
- **Size:**
The total size of the files accessed during the session
- **Last Accessed:**
The time when a user last visited a site or last sent email

Click the **Next** and **Previous** arrows on the toolbar to navigate to other users in the active or idle user list.

You can also email any active or idle user with the details of their Internet and network activity (see *Emailing Users in Live Status* on page 74).

Note:

For idle users, only the details their most recent session is displayed

Emailing Users in Live Status

WebSpy Live enables you to email the details of alerts to users. This enables you to attend to unacceptable Internet and email use as quickly as possible. You can also send emails to any of your active or idle users, even if they have not triggered an alert.

For example, if an Unacceptable Content alert is triggered, you can send an email to the offending user, outlining what, when and for how long they were browsing inappropriately.

If Live Status is not open, launch it by clicking the Live icon in your system tray.

To email alert details to a user:

1. Double-click an alert to launch the Alert Details dialog
2. Click the **Email** button on the toolbar to launch the Email to dialog. The name of the user who raised the alert is displayed in the 'Address' edit box. Edit this address if necessary.
3. Click **OK** to launch a new email message using your default email program. The recipient, subject and summary information in the Alert Details dialog will be added to the email message. If necessary you can edit any of the details before sending your message.

To send an email to an active or idle user:

1. Double-click on a user to launch the User Details dialog for that user



2. Click the **Email** button on the toolbar to launch the Email to dialog. The name of the user is displayed in the 'Address' edit box. Edit this address if necessary.
3. Click **OK** to launch a new email message using your default email program. The recipient, subject and summary information in the User Details dialog will be added to the email message. If necessary, you can edit any of the details before sending your message.

Hint:

Live enables you to send more comprehensive emails from Live Summary based on information for all users, alerts and sessions for the time period that Live has been monitoring.

You can also configure triggers to automatically email users when alerts are raised. This is configured on the Email Notification page of the Trigger Wizard (see Using the Trigger Wizard on page 17).

Adding Users to User names

Live Status and Live Summary may display data in an undesirable format such as an IP address or email address, instead of a user name. You can give any item listed in Live Status or Live Summary a more meaningful display name by adding it to a user name alias.

For example, if Live Status displays an IP address such as, 192.168.0.9, but you know that the person using this IP address is John, you can assign them to the user name alias 'John'. This changes all instances of the IP address in Live Status to the word 'John'.

Users can be assigned to user names using the Aliases screen in Live Configuration (see Adding User Names on page 43), however you can do this quickly and easily using the Live Summary and Live Status dialogs.

To add a user to a user name alias from Live Summary or Live Status:

1. Right-click on a user's name in either dialog
2. Select **Add to alias...** from the pop-up menu to launch the Quick Alias dialog
3. The user's name that you right-clicked appears in the 'Item' edit box. Edit this name if necessary
4. Select 'User names' from the 'In' drop down list
5. Select a user name that you want to assign the user to from the 'As' drop down list. If you want to create a new user name, type the name in the drop down list.
6. Click **OK** to assign the user to the user name alias

Assigning users to user names using Live Status and Live Summary updates the user's display name as well as adding them to the alias.

Note:

You can check and edit your user name aliases using the 'User names' tab in the Aliases screen of Live Configuration (see About User Names on page 42).

Adding Users to Departments

Users can be assigned to departments using aliases in Live Configuration (see Adding Departments on page 58); however you can do this quickly and easily using the Live Summary and Live Status dialogs.



To add a user to a department from Live Summary or Live Status:

1. Right-click on a user's name in either dialog
2. Select **Add to alias...** from the pop-up menu to launch the Quick Alias dialog
3. The user's name that you right-clicked appears in the 'Item' edit box. Edit this name if necessary.
4. Select 'Departments' from the 'In' drop down list
5. Select a department that you want to assign the user to from the 'As' drop down list. If you want to create a new department, type the new name in the drop down list.
6. Click **OK** to assign the user to the department alias

Note:

You can check and edit your departments and their associated users by going directly to Departments in Live Configuration (see About Departments on page 57).

Disabling Triggers from Live Status

If you are no longer interested in viewing alerts for a particular trigger, you can disable the trigger directly from the Live Status dialog.

To disable a trigger:

1. Right-click on the trigger group heading you want to disable in the Live Status dialog.
2. Select the **Disable** option from the pop-up menu.

The trigger will no longer generate any alerts. If you have more than one trigger with the same name, all these triggers will be disabled. You can also enable the trigger from Live Status (see Enabling Triggers from Live Status on page 76)

Hint:

If you add more than one trigger with the same name, the alerts for these triggers are grouped under the one trigger heading in Live Status. This can be useful for assigning different priorities to varying extremes of the same type of alert.

Note:

Triggers only appear in Live Status when they trigger an alert. If you want to disable a trigger that is not in Live Status, you will need to disable it from Live Configuration.

Enabling Triggers from Live Status

If you have any disabled triggers visible in Live Status, you can enable them again from Live Status.

To enable a currently disabled trigger:

1. Right-click the trigger group heading that you want to enable in the Live Status dialog
2. Select **Enable** from the pop-up menu

The trigger will again start generating any alerts. If you have more than one trigger with the same name, all these triggers will be enabled. To disable a trigger, see Disabling Triggers from Live Status on page 76.

**Hint:**

If you add more than one trigger with the same name, the alerts for these triggers are grouped under the one trigger heading in Live Status. This can be useful for assigning different priorities to varying extremes of the same type of alert.

Note:

Triggers only appear in Live Status when they trigger an alert. If you want to enable a trigger that is not in Live Status, you will need to enable it from Live Configuration.

Suspending Live

Live enables you to suspend Live Status so that no new alerts are displayed until Live is un-suspended. You may want to do this if you do not want to be distracted by new alerts for a short period of time.

To suspend Live

1. Right-click the Live icon in the system tray
2. Select **Suspend** from the popup menu

Live Status indicates that it is suspended and no new alerts are raised. You can use the rest of the application as usual while Live is suspended.

