



# Vantage Giga 2.2 User Guide

This document is intended to help you to start using WebSpy Vantage Giga. For more detailed information, please see the Vantage Giga help guide. This can be accessed via Help | Contents on the main menu.

Please send all issues or queries to WebSpy support ([support@webspy.com](mailto:support@webspy.com))

## Table of Contents

Table of Contents.....	1
Quick Start Tutorial .....	4
Importing log files .....	4
Running an Analysis .....	5
Browsing Summaries.....	6
Applying Aliases .....	8
Creating Reports .....	8
Generating Reports.....	9
Creating Tasks .....	10
Creating Organizational Structures.....	12
End of Tutorial.....	12
Registering .....	14
Vantage Giga.....	14
Upgrading.....	15
Upgrading from Previous Versions .....	15
Importing .....	17
Storages .....	17
Supported Log Files.....	17
Importing log files .....	17
Importing from a database .....	18
Importing Windows Event Logs .....	19
Advanced Importing Features.....	20
Storage Partitioning .....	21
Import Issues.....	21
Repairing Storages .....	23
Purging Storages .....	23
Summaries .....	24
Summaries .....	24
Running an Analysis .....	24
Running a Template Analysis .....	25
Precalculated Analysis.....	27
Summary Selection .....	28
Summaries created from URLs .....	28



- Schemas Explained..... 29
- Using Extensions ..... 30
- Reports..... 30
  - Reports..... 30
  - Creating an Analysis Template..... 32
  - Advanced Analysis Templates..... 33
    - Multi-key queries: ..... 33
    - Custom Aggregate Columns..... 34
  - Creating Trend Reports..... 35
  - Generating Reports..... 36
  - Collating Reports..... 37
    - Issues..... 38
  - Report Publishing..... 39
  - Report Documents ..... 40
  - Sessions and Browsing Time ..... 41
- Aliases ..... 42
  - Configuring Aliases..... 42
  - Adding alias groups and items ..... 43
  - Applying Aliases ..... 44
  - Using Wildcards ..... 45
  - Importing user names from your network ..... 46
  - Resolving IP Addresses..... 48
  - Troubleshooting Aliases..... 50
- Filtering ..... 51
  - Filtering ..... 51
  - Filter Expression Language ..... 52
    - Operators ..... 52
    - Functions..... 55
  - Having Filters..... 57
- Profiles ..... 58
  - Profiles ..... 58
  - Troubleshooting Profiles..... 59
- Tasks..... 60
  - Creating Tasks..... 60



- Organization..... 62
  - Organization..... 62
  - Importing your Organization..... 62
  - Importing and Exporting CSV Files ..... 64
    - CSV File Format ..... 64
  - Manually Creating your Organization ..... 65
    - Adding Groups ..... 65
    - Adding People (Users)..... 65
  - Deleting your Organization ..... 65
  - Converting to Aliases ..... 65
- Options..... 67
  - General Options ..... 67
  - Import Options..... 67
  - Summaries Options..... 68
  - Report Options..... 69
  - Color Options ..... 69
  - Path Options ..... 70
  - Email Options..... 70
  - Proxy Options..... 70
  - Cost Options..... 71
  - Module Options ..... 71
  - Performance Options..... 72
- Contact WebSpy..... 73
  - WebSpy North America ..... 73
  - WebSpy Europe..... 73
  - WebSpy Australia ..... 73
  - WebSpy Support ..... 73



## Quick Start Tutorial

Thank you for downloading or purchasing WebSpy Vantage Giga.

This tutorial will guide you through Vantage Giga 's main functions to help you start analyzing and reporting on your network log files.

These functions include:

- ➔ Importing your log files into a storage.
- ➔ Running an Analysis on your storage.
- ➔ Browsing your Summaries.
- ➔ Applying Aliases to your Summaries.
- ➔ Creating and Generating reports.
- ➔ Creating and running tasks.
- ➔ Creating your Organizational Structure.

### Importing log files

Vantage Giga enables you to analyze and report on the information contained within log files from common network devices such as proxy servers, firewalls, routers and gateways. For a list of supported formats, please see our website.

Before you can start analyzing and reporting on your network data, you need to import your log file data into a storage. Storages are optimized for quick data access so you can analyze and report on the data you're interested in faster.

This tutorial uses Sentinel.log included with the application you downloaded. Sentinel is a packet capture tool that you can install on your network to log network traffic.

**Try this:** Import log files into a storage:

1. Open Vantage Giga and click the **Storages** tab at the top of the screen.
2. Click the **Import logs** link in the 'Inputs' task pad. This launches the Input dialog.
3. On the **Storages** page, click the 'Create a new storage' radio button and enter the name 'My Storage' into the 'Name' edit box and click **Next**.
4. On the **Input Type** page, select 'Local or networked files and folders' and click **Next**.
5. On the **Input Specifications** page, select the format 'WebSpy' and click **Next**.
6. On the **Input Selection** page, click **Add | File**. Navigate to My Documents\WebSpy\Vantage Giga 2.1\Log, select **WebSpy Sentinel.log** and click **Open**.
7. Click **OK** on the Input Dialog to begin the import process.

*Optimization Tip:* You can get better performance out of Vantage Giga by configuring some of the settings on the 'Advanced' pages of the Inputs dialog.

While Vantage Giga imports data, it also runs an analysis on your data at the same time. This analysis is then saved back into the storage. This means that every time you want to analyze the storage, the first level of Summaries are instantly available (for more information see 'Precalculated Analysis').

As Vantage Giga imports WebSpy Sentinel.log, you can view the progress of the import on the Storages dock. The Storages dock displays the size of the log file (illustrated as size imported / total size), the number of records imported, and the percentage complete (shown in the progress column). It also shows the format of the log file. This is useful if you are importing multiple files of different formats.

Any issues that are encountered during the import are displayed at the bottom of the screen. For more information see Import Issues.

If any of the log files you have imported are still being updated by your logging device, you can easily import the new hits by clicking the Import all new data link in the 'Inputs' task pad. You can also clear all the imported hits and reload the information from your log files by clicking the Reload all link in the 'Inputs' task pad.

## ***Running an Analysis***

Running an Analysis is the process of reading the information in your storage and creating Summaries. Summaries can be interactively browsed and filtered using the Summaries dock, enabling you to drilldown into all areas of your network activity.

There are two types of Analyses:

### **Ad-hoc Analysis**

An Ad-hoc Analysis displays all 'top-level' or 'overview' Summaries that you can drilldown into. When you drilldown, Vantage Giga runs another analysis to retrieve the next group of Summaries from your storage. This type of analysis is great for interrogating your data on demand, but it is recommended that you only perform Ad-hoc Analyses on relatively small amounts of data, such as a day or a week, as the time it takes to perform each drilldown is affected by the amount of data Vantage Giga needs to analyze.

### **Template Analysis**

If you know what you want to analyze, such as the top 10 users and the largest file downloads, you can create an Analysis Template that displays just this information, and select it when running an analysis (see 'Running a Template Analysis'). This is effectively the same as running a report, only the results are displayed in the Summaries screen, allowing you to drilldown past what has been defined in your template.

You can select the type of analysis you want to run from the 'Analysis Type' page of the Analysis dialog.

***Try this:*** Run an Ad-hoc Analysis:

1. Click the **Summaries** tab at the top of the screen. This takes you to the Summaries dock.
2. Click the **New Analysis** link in the 'Summaries' task pad to launch the Create Analysis dialog.
3. Select 'My Storage' from the 'Storage' list.
4. Select 'Sentinel Web' from the 'Schema' list.
5. Click **Next**.
6. On the 'Analysis Type' page, select the 'Ad-hoc Analysis' radio button and ensure 'Use precalculated analysis if available' checkbox is checked



## 7. Click **OK**.

*Note: You can filter the analysis using the Filter page. For more information see 'Filtering'. You can also select the summaries that you want created using the summaries page. For more information see 'Summary Selection'.*

To create a Template Analysis, simply select the Analysis Template you want to run from the 'Template' drop down list on the Analysis Type page. For more information see 'Running a Template Analysis'.

Once your analysis has been run, you can interactively browse your Summaries.

### ***Browsing Summaries***

Once an Analysis has been run, Vantage Giga displays all the generated Summaries in the Summaries dock. The Summaries dock is a powerful interface that enables you to interactively analyze any information contained in your imported log files.

You can toggle the Summary Tree on or off using the button at the top of the screen. This lists all available Summaries and allows you to quickly jump to any Summary at any given drilldown level.

The right-hand pane also displays the list of Summaries for the schema you analyzed. Each Summary that contains more than one item is hyperlinked. Clicking a hyperlinked summary takes you to the corresponding summary where you can view the actual information.

Why aren't all my Summaries hyperlinked?