To un-suspend *Live*:

1. Right-click the Live icon in the system tray
2. Select **Un-suspend** from the popup menu

All alerts that occurred during the time *Live* was suspended are then raised, and *Live* continues to generate alerts as they occur.

Resetting Live

You can reset *WebSpy Live* to clear all information in Live Summary and Live Status, as well as free up memory on your machine.

To reset *Live*:

1. Click on the **Live** button in the top left hand corner of Live Status
2. Select **Reset** from the menu
3. Click **Yes** on the confirmation dialog

Note:

Resetting *Live* clears all your accumulated summaries, alerts and users. You can also 'Dismiss All' to clear all alerts without clearing your list of active and idle users. See Dismissing Alerts.

Live automatically clears data that is older than the number of hours specified in General Options (see General Options on page 85).

Shutting Down Live

If you do not want to run *WebSpy Live* anymore, you can shut the program down. It is important to note that simply clicking the close button in the top right



corner of Live Status does not actually close the program, it only minimizes the dialog.

To shut down *Live*:

- Right-click on the Live icon in your system tray and select 'Shutdown' from the pop-up menu

OR

- If Live Status is already open, click the **Live** button at the top of the dialog and select **Shutdown** from the menu.

Note:

When you shut down Live, your accumulated summaries and alerts are automatically saved and re-opened next time Live is started. Alerts outside of the purge time specified in General Options are not displayed when you re-open (see General Options on page 85).



4. Live Summary

About Live Summary

Live Summary collates information about the Internet and email activity, as reported by your proxy server or logging device, of all users being monitored. Live Summary enables you to browse all activity categorized by user and user sessions.

To open Live Summary, right-click on the Live icon in your system tray and select **Summary** from the pop-up menu. Alternatively, if you already have Live Status open, click the **Summary** button at the top of the dialog.



The screenshot shows the 'Live Summary' application window with a 'Users' tab selected. The window displays a table of user activity. The table has columns for 'User / Sender', 'Sessions', 'Elapsed (H...)', 'Hits', 'Size (KB)', and 'Activity'. The data is as follows:

User / Sender	Sessions	Elapsed (H...)	Hits	Size (KB)	Activity	
Des Taviner	1		1	45.3	Idle	
Eva Sharpe	1	00:02:30	2	1.4	Idle	
Gary Best	2		2	41.2	Idle	
Gina Gold	1	00:52:59	101	28.5	Idle	
Graig Gilmore	3	00:30:26	825	4,155.8	Honey Harman	
Honey Harman	4	00:24:31	85	1,261.5	Graig Gilmore	
Jack Meadows	1		1	6.0	Idle	
Jim Carver	4	00:07:47	10	142.6	Idle	
Jo Parrish	1		1	1.2	Idle	
Ken Drummond	1		1	9.8	Idle	
Mickey Webb	3		83	18,969.3	Idle	
Paul Riley	2	00:11:24	44	331.7	Idle	
Phil Hunter	2	00:07:19	7	3,014.0	Idle	
Polly Page	1		1	62.9	Idle	
Reg Hollis	1	00:04:50	150	494.7	Idle	
Robbie Cryer	1	00:06:07	29	257.8	Idle	
Samantha Nixon	1	00:03:27	15	180.6	Idle	
Server	8	00:19:19	28	108.9	reannahale2655s@bigf...	
Sheelagh Murphy	3	00:05:50	197	4,578.8	Idle	
Tony Stamp	4	00:00:33	21	295.4	Idle	
Total:	45	80	04:24:00	2,366	38,880.0...	Active: 4

Figure 11: Live Summary - Users Level

Live Summary organizes user data by the following levels:

- Users Level
- User Sessions Level
- Site Level

To view summary details for a user, click on the user's hyperlinked name to drilldown to the next level. You can also click on a user and then use the **Up** and **Down** arrows on the toolbar to navigate between levels. For more information, see Navigating Between Summary Levels on page 80.

In Live Summary you can also:

- Add keywords to a profile (see Adding Keywords to Profiles on page 83)
- Browse to a URL (see Browsing to a URL on page 82)
- Add a user or site to an Alias(see Adding Users or Sites to Aliases on page 83)
- Email summary details to users (see Emailing Users in Live Summary on page 81)
- Sort your data by a particular column (see Sorting Data on page 81)



Navigating Between Summary Levels

Live Summary organizes user data by the following levels:

- Users Level
- User Sessions Level
- Site Level

In Live Summary you can use the **Up** and **Down** arrows on the toolbar to navigate between different summary levels.

Users Level

When you first open Live Summary, the Users Level is displayed. The Users Level displays all users that have utilized your Internet and email resources.

The following information is displayed at the User Level:

- **User name**
The name of a person or computer using your organization's network
- **Sessions**
The total number of sessions for a user over the period that *Live* has been monitoring
- **Elapsed Time**
The total period of time that a user spent using Internet and email resources over the period *Live* has been monitoring
- **Hits**
The total number of hits a user has raised for the period that *Live* has been monitoring
- **Size**
The total size of downloaded resources for the period that *Live* has been monitoring
- **Activity**
A description of what a user is currently doing

Each user's name is a hyperlink, and clicking a user's name takes you to User Sessions Level for that user.

User Sessions Level

The User Sessions Level lists all the sessions for the user you clicked on at the Users Level.

The following information is displayed at the User Sessions Level:

- **Session Start**
The date and time that the user session started.
- **Sites**
The number of sites visited during the session.
- **Elapsed Time**
The total period of time between when the session first started, to when the user stopped using network resources.
- **Hits**
The total number of hits the user made during the session.
- **Size**
The total size of downloaded resources for the session.



Each user session is a hyperlink, and clicking a User Session, takes you to Site Level for that session. To return to the Users Level, click the **Up** arrow on the toolbar.

Site Level

The Site Level displays all the site names visited, or recipients, for the session you selected at User Sessions Level.

The following information is displayed at the Site Level:

- **Site/Recipient**
The name of the web address, email address or other Internet server a user accessed during the session.
- **Hits**
The total number of hits the user made to the site or recipient.
- **Size**
The total size of resources that the user downloaded from or sent to the site or recipient.
- **Last Accessed**
The time when the user last accessed the site or recipient. This can be the time of the last resource downloaded from a site, or the time the user last sent an email to the recipient.

You can launch any site in your default web browser, or a new email in your default email program with a recipients name in the 'To' field (see Browsing to a URL on page 82 and Emailing Users in Live Summary on page 81).

To return to the User Sessions Level, click the **Up** arrow on the toolbar.

Sorting Data

You can sort the data in Live Summary by any column. This enables you to organize your information in an order that is easier to analyze.

To sort a list of data by a particular column, click on the column heading. An arrow appears in the column heading to indicate whether the data is sorted in ascending order or descending order.

For example, clicking on the Sessions column heading at the Users Level of Live Summary sorts your data by session length.

To reverse this order from ascending to descending or vice-versa, click on the column heading again.

To sort by a different column, click on the appropriate column heading.

You can also sort data by columns in the Alert Details (see Alert Details Dialog on page 70) and User Details dialogs (see User Details Dialog on page 73), as well as most views of the Live Configuration.

Emailing Users in Live Summary

You can export the details of any level in Live Summary to an email, enabling you to send details of network activity to anyone with an email address.



For example, you can send an email to a user outlining the details of their Internet sessions during the day by sending an email from User Session Level in Live Summary.

If Live Summary is not open, launch it by right-clicking the Live icon in your system tray and selecting **Summary** from the pop-up menu.

To send an email in Live Summary:

1. Navigate to the summary level you want to export to an email (see Navigating Between Summary Levels on page 80)
2. Click the **Email** button on the toolbar to launch the Email to: dialog. An email address may be displayed in the Email to: dialog, depending on the Level of Live Summary you are currently on. If you are on the Users Level, an email address is not displayed. If you are on User Sessions or Site Level, the email address of the user you drilled down into is displayed. For example, if you are on the User Sessions or Site Level, the email address of the user you drilled down into is displayed.
3. Edit the email address, or type a new email address into the 'Address' drop down box as required
4. Click **OK** to launch a new email message using your default email program

The recipient, subject and summary information will be exported to the email message. If necessary you can edit any of the details before sending your message.

You can also launch a new email addressed to any recipient listed at the Site level in Live Summary

To do this:

1. Navigate to Site Level in Live Summary (see Navigating Between Summary Levels on page 80)
2. Right-click a recipient's name
3. Select **Browse:** from the pop-up menu

An email is launched using your default email program with the recipients name in the 'To' field.

Hint:

You can also email a user the details of an alert using the Alert Details dialog (see Alert Details Dialog on page 70).

Browsing to a URL

WebSpy Live enables you to browse to sites that users have visited. You may want to do this to obtain more information about a site, in order to add it to a profile or Site name alias.

You can browse to a URL from the Site Level of Live Summary.

To browse to a site:

1. Navigate to the Site Level of Live Summary (see Navigating Between Summary Levels on page 80)
2. Right-click on the site or resource name and select **Browse:** from the pop-up menu

The site is then launched in your default Internet browser. This option makes viewing the content of a web page easy, and is also very useful for refining and checking profiles.

**Note:**

If you browse to a site, *Live* will show you visiting the site.

You can also launch an email to any recipient listed at the Site level. For more information see *Emailing Users in Live Summary*.

Adding Users or Sites to Aliases

In the Users Level or Site Level of Live Summary, you can add a user or site to a new or existing alias. You may want to do this to change a site or user's display name to something more meaningful.

For example, if you have a user that is currently displayed as john.s@webspay.com, you can create a new alias called 'John', and add the user to it. All instances of john.s@webspay.com will then be displayed as John.

To add a user or site to an alias:

1. Launch Live Summary, by right-clicking on the Live icon in the system tray and selecting Summary from the pop-up menu.
2. Navigate to Site Level for one of your users in Live Summary (see *Navigating Between Summary Levels* on page 80)
3. Right-click on a recipient or site in Live Summary.
4. Select **Add to alias...** from the pop-up menu to launch the Quick Alias dialog
5. The item that you right-clicked appears in the 'Item' drop down list. Edit this name if necessary
6. Select whether you want to add the item to a user name, site name or department alias type from the 'In' drop down list
7. Select an alias that you want to assign the item to from the 'As' drop down list. If you want to create a new alias, type its name in the drop down list
8. Click **OK** to assign the item to the alias

Note:

You can edit your aliases by going directly to Aliases in Live Configuration (see *About Aliases* on page 40).

Adding Keywords to Profiles

You can quickly assign keywords to profiles in Live Summary. While you are browsing the sites / recipients that members of your organization have accessed, you can quickly add any site or address to the include or exclude keyword list for any profile.

To add keywords to a profile from Live Summary:

1. Launch Live Summary, by right-clicking on the Live icon in the system tray and selecting Summary from the pop-up menu.
2. Navigate to Site Level for one of your users in Live Summary
3. Right-click a site/recipient and select **Add to profile...** from the pop-up menu. This launches the Quick Profile dialog
4. The site/recipient you selected appears automatically in the 'Keyword' drop down list. You can edit this keyword as desired.

For example, if you select the keyword www.webspay.com, you can edit this so that only 'webspay' is added to the profile.



5. Select whether you want to add the keyword to the profile's includes or excludes list using the appropriate radio buttons
6. Select the profile that you wish to add the keyword to from the Profile drop down list, or type a new profile into the list
7. Click **OK**

Note:

Changes to your profiles are only applied to the new hits coming in from your log files. Hits that have already been processed by *Live* do not trigger alerts if they match the keywords of a recently updated profile.



5. Live Options

Live Options

Live Options has four tabs that will enable you to configure various parts of *WebSpy Live*.

To access Live Options right-click the Live icon in your system tray and select 'Options' from the pop-up menu, or by going to **Tools | Options** from the main menu of Live Configuration.