Notice that some of the summaries are not hyperlinked. These are the summaries that only contain one item. For example, if your storage only contains data from the one year, the Year summary will not be hyperlinked. Also notice that these summaries do not exist in the Summaries tree to the left. It does not make sense to drilldown into these items as the drilldown will only be reanalyzing the same data, and you will have exactly the same data set at the end of the drilldown. You can turn this feature off by selecting **Tools | Options | General** and uncheck the 'Hide Summaries with only one item' checkbox.

***Try this:*** Viewing Summaries:

1. Toggle the Summary Tree to on by clicking the button.
2. Click on **User Summary** in the Summary Tree. All the Users in your storage are displayed in the right hand pane. The number of Hits, Duration and Size of data transmitted are also displayed. The bottom right hand pane charts the top 25 items in the Summary.
3. Click the 'Hits' column heading to sort the Summary by this field. You will notice the vertical axis of the chart changes depending on the column you are sorting by.

You will notice that the Summary items in the right hand pane are hyperlinked. You can Drilldown into any Summary item to view Summaries that pertain only to that summary item.

***Try this:*** Drilldown into the User with the most number of Hits:

1. Click the User at the top of the list. Vantage Giga performs a drilldown and retrieves all the Summaries that pertain to that User.



2. Once the drilldown is complete, all the generated Summaries are listed underneath the User in the Summary Tree. Click next to the User to display the list of generated Summaries.

Once you have drilled down into a specific Summary item, you can view any Summary by selecting it in the Summary Tree. You can then repeat the Drilldown process with any of the Summary items displayed.

You can also Drilldown into a Summary item and jump to a specific Summary in one easy step using the right-click Drilldown function.

**Try this:** View the Site Profile for a specific User using the right-click Drilldown function:

1. Go to the **User Summary** by clicking this Summary in the Summary Tree.
2. Right-click on the first User in the list and select Drilldown from the pop-up menu.
3. Select the **Site Profile** Summary from the sub-menu.

Vantage Giga then performs a drilldown into the first User in the list and displays the Site Profile Summary.

Your drilldown path is displayed at the top of the right hand pane. You can easily jump back to a previous level by clicking the appropriate button in this drilldown path. You can also select a different Summary at any level by dropping down the drop down menu on any of these buttons at the top of the pane. You can also use the Summary tree to browse through all your drilldowns and Summaries.

You can also filter the list of summary items using the Find edit box at the top of the screen. Simply enter the term you want to filter by and click the Find button. To clear the filter, click the Clear button.

**Try This:** Find all Google web sites:

1. Click the **Site Name** summary in the Summary Tree.
2. Enter 'Google' into the edit box in the Find task pad. All the sites that includes Google are displayed in the list.

Once you are confident browsing your Summaries and drilling down into Summary items, you can utilize the Summaries dock to dynamically extract any information you want to analyze from your imported log files.

## Applying Aliases

When browsing your Summaries, you may want to group items together or represent some Summary items with more meaningful names. It is possible to perform these functions using Aliases.

For example, if you are viewing the Users contained within your User Summary, you may want to show the users actual name, or a shorten name to what is actually contained in the summary.

Some example Aliases are provided with the Vantage Giga install file you downloaded.

**Try this:** View the list of sample aliases:

1. Go to the Aliases dock by clicking the **Aliases** tab at the top of the screen.
2. Select any alias on the left to view the Alias Groups and Items in the right hand pane. The Alias Group is the name that will be displayed when any of the Group's Items match a Summary Item.

Any of these aliases can be applied to your Summaries in the Summaries dock using the Apply Aliases button on the toolbar in the right hand pane.

**Try this:** To apply Aliases to your Summaries:

1. Return to the Summaries dock by clicking the **Summaries** tab at the top of the screen.
2. Ensuring you have the 'My Storage' Analysis open in (created in the topic 'Running an Analysis'), select the **User Summary** in the Summary Tree.
3. Select 'Departments' in the Aliases task pad. All the Users are now represented by Department Names. Any Users that do not match a Department Name are grouped into the 'Unknown' Alias Group.

Aliases only apply to specific Summaries. This is configured on the Aliases dock and is explained in the topic 'Configuring Aliases'. When browsing your Summaries, only Aliases that apply to the Summary you are viewing can be selected in the Aliases task pad.

Once an alias has been applied, you can drilldown into it as you can with any other Summary item.

## Creating Reports

Vantage Giga enables you to produce report documents which you can send to other members of your organization, or archive.

The Reports dock enables you to configure, generate and collate reports as well as manage any existing reports. To access the Reports dock, click the Reports tab at the top of the screen.

All Report templates are listed on the Reports screen. Each template has an Edit button and a Generate button. At bottom of the screen is the Reports Manager pane that lists all previously generated reports.