The following tabs are available:

- **General:**
Adjust the way in which the values of size and time are displayed in Live Summary and Alert Details. For more information, see General Options on page 85.
- **Display:**
Specify the way information is displayed in Live. For more information, see Display Options on page 86.
- **Sound:**
Specify the sounds used to notify you of an alert. For more information, see Sound Options on page 87.
- **Locations:**
Define the default locations of all files used in Live. For more information, see Location Options on page 87.
- **Email:**
Configure Live to use your SMTP server when automatically sending emails see .

It is possible to reset all the options on the active tab of Live Options back to their original defaults by clicking on the **Defaults** button at the bottom left of the dialog.

General Options

The General tab of the Live Options dialog enables you to configure various options that dictate how *WebSpy Live* behaves and displays data.

To view General options:

1. Open the Live Options dialog by right-clicking the Live icon in your system tray and selecting **Options** from the pop-up menu
2. Click the General tab

On the General Options tab, you can:

- **Set Live to run every time you log into your computer**
Check the 'Launch WebSpy Live on startup' checkbox to automatically launch *Live* for you.
- **Set the user session threshold time.**
The threshold time is the maximum amount of amount of time between two hits before the second hit is considered part of a separate user session. The default is 5 minutes. Type the time in the format Hours:Minutes:Seconds into the 'User Session Threshold' edit box.



- **Specify how old data needs to be before *Live* clears it from memory**
Type the age data needs to be before it is deleted (in hours) into the 'Purge data older than' edit box.
- **Set the unit that *Live* uses to display size values**
Choose a unit (GB, MB, KB, B) from the 'Units used to display Size' drop down list.
- **Set the format for displaying elapsed times in *Live***
Elapsed times are displayed in Live Summary and in Alert Details dialogs. Select the desired format from the 'Units used to display 'Elapsed' drop down list.
- **Synchronize profiles and aliases between WebSpy Products**
If you are running another WebSpy product such as *WebSpy Analyzer* that also uses profiles and aliases, you can keep these files synchronized. This means that if you add an alias or profile in one WebSpy application, this change will also be made in the other WebSpy applications that have the synchronize option turned on. Check the 'Keep Profiles and Aliases synchronized between WebSpy applications' checkbox to turn this feature on.

Note:

You can change the name of Aliases in Analyzer Giga, but you cannot in Live, Analyzer Standard or Premium. For aliases to remain synchronised between Analyzer Giga and these applications, aliases must have the same name. For example, if you rename the Usernames alias in Analyzer Giga, your Usernames in Live will be deleted.

It is possible to reset all the General options back to the original defaults. To do this click the **Defaults** button at the bottom of the dialog.

Display Options

The Display tab of the Live Options dialog enables you to specify the way Live Status behaves and displays information.

To view Display options:

1. Open the Live Options dialog by right-clicking the Live icon in your system tray and selecting **Options** from the pop-up menu
2. Click the Display tab

On the Display Options tab, you can:

- **Set unseen alerts to flash**
You can enable alert icons to flash in Live Status and the system tray when an alert is raised. Check the 'Flash when there are unseen alerts' checkbox. Alert icons will stop flashing once they have been displayed, or marked as read.
- **Set Live Status to always display on top of any active windows**
Check the 'Display Live Status on top' checkbox to always display Live Status on top. Un-check this checkbox to enable other windows to display on top of Live Status.
- **Set Live Status to pop-up when an alert is raised.**
Check the 'Popup Live Status when an alert is triggered' checkbox to force Live Status to display when an alert is triggered. Leave this option un-checked if you do not want Live Status to pop-up. New alerts will still flash in the system tray providing the 'Flash when there are unseen alerts' option is checked.
- **Sort Active and Idle users**
You can sort Active and Idle users alphabetically, or by those who have been



most recently active or idle. Check the 'Sort users by most recently active' checkbox to display the most recently active or idle users at the top of the list in Live Status. Un-check this option to sort users alphabetically.

- **Set Live Status to hide automatically**

You can set Live Status to hide automatically after a set period of time. Check the 'Automatically hide Live Status after 'n' seconds' checkbox, and type a value for 'n' into the edit box. For example, to hide Live Status after 30 seconds, enter '30' into the edit box.

It is possible to reset all Display options back to the original defaults. To do this click on the **Defaults** button at the bottom left of the dialog.

Sound Options

You can associate a different sound with each priority level alert that is raised by *WebSpy Live* as well as to alert you when an input issue occurs.

To view Sound options:

1. Open the Live Options dialog by right-clicking the Live icon in your system tray and selecting **Options** from the pop-up menu
2. Click the Sound tab

To enable sounds in *Live* you need to ensure the 'Play a sound when an alert is triggered' checkbox is checked.

To discover what sound is used for each priority, select the alert type in the list and click the **Test** button. The sound will be played.

You can change the sound of any alert type.

To specify a new sound:

1. Select the sound for the priority level alert or input issue you want to change
2. Click the **Modify...** button on the tab page to launch the Open dialog
3. Navigate to the location of your new sound, select the sound and click on the **Open** button. The location of the new sound will be displayed in the Sound tab
4. Click **OK** to apply your changes and exit Live Options or click **Cancel** to exit without making any changes

Hint:

It is possible to reset all Sound options back to the original defaults. To do this click on the **Defaults** button at the bottom of the dialog.

Location Options

WebSpy Live uses a number of folders to save and store the information it needs to run. These folders are created automatically when the program is installed. You can view and modify the locations that *Live* used to store this information using the 'Locations' tab of the Live Options dialog.