You can create three types of reports:



### Analysis Reports

Analysis Reports enable you to define customized drilldown paths and Summaries. Analysis



Reports can be generated as a printable or online report, or viewed in the Summaries dock by running a Template Analysis (see 'Running a Template Analysis').

➔ **Trend Reports**

Trend Reports utilize statistical functions to calculate trends over time and predict values in the future (see 'Creating Trend Reports')

➔ **Comparison Reports**

Comparison Reports enable you to quickly define up to four drilldowns that you want to view. The process of creating a Comparison Report is explained below.

*Try this:* Create a quick Comparison report:

1. Click the **Reports** tab at the top of the screen. This takes you to the Reports dock.
2. Click the **Comparison Reports** tab at the top of the Reports screen.
3. Click the **New Template** link in the Templates task pad. This launches the Add Template dialog.
4. Type **My Comparison Report** in the Name edit box.
5. Select 'Sentinel Web' from the Schema drop down list.
6. Select the 'Comparison' radio button and click **OK**. A new Comparison Report Template is added to the Reports screen.
7. Click the **Edit** button on this template.
8. Ensure the '1' check box is checked enable the options for the first drilldown.
9. Select **User** from the Summary drop down list and select **Usernames** from the Alias drop down list. Select **Hits** from the Order By drop down list.
10. Check the '2' check box to enable the options for the second drilldown.
11. Select **Site Name** from the Summary drop down list and select **Hits** from the Order By drop down list. Leave the Alias drop down list set to none.

You have now configured a Comparison Report to drilldown into Users and display all the Site Resources for each one. You can now generate the Comparison Report to create a printable or online document (explained in the next topic 'Generating Reports').

Creating Trend Reports is explained in the topic 'Creating Trend Reports'.

You created an Analysis Report in the topic 'Creating an Analysis Template'. In addition to being able to run it in Summaries (see 'Running a Template Analysis') you can use it to generate a printable or online document (see 'Generating Reports').

## Generating Reports

Vantage Giga comes with a list of predefined report templates that you can generate. You can also create your own customized report templates.

Reports can be generated in the following formats:

- ➔ Web Document (MHT)
- ➔ Web Document (HTML, Loose files)
- ➔ Microsoft® Word Document (DOC)
- ➔ Text Document (TXT)
- ➔ Comma Separated File (CSV)



**Try This:** Generate a report:

1. Click the **Reports** tab at the top of the screen. This takes you to the Reports dock.
2. Select the tab that contains the Report Template you want to generate. In this case, select the **Comparison Reports** tab.
3. Select 'My Comparison Report' you created in the previous topic and click the **Generate** button located on the template. This launches the Generate Report dialog.
4. On the **Storages** Tab, check 'My Storage' that you created in the topic 'Importing log files'. Click **Next**.
5. On the **Format** Tab, click the **Web Document MHT** radio button. This will create an MHT file which is a packaged HTML document. Click **Next**.
6. On the **Publish** Tab, enter **My Generated Report** in the Name edit box. Check the 'Display the report using the default viewer' checkbox. Click **Next**.
7. Click **OK**.

Vantage Giga then generates the report and opens it using the default viewer for the format you selected in step 5.

Web Document MHT reports can be created as a packaged document (MHT) or as loose HTML, where all the graphics, styles and html pages are contained in a folder. MHT files can only be viewed in Microsoft® Internet Explorer. To view HTML reports in other browsers, generate them as loose HTML.

*Note: You can filter your reports using the Filter tab of the Generate Report dialog. For more information see Filtering. There are also other publishing options for reports such as emailing the report and copying it to a location. For more information, see Report Publishing.*

You can also create a separate report document for each item in a Summary. For example, you can create a separate report for each user or each department in your organization.

Vantage Giga also allows you to create reports that can be collated at a later stage. On the Publish page of the Generate Report wizard you can tag your report as available for collation. Reports that are available for collation are listed on the Collatable Reports tab of the Report Manager.

## Creating Tasks

Most actions you perform in Vantage Giga can be set to run automatically as part of a task. Importing data and running reports can therefore be done overnight, ready for you in the morning.

To create a task:

1. Click the **Tasks** tab at the top of the screen. This takes you to the tasks dock.
2. Click the **New Task** link in the Tasks task pad. This launches the Task Options dialog.
3. On the **General** page, enter a name for your task such as 'Weekly network usage report task'. Click **Next**.
4. On the **Schedule** page, check the 'Run task using Windows Task Scheduler' check box. The 'Key' that is displayed can be used to identify the Windows Job that gets created.
5. Select when you would like the task to run. For example, Start: 01/05/2005 at 06:00:00, Recurrence: Weekly - every 1 week on Fridays. Click **Next**.