To view Location options:

1. Open the Live Options dialog by right-clicking the Live icon in your system tray and selecting **Options** from the pop-up menu.
2. Click the Locations tab



The following items are displayed in the list on the Location tab, along with a corresponding location path:

- **Triggers**
The location path displayed next to 'Triggers' is where *Live* stores your *.Triggers files. These files are created when you save your triggers, and can be opened at any time.
- **State**
The location path displayed next to 'State' is where *Live* saves all information it has imported from your log files. The files in this folder can become quite large, if you have specified a long purge time in General Options (see General Options on page 85).
- **Profiles**
The location path displayed next to 'Profiles' is where *Live* stores your *.Profiles files. These files are created when you save your profiles and can be opened at any time (see About Profiles on page 33).
- **Loaders**
The location path displayed next to 'Loaders' is where *Live* stores the information required to read the data in your log files.
- **Aliases**
The location path displayed next to 'Aliases' is where *Live* stores your *.UserNames, *.SiteNames, *.Departments, *.FileTypes alias files. These files are created when you save your aliases and can be opened at any time (see About Aliases on page 40).
- **Sounds**
The location path displayed next to 'Sounds' is where *Live* stores the sounds used when alerts are triggered. You can change this default location here, or select other sounds on the Sounds tab of the Options dialog.
- **Help**
The location path displayed next to 'Help' is where *Live* stores the Help file. This Help file is launched whenever you press **F1**, and provides assistance for the area of *Live* you are currently working in.
- **Temp**
The location path displayed next to 'Temp' is the location *Live* uses to store temporary files that it creates when performing certain operations. WebSpy recommends that you do not change this location.
- **Logs**
The location path displayed next to 'logs' is the default log file location *Live* uses when you add a new input. This location path is updated when you add an input with a different location (see About Inputs on page 6).

You can modify any of these default locations. You may want to do this to store information, such as your aliases or profiles lists, in a more convenient location.

To modify a path for a folder:

1. Select the path you want to modify in the list
2. Click the **Modify...** button to launch the 'Browse for Folder' dialog
3. Navigate to the location of the desired folder and click **OK** to update the information

The new path to the folder will be displayed in the Locations tab.

It is possible to reset all Locations options back to the original defaults. To do this click the **Defaults** button at the bottom of the dialog.



Email Options

WebSpy Live uses SMTP (Simple Mail Transport Protocol) to automatically send emails when alerts are raised. You need to configure *Live* to use your SMTP server so that emails can be automatically sent when alerts are raised. This is done on the Email tab of the Live Options dialog.

To view Email options:

1. Select **Tools | Options** from the main menu. This launches the Live Options dialog
2. Click the Email tab

In Email options you need to:

- **Enter the server name**
Enter the name of your SMTP server into the 'Server' edit box. This is usually the same server you use to send and receive your own emails. If you do not know the name of your SMTP server, contact your system administrator or Internet service provider.
- **Enter the port number**
Enter the port number *Live* should use for sending SMTP emails into the 'Port' edit box. The standard port number for SMTP is 25 and this is the default. If are using a customized email system you can specify another port number.
- **Enter the sender email address**
In the 'Sender Address' edit box, enter the email address that should appear in the 'From' field on each email that *Live* automatically sends.

Once you have entered all the SMTP details, you can configure triggers to automatically send emails to users each time an alert is triggered. For more information, see Email Notification page of the Trigger Wizard on page 26.

Extensions Options

The Extensions Tab on the Live Option dialog, enables you to configure third party applications that you can launch from Live Status.

For example, Microsoft® Windows™ Remote Desktop Connection is a popular application for logging on to another computer running Microsoft® Windows™. Once configured on the Extensions tab, you can right-click an IP address in Live Status and Remote Desktop to that computer.

To view Extensions options:

1. Open the Live Options dialog by right-clicking the Live icon in your system tray and selecting Options from the pop-up menu.
2. Click the Extensions tab

To configure an extension for a third party application, you need to know the location of the application's executable file and the syntax of any command line expressions you can pass to it.

For example, the application name for Microsoft® Windows™ Remote Desktop Connection is 'mstsc.exe' and is usually located in the Windows System directory. You can run it from a command line prompt by entering the path and file name (for Windows XP this is "C:\Windows\System32\mstsc.exe"). You can also pass an IP address or computer name to the application by appending /v: to the command,



followed by the IP address or computer name you want to Remote Desktop to. For example, "C:\Windows\System32\mstsc.exe" /v:MyServer

Please consult your software vendor's documentation or technical support staff for executable file locations command line expressions.

Live can pass any item displayed in Live Status to a third party application configured on the Extensions Tab.

To configure a third party extension:

1. Go to the Extensions tab on the Live Options dialog and click the **Add...** button
2. Enter a name or description for the third party application into the Description field (for example, 'Remote Desktop'). This description will be added to the right-click menu on the Live Status dialog
3. Enter the command line expression required to launch the application and substitute %1 where you want Live to insert the item in Live Status (for example, "C:\Windows\System32\mstsc.exe" /v:%1). You can click the **Browse** button to navigate to the executable file
4. Click **OK**

You can edit or delete any extension by clicking the buttons at the bottom of the dialog.

To launch the application from Live Status:

5. Right-click an alert, or an active or idle user
6. Select the name you entered in step two above from the pop-up menu (for example, 'Remote Desktop'). The third party application will launch, and if %1 was entered in the command line expression in step 3 above, the item you right-clicked will be inserted into the command and passed to the application.

Other useful extensions you may like to add include:

Application	Command Expression	Description
Ping	<file path> /t %1 Example: "C:\WINDOWS\system32\ping.exe /t %1"	Ping tests whether a computer is reachable.
Trace Route	<file path> %1 Example: "C:\WINDOWS\system32\tracert.exe %1"	Trace route traces the routing path to a specific computer.

Appearance Options

The Appearance tab enables you to change the font and color that Live uses.

To change the font that Live uses to display text throughout the application, select the desired font from the 'Display Font' drop down list.

Note:

The application has been optimized for use with either Verdana or Tahoma. If you select another font, some text may be truncated.

To change the color theme that Live uses:

1. Click the **Auto** button. This launches the Color Chooser dialog.
2. Select the color to base the new color scheme on
3. Click **OK** on the Color Chooser dialog. The range of colors that Live will use are displayed in the Color Theme box. You can change any of these



individually by double-clicking the color and selecting a new one from the Color Chooser dialog.

4. Click **OK** on the Options dialog. You need to restart Live before the new color options take effect.
5. You can reset the color back to the default color scheme by clicking the Reset button.



6. Glossary

Glossary

Below is a list of terms that you may come across during the course of using *WebSpy Live*.

Active user

An active user is a user that is currently utilizing your network resources (such as Internet or Email). Active users are listed in Live Status.