6. On the **Authentication** page, enter the Windows user name and password that you want the task to run as, for example 'mydomain\john.citizen'.
7. Click **OK**.

*Tip:* You can receive notification each time your task runs, by configuring the task to send results to an email address using the 'Send task results by email' option on the General page.

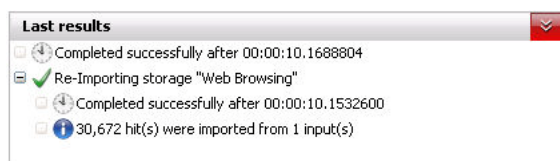
Now that you have created a task, you can add actions to the task.

To add actions to a task:

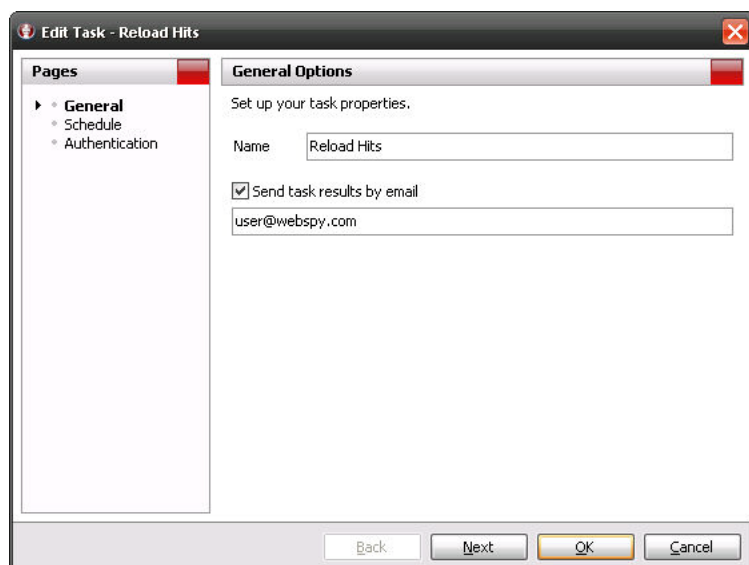
1. Select the task you created in the Tasks list.
2. Click the **Add Action** button in the right-hand pane and select the action you want to run.
3. The action will be added to the Actions list and will include a number of sub-actions. For example, the 'Run a comparison or analysis report' task action has two sub-actions: 'Select template' and 'Configure report'.
4. Double-click each sub-action to configure them.
5. Once you have added all the actions you want the task to run, and configured all the sub-actions, you can run the task by clicking the **Run Task** link in the Tasks task pad. This is a good way to test that the task is working as you expect.
6. Once you are happy with your task, you can leave it to run as scheduled.

*Tip:* Tasks are not only useful for running actions at convenient times, but also for setting up batch jobs. For example, if you always want to run a set of 10 reports, you can configure a task that runs these reports, and simply click the 'Run Task' button when you want to generate those reports. This is much more convenient than generating each report one by one. On the Task Options dialog, uncheck the 'Run task using Windows Task Scheduler' check box' so that the task doesn't try to run at a scheduled time.

Once completed, task results are displayed in the Last Results section of the selected task.



These results can also be sent by email. This option can be found on the General page of the task options, accessed via Edit Task.



## Creating Organizational Structures

Vantage Giga allows you to create users and organize them into multi-level groups representing your organizational structure. Users are mapped to information in your log files, enabling effective reporting on any organizational unit.

The Organization dock enables you to configure and manage your organization. To access the Organization dock, click the Organization tab at the top of the screen.

You can create your organizational structure by importing or by manually adding users and groups. Once you have an organizational structure you can assign aliases to individual users and groups.

*Try this:* Add a new user manually:

1. Click **Add Person**
2. Enter a display name for the user in the first entry box
3. Enter a login name and email address
4. Add any additional ways the user can be identified through log files in the Additional attributes section such as IP addresses, computer names, and authenticated usernames
5. The **Hierarchy** tab allows you to specify whether the user has either a manager or subordinates or both

You have now created a organization with one person. To learn more about representing your organizations structure view the 'Organization' topic.

## End of Tutorial

That concludes the quick start tutorial. You should now have enough information to start using Vantage Giga to analyze and report on your own log files.

If you require more information, please visit the WebSpy web site at [www.webspy.com](http://www.webspy.com). You can also contact WebSpy Support by emailing [support@webspy.com](mailto:support@webspy.com) or visiting our support page.