Alerts

An alert notifies you when a user has breached the conditions of one of your triggers. An alert is represented by an alert icon in both your system tray and in Live Status under its associated trigger. For more information, see Alerts.

Aliases

Aliases enable you to group and represent data items in your log files such as users, IP addresses, and file types in more meaningful ways. For more information, see About Aliases.

Cumulative Triggers

Cumulative triggers enable you to set up alerts based on the total activity of your users. Cumulative triggers can be based on the total amount of time users have spent browsing, or the total size of resources they have downloaded. For more information, see About Triggers.

Departments

You can group users of your network resources into departments such as 'Accounts', or 'Management'. Department aliases can be selected when defining triggers to alert you to the Internet and network activity of members of a department. Departments is the only alias type available for filtering your inputs. For more information, see About Departments.

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 logs users on to domain accounts.

A backup domain controller is kept up to date with changes by the primary domain controller, and can be used if the primary domain controller is not available. *Live* uses Domain Controllers in the Department Wizard.

Excludes Keywords

Each of your defined Profiles has an 'excludes' keywords list. If a hit contains a word that matches any keywords in a profile's excludes keyword list, the hit will not be placed in the profile, even if it matches one of the profiles include keywords. For more information, see About Profiles. See also Includes keywords.

Failed Hit

A failed hit is a request for a web resource that has a status of failed or unsuccessful. A failed hit may occur 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.

Live displays all failed hits in red. The associated protocol icon for a failed hit will have a small red cross in the bottom left hand corner. You can filter out failed hits using the Input Wizard.

File Transfer

File transfer refers to Internet traffic transmitted via FTP (File Transfer Protocol). Files are usually transmitted on port 21. FTP is represented by its own protocol icon.

File Mask

A file mask is a group of letters, numbers or wildcard characters used for searching for files that fit that mask. Two wildcard characters can be used in a file mask, * and ?

* means any character or group of characters and ? means any single character.

For example, ??ab.log will pick up:

- cdab.log
- ciab.log

but not:

- cdaab.log
- cdrab.log

whereas, *ab.log will pick up all four.

You can use File Masks in the Input Wizard when choosing the log files you want to monitor.

File Extension

A file extension is the part of the filename consisting of the letters to the right of the period. The file extension identifies the type of file, so that your operating system knows what program to associate the file with. For more information see About File types.

File types

File types enable you to group file extensions, such as 'htm', 'xml', 'css', into a representative name, such as 'Web Document'. Defined file types can then be used in triggers. For more information see About File types.

Firewall

A firewall is hardware and/or software that separates portions of a network for security purposes or to protect the network server from damage or unauthorized access. A firewall prevents direct communication between network and external computers by routing communication through a proxy server outside of the network.

Gateway

A gateway is a device for exchanging data across incompatible networks that use different protocols. The term gateway is also used to describe entry and exit points for data on a network.

**Hits**

A hit is an individual file or item downloaded from an Internet site to your computer. One web page can be made up of many hits - the main page, the pictures on the page, the files on the page and so on.

This term can be confusing, since there are a couple of other meanings. For example, each item returned by a search engine is sometimes called a hit, and some people describe the number of visitors to a web site as a whole as the number of hits that site has had.

The actual content of a hit can vary widely. A hit may consist of a small picture or a large amount of text, or be very large or very small. Therefore, the effect of that single hit on an organization's total Internet usage can be hard to quantify.

In some situations, a user cannot control the content of the hits they access, such as in the case of advertising pop-up messages.

Idle user

An idle user is a user that has accessed your network resources, such as Internet or email, but is not currently using them. Idle users are listed in Live Status. See also Active user.

Includes Keywords

Each of your defined Profiles has an 'includes' keywords list. If a hit contains a word that matches any keywords in a profile's includes keyword list, the hit will be assigned to that profile. For more information, see About Profiles. See also Excludes keywords.

IP Address

An IP address is a unique string of numbers that identifies a computer on the Internet or on a network. It consists of four numbers between 0 and 255 separated by dots, e.g. 165.113.245.2. This number may be represented by a simple name e.g. www.webspy.com using IP address resolution. For more information, see Resolving IP Addresses.

Live Configuration

The Live Configuration dialog is the window 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. For more information, see About Live Configuration.

Live Status

Live Status is a dialog that displays a list of 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. For more information, see About Live Status.

Live Summary

Live Summary collates information about the Internet activity of all users being monitored. Using Live Summary, you can browse all network activity categorised by user and user sessions. For more information, see About Live Summary.

Log Files:

Proxy servers, Internet and mail gateways can usually be configured to keep a record of all traffic that passes through them. This information is kept in a file



called a log file. Different proxy servers have different methods of recording information to the log file. *WebSpy Live* is currently able to monitor over 80 popular log formats. For more information see About Inputs.

Mail

Mail refers to Internet traffic received via SMTP (Simple Mail Transfer Protocol). SMTP is a TCP/IP protocol used in sending and receiving email. However, since it is limited in its ability to queue messages at the receiving end, it's usually used with one of two other protocols, POP3 or IMAP, which let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending email and either POP3 or IMAP for receiving messages that have been stored for them at their local server. SMTP traffic is usually transmitted on port 25 and POP3 traffic is usually transmitted on port 110. Mail is represented by its own protocol icon.

Newsgroups

A newsgroup is a discussion about a particular subject consisting of emails 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). News is usually transmitted on port 119. News is represented by its own protocol icon.

Priority Levels

You can assign a priority level to a trigger to indicate how important the trigger is. A trigger assigned a low priority generates alerts represented by a green icon. Triggers assigned medium and high priorities generate yellow and red alerts respectively.



Low priority alert



Medium priority alert



High priority alert

Profiles

Profiles enable you to categorize the Internet resources accessed by members of your organization based on a list of keywords. Profiles can be used when defining triggers, to alert you of specific types of browsing or network activity.

Protocol

A protocol is a special set of rules or conventions for communication between two computers. Both computers must recognize and observe the protocol. Different types of Internet traffic use different protocols which are often described in an industry or international standard. Examples of protocols include HTTP (web traffic), SMTP (mail) and FTP (File Transfer). Live indicates protocols using different Protocol Icons.