If you are testing a pre-release version of this product, such as a technology preview, beta, or release candidate, please submit your feedback using our beta feedback page.

If you would like to receive updates when pre-release versions are made available, as well as get access additional testing resources, please register as a WebSpy beta tester by submitting your details using our beta registration page.

Thank you for using WebSpy Vantage Giga.

## Registering

To register your copy of Vantage Giga you must request your unlock code. Your computer must have an active Internet connection to be able to register your software. You should only register the software on the computer you wish to use, as the unlock code generated will only work on that computer.

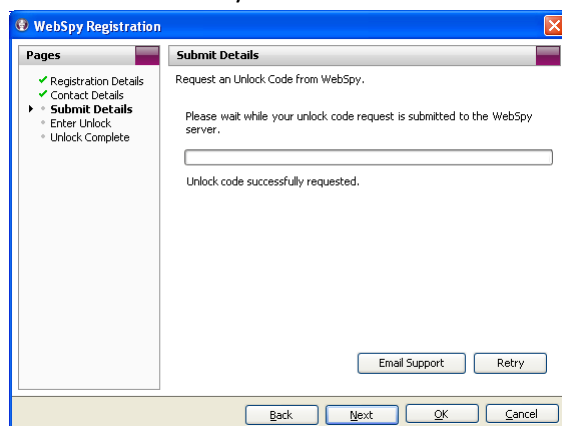
*Note: If you do not register your WebSpy software, your trial will run out 30 days from the date you first use the program.*

### Vantage Giga

To request your unlock code to register Vantage Giga:

1. Click on the **Register** button.
2. Enter your details into the **Registration Wizard**.

Please ensure that your E-mail address and serial number are correct.



3. After submitting your details, click **OK** to exit the wizard.

Your unlock code will be emailed to you within 36 hours from [support@webspy.com](mailto:support@webspy.com). Once you have received an email containing your unlock code you can finish the registration process.

To enter your unlock code and register Vantage Giga:

1. Go back to the Registration Wizard.
2. On the **Enter Unlock** page, enter your unlock code by copying and pasting it from the support email.
3. Click **OK** to finish the wizard.

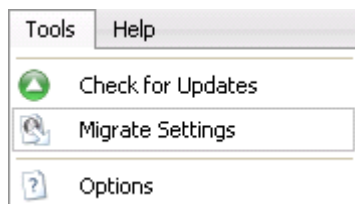
Congratulations, you have registered your copy of Vantage Giga.

## Upgrading

### Upgrading from Previous Versions

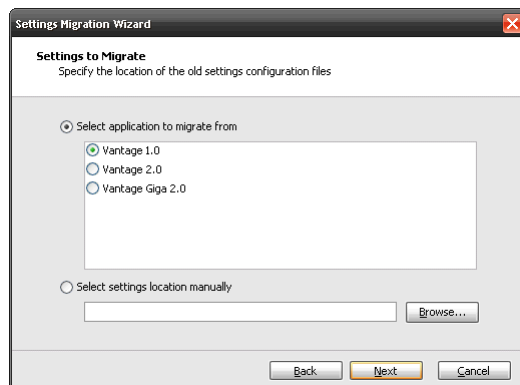
If you are upgrading from an earlier version of Vantage, you have the option to migrate your old settings files across. These files may include your Storages, Aliases, Profiles, Reports etc. This can be achieved through the Settings Migration Wizard.

The Settings Migration Wizard can be found under the Tools menu listed as Migration Settings.

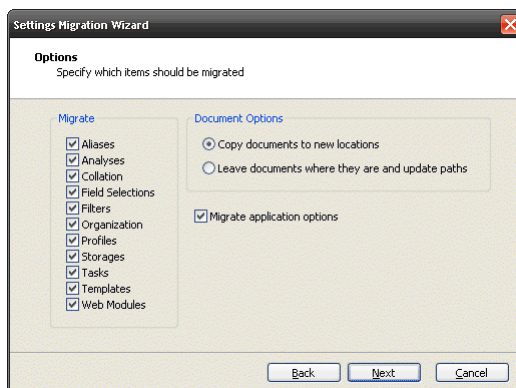


#### Using the Settings Migration Wizard

1. Open Vantage Giga.
2. Select **Tools | Migrate Settings**.
3. Click **Next** on the welcome dialog.
4. On the Settings to Migrate dialog you will notice two migration options, **Select application to migrate from** and **Select settings location manually**. If the previous version of Vantage is currently installed it will appear as an option under "Select application to migrate from". If Vantage is not installed you can browse to the .settings file. Select the previous install and click **Next**.



5. The **Options** screen allows you to select the files you wish to migrate. Under the **Document Options** you will notice two options. The first option, **Copy documents to new locations**, copies the files you wish to migrate into their corresponding locations in the new version of Vantage Giga. The second option, **Leave documents where they are and update paths**, sets Vantage Giga's folder paths to those of the previous version. The **Migrate application options** will set Vantage Giga's options to those of the previous version. Select the options you desire and click **Next**.



6. Proceed through and complete the rest of the wizard.

## Importing

### **Storages**

Vantage Giga imports log files created by your logging device into a special database file called a storage. Vantage Giga uses these storages for accessing the information in your log files quickly and efficiently when producing reports.

To access storages, click the Storages tab at the top of the screen. This takes you to the Storages dock.

To import log files into a new or existing storage, click the Import Logs link in the Inputs task pad. You can then import logs into this storage by clicking the Add button in the right hand pane. You can import text-based log files from a local, networked or FTP location (see 'Importing log files'), or data from SQL databases (see 'Importing from a database'). You can also import Windows Event Logs directly from PCs or Servers on your network.

Vantage Giga enables you to import an unlimited amount of log file data into a storage, and have an unlimited number of storages open at the one time.

Storages can be partitioned by any Summary to improve the speed of your analysis and reporting. For more information see 'Storage Partitioning'.

Storages are saved in the Storages folder by default with the extension \*.Storage. You can change the default location using 'Path Options'.

### **Supported Log Files**

Vantage Giga enables you to analyze and report on the information contained within log files from common network devices such as proxy servers, firewalls, routers and gateways.

For a list of supported log formats, please visit our supported log formats page <http://www.webspy.com/support/logformats.aspx>.

WebSpy is continuously writing support for new log files. If your log file is not supported, please email a log file sample to [support@webspy.com](mailto:support@webspy.com).

### **Importing log files**

Vantage Giga enables you to analyze and report on the information contained within log files from common network devices such as proxy servers, firewalls, routers and gateways. For a list of supported formats, please see 'Supported log files'.

Before you can start analyzing and reporting on your network data, you need to import your log file data into a storage. Storages are optimized for quick data access so you can analyze and report on the data you're interested in faster.

This tutorial uses Sentinel.log included with the application you downloaded. Sentinel is a packet capture tool that you can install on your network to log network traffic.

Try this: Import log files into a storage:



1. Open Vantage Giga and click the **Storages** tab at the top of the screen. This takes you to the Storages dock.
2. Click the **Import** logs link in the 'Inputs' task pad. This launches the Input dialog.
3. On the **Storages** page, click the 'Create a new storage' radio button and enter the name 'My Storage' into the 'Name' edit box and click **Next**.
4. On the **Input Type** page, select 'Local or networked files and folders' and click **Next**.
5. On the **Input Specifications** page, select the format 'WebSpy' and click **Next**.
6. On the **Input Selection** page, click **Add | File**. Navigate to My Documents\WebSpy\Vantage Giga 2.1\Logs, select **WebSpy Sentinel.log** and click **Open**.
7. Click **OK** on the Input Dialog to begin the import process.

*Optimization Tip:* You can get better performance out of Vantage Giga by configuring some of the settings on the 'Advanced' pages of the Inputs dialog.

While Vantage Giga imports data, it also runs an analysis on your data at the same time. This analysis is then saved back into the storage. This means that every time you want to analyze the storage, the first level of Summaries are instantly available (for more information see 'Precalculated Analysis').

As Vantage Giga imports WebSpy Sentinel.log, you can view the progress of the import on the Storages dock. The Storages dock displays the size of the log file (illustrated as size imported / total size), the number of records imported, and the percentage complete (shown in the progress column). It also shows the format of the log file. This is useful if you are importing multiple files of different formats.

Any issues that are encountered during the import are displayed at the bottom of the screen. For more information see 'Import Issues'.

If any of the log files you have imported are still being updated by your logging device, you can easily import the new hits by clicking the Import all new data link in the 'Inputs' task pad. You can also clear all the imported hits and reload the information from your log files by clicking the Reload all link in the 'Inputs' task pad.

### ***Importing from a database***

In addition to importing from a file system Vantage Giga also enables you to import from log data from an SQL database.