Recipient

The recipient is the destination of specific data transfer. For example, a recipient can be the name of a person that received an email, or the name of a computer that is being accessed remotely via the telnet protocol.

Resource name

Resources are the individual items that you download from the Internet. The resource name is the part of the URL that comes after the first forward slash



character. For example, `www.webspy.com/logo.gif` indicates there is a resource called `/logo.gif` stored at the site `www.webspy.com`.

Session Trigger

A Session trigger alerts you to users that are browsing excessively, and/or downloading large amounts within the one session.

Secure web

Secure web refers to transferring Internet traffic using a form of encryption to increase the security of the transmitted information. Secure web uses the protocol 'Hypertext Transfer Protocol Secure' (HTTPS), and is usually transmitted on port 443. Secure web is represented by its own protocol icon.

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 be used in triggers. For more information, see About Site Names.

Single Hit Triggers

Single Hit triggers enable you to specify alert conditions based on individual hits in your log files. Using a Single Hit trigger, you can set up *Live* to raise alerts based on any or all of the following conditions: Size, Users, Site names, File types, Departments, Profiles, and Protocols. For more information, see About Triggers.

Site Level

The Site Level of Live Summary displays all the site names, or recipients for the session you selected at the User Session Level.

System Tray

Your computer's system tray is the small section of your taskbar (the gray section with the Start button) that usually shows your computer's clock.

Telnet

Telnet enables you to access another computer across the Internet, assuming you have permission to do so. Such a computer is known as a 'host' computer. Telnet is usually transmitted on port 23. Telnet is represented by its own protocol icon.

Triggers

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

URL

A URL can be thought of as the 'address' for any item available on the Internet. URL stands for either Universal Resource Locator or Uniform Resource Locator, depending on the source of the definition. A URL is the name or IP address of a site and resource that you would type into the Address box in your Internet browser, e.g. `http://www.webspy.com`.

Users

Users the people or computers that are currently utilizing your Internet or email resources. Depending on the information that your log files record, users can



include people browsing the Internet, sending email, or using other resources such as telnet. Users are listed in Live Status.

Users Level

The Users Level of Live Summary displays all users that have utilized your network resources, such as Internet and email. By clicking a user's name, you can drilldown to the User Sessions Level.

User names

User name aliases enable you to represent IP addresses, email addresses and computer names, by an actual user name such as 'Joe Citizen'. This user name is then used to represent all the Internet and network activity of this user in Live Status and Live Summary.

User Session

A user session is a period of time that a user spent using Internet or email resources without a break. If a user accesses two or more resources within a set threshold time, then *Live* groups those resources as part of a single user session.

For example, if a user browses to a web page, and then browses to another web page within the set threshold time, the two web pages are grouped into the one session. Any other network activity carried out by the user within this time frame, such as sending an email, is also grouped into the session.

A session ends when the user has been idle (not browsing) for longer than the set threshold time.

You can define how close two hits need to be before they are grouped into the same user session in General Options. The default is 5 minutes.

User Sessions Level

The User Sessions Level of Live Summary lists all the sessions for the user you clicked on at the Users Level.

Web

Web refers to any Internet traffic received via HTTP (Hypertext Transfer Protocol). HTTP is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web (WWW). It is usually transmitted on ports 80 or 8080. Web is represented by its own protocol icon.

Hits Explained

A hit is an individual file or item downloaded from an Internet site to your computer. One web page can be made up of many hits - the main page, the pictures on the page, the files on the page and so on.

This term can be confusing, since there are a couple of other meanings. For example, each item returned by a search engine is sometimes called a hit, and some people describe the number of visitors to a web site as a whole as the number of hits that site has had.

The actual content of a hit can vary widely. A hit may consist of a small picture or a large amount of text, or be very large or very small. Therefore, the effect of that single hit on an organization's total Internet usage can be hard to quantify.



In some situations, a user cannot control the content of the hits they access, such as in the case of advertising pop-up messages.



7. Index

- about
 - Aliases, 43
 - Departments, 61
 - File types, 56
 - Inputs, 6
 - Live Configuration, 5
 - Live Status, 73
 - Live Summary, 87
 - Profiles, 35
 - Site Names, 51
 - Triggers, 17
 - User Names, 45
 - WebSpy Live 2.1, 1
- adding
 - departments, 62
 - file types, 57
 - inputs, 7
 - keywords, 36
 - profiles, 35
 - profiles lists, 41
 - site names, 52
 - triggers, 18
 - user names, 46
 - users to departments, 82
 - users to user names, 82
- alert
 - about, 74
 - details, 76
 - icons, 74
 - priority, 74
- alert, 74
- aliases
 - about, 43
 - departments, 61
 - file types, 56
 - site names, 51
 - user names, 45
 - using wildcards, 46, 52, 62, 70
- aliases, 43
- automatic updates, 2
- browsing to urls, 91
- changing
 - trigger priority, 34
- creating
 - departments lists, 65
 - file types lists, 59
 - profiles lists, 41
 - site names lists, 54
 - triggers lists, 32
 - user names lists, 49
- cumulative triggers, 25, 30
- default
 - departments, 67
- deleting
 - departments, 64
 - file types, 58
 - inputs, 15
 - keywords, 38
 - profiles, 39, 40
 - site names, 53, 54
 - triggers, 31, 32
 - user names, 48
- department wizard
 - Department Conflict Page, 69
 - Domain Controller Page, 68
 - Final Page, 70
 - Groups Page, 69
 - Users Page, 69
 - using, 68
- department wizard, 68
- departments
 - about, 61
 - adding, 62
 - creating, 65
 - deleting, 64
 - editing, 63
 - exporting to CSV, 66
 - filtering by, 14
 - importing from CSV, 66
 - Importing Windows Users, 67
 - opening, 65
 - saving, 65
 - using the unassigned list, 63
- departments, 61
- disabling
 - inputs, 15
 - triggers, 33, 83
- disabling, 83
- dismissing alerts, 78
- display options, 94
- displaying
 - alert details, 76
 - information guides, 5
 - sidebar, 5
 - user details, 80
- displaying, 80
- domain controller, 67, 68
- editing
 - departments, 63
 - file types, 57
 - input, 14
 - keywords, 38
 - profiles, 38
 - site names, 53
 - triggers, 31
 - user names, 47
- email options, 97
- emailing



- automatic, 28
 - in live status, 81
 - in live summary, 90
- emailing, 81
- enabling
 - inputs, 15
 - triggers, 34, 84
- exporting
 - departments, 66
 - file types, 60
 - profiles, 42
 - site names, 55
 - user names, 50
- failed hits
 - description, 101
 - filtering, 12
- file locations, 96
- file types
 - about, 56
 - adding, 57
 - creating, 59
 - deleting, 58
 - editing, 57
 - exporting to CSV, 60
 - importing from CSV, 60
 - opening, 60
 - saving, 59
- file types, 56
- filtering
 - by departments, 12, 14
 - by profiles, 12, 13
 - by protocol, 12, 13
 - failed hits, 12
 - inputs, 12
- general options, 93
- getting started, 2
- glossary, 101
- hiding
 - information guide, 5
 - sidebar, 5
- hits, 107
- importing
 - departments, 66
 - file types, 60
 - profiles, 42
 - site names, 56
 - user names, 51
 - Windows Users, 67
- information guides, 5
- input issues, 16
- input wizard
 - Additional Filters Page, 12
 - Advanced Settings Page, 11
 - Department Filter Page, 14
 - Filters Page, 12
 - Final Page, 14
 - Folder Page, 9
 - Profile Filter Page, 13
 - Protocol Filter Page, 13
 - Using the Input Wizard, 8
- input wizard, 8
- inputs
 - about, 6
 - adding, 7
 - advanced settings page, 11
 - deleting, 15
 - disabling, 15
 - editing, 14
 - enabling, 15
 - issues, 16
 - log files, 8
 - wizard, 8
- inputs, 6
- IP address
 - definition, 101
- IP address, 47
- keywords
 - adding, 36
 - deleting, 38
 - editing, 38
 - tips, 37
- keywords, 38
- Live configuration
 - about, 5
 - about aliases, 43
 - about inputs, 6
 - about profiles, 35
 - about triggers, 17
 - options, 93
- Live configuration, 5
- Live Status
 - about, 73
 - active users, 80
 - adding users to Departments, 82
 - adding users to User names, 82
 - alerts, 74
 - collapsing and expanding groups, 75
 - disabling triggers, 83
 - dismissing alerts, 78
 - displaying alert details, 76
 - displaying user details, 80
 - emailing users, 81
 - enabling triggers, 84
 - idle users, 80
 - marking alerts as read, 79
 - navigating, 73
 - protocol icons, 75
 - resetting live, 85
 - shutting down live, 85
 - suspend, 84
 - unsuspend, 84
- Live Status, 73
- Live Summary
 - about, 87



- adding keywords to profiles, 92
- adding users to departments, 91
- adding users to user names, 91
- browsing to url, 91
- emailing users, 90
- site/recipient level, 88
- sorting columns, 89
- user sessions level, 88
- users level, 88
- using, 88
- Live Summary, 87
- location options, 96
- log files
 - adding, 7
 - properties, 10
- log files, 8
- minimum requirements, 1
- navigating
 - live configuration, 5
 - live status, 73
 - live summary, 87, 88
 - to URLs, 91
- opening
 - departments, 65
 - file types, 60
 - profiles lists, 41
 - site names, 55
 - triggers, 33
- options
 - about, 93
 - display, 94
 - email, 97
 - general, 93
 - locations, 96
 - sounds, 95
- options, 93
- overview, 1
- profiles
 - about, 35
 - adding, 35
 - adding keywords, 36
 - creating list, 41
 - deleting, 39, 40
 - editing, 39
 - filtering, 13
 - list, 40, 41
 - miscellaneous, 43
 - opening list, 41
 - renaming, 39
 - saving list, 40
 - tips, 37
- profiles, 35
- protocol
 - definition, 101
 - filtering, 13
 - icons, 75
- protocol, 101
- resetting live, 85
- resolving IP addresses, 47
- saving
 - departments, 65
 - file types, 59
 - profiles lists, 40
 - site names, 54
 - triggers, 32
 - user names, 49
- saving, 32
- session trigger, 24, 30
- shutting down live, 85
- sidebar
 - hiding, 5
- sidebar, 5
- Simple Mail Transfer Protocol, 97
- single hit triggers, 20, 29
- site names
 - about, 51
 - adding, 52
 - creating, 54
 - Deleting, 53, 54
 - editing, 53
 - exporting to CSV, 55
 - importing from CSV, 56
 - opening, 55
 - saving, 54
- site names, 51
- sound options, 95
- trigger wizard
 - cumulative trigger page, 25
 - departments page, 23
 - file types page, 23
 - finish page, 29
 - profile page, 24
 - protocol page, 24
 - session trigger page, 24
 - single hit trigger page, 20
 - site names page, 22
 - size page, 22
 - time page, 26
 - type page, 19
 - user names page, 22
 - using, 18
- trigger wizard, 18
- triggers
 - about, 17
 - adding, 18
 - cumulative, 19
 - deleting, 31
 - disabling, 33, 83
 - editing, 31
 - enabling, 34, 84
 - opening, 33
 - saving, 32
 - session, 19
 - single hit, 19



- wizard, 18
- triggers, 17
- unassigned list
 - departments, 63
 - user names, 46
- url
 - browsing to, 91
 - definition, 101
- user groups, 69
- user names
 - about, 45
 - adding, 46
 - creating, 49
 - deleting, 48
 - editing, 47
 - exporting to CSV, 50
 - importing from CSV, 51
 - opening, 50
 - resolving IP addresses, 47
 - saving, 49
 - using the unassigned list, 46
- using
 - wildcards, 46, 52, 62, 70
- views
 - Aliases, 43
 - Inputs, 6
 - Profiles, 35
 - Triggers, 17
- wildcards, 46, 53, 63, 70