To import log data from a database:

1. Click the **Storages** tab at the top of the screen to go to the Storage dock.
2. Click the **Import Logs** link in the Inputs task pad. This launches the Input Dialog.
3. On the **Input Type** page of the Input Dialog, select 'Database Connection' and click **Next**.
4. On the **Loader Selection** page, select the Loader Group that corresponds to the log data you are importing (such as Microsoft ISA). Click **Next**.
5. On the **Input Selection** page, click the **Add** button. Select the type of database you're connecting to (MS SQL or MySQL), and enter the database server name.

*Note: If you're importing from a Microsoft ISA MSDE database, enter <servername>\MSFW. MSFW is the MSDE instance on Microsoft ISA.*



6. If required, enter a database or table filter to only select certain databases or tables on your server (such as those with 'WEB' in the name). Enter \* to select all databases and tables on your server. You have the option to remove them in the next step 8.
7. Select the authentication method you want to use to connect to your database server. Enter your username and password if you are not using Windows Authentication'. Click **OK**.
8. The **Input Selection** page now displays all the databases and tables in the databases you specified. You can add further databases, edit or delete existing databases using the buttons on the toolbar.
9. Click **OK** on the Input Dialog to begin the import.

As Vantage Giga imports log data from your database you can watch the progress of the import on the Storages dock. The Storages dock displays the number of records imported, the size of data imported, the number of rows imported, and the percentage complete (shown in the progress column). It also shows the format of the log file. This is useful if you are importing multiple files of different formats.

Any issues that are encountered during the import are displayed at the bottom of the screen. For more information see 'Import Issues'.

*Hint: As Vantage Giga imports from your database, you can monitor your PC's CPU and Memory usage in the status bar at the bottom on the window.*

If any of the tables you have imported are still being written to by your logging device, you can easily import the new hits by clicking the Import all new data link in the Inputs task pad. You can also clear all the imported hits and reload the information from your log files by clicking the Reload all button on the toolbar.

## **Importing Windows Event Logs**

Vantage Giga features improved Windows Event Log support.

Designed to provide an audit trail of system use, Event Logs record the actions that occur within your system, such as users logging in, failure of a component to start, or an attempt to print a document. Every event that occurs across a network can be recorded in an Event Log file. The list of events that are recorded by default can be modified to reflect the needs of your organization's system. For more information on Event Logs, please see our online whitepaper.

To import Event Log data:

1. Click the **Storages** tab at the top of the screen to go to the Storage dock.
2. Click the **Import Logs** link in the Inputs task pad. This launches the Input Dialog.
3. On the Input Type page of the Input Dialog, select 'Windows Event Log' and click Next.
4. On the Loader Selection page, select 'Microsoft Windows Event Log'. Click **Next**.
5. On the Input Selection page, click the **Add** button. Select where you would want to retrieve Event Logs from.

*Note: If you're retrieving Event Logs from multiple computers, click Add/Remove Computers and select which computers you would like to retrieve Event Logs from. You will also need to enter your username and password for authorization.*



6. Select the date format and time offset.  
*Note: You can also enter a Display Name for the computer/s you have selected.*
7. Click **OK** after you have finished configuring your settings.
8. Click OK on the Input Dialog to begin the Import process.

As Vantage Giga imports Event Log data you can watch the progress of the import on the Storages dock. The Storages dock displays the number of records imported, the size of data imported, the number of rows imported, and the percentage complete (shown in the progress column).

Any issues that are encountered during the import are displayed at the bottom of the screen. For more information see 'Import Issues'.

*Hint: As Vantage Giga imports from your database, you can monitor your PC's CPU and Memory usage in the status bar at the bottom of the window.*

You can easily import new hits from your Event Logs by clicking the Import all new data link in the Inputs task pad. You can also clear all the imported hits and reload the information from your Event Log files by clicking the Reload all button on the toolbar.

### **Advanced Importing Features**

When you import data into a storage, there are some advanced options you can take advantage of to optimize the speed of importing, analysis and reporting.

#### **The Field Selection Page**

This page enables you to exclude fields from being imported into your storage. The less fields you import, the smaller your storage will be and the faster your analysis and reporting will be.

#### **The Filters Page**

You can filter out unnecessary information from being imported into your storage. The less information you import into your storage, the smaller the storage will be and the faster your analysis and reporting will be. For information on configuring filters, see 'Filtering'.

#### **The Partitioning Page**

By default, storages are partitioned (internally split up) by date. This means that if you drilldown into date, Vantage Giga only has to read part of the storage to retrieve that information instead of the entire storage. If the first drilldown you do is into users, you can partition your storage by users so that Vantage Giga only has to read the storage partition for the user you drilled down into. This can greatly increase analysis and reporting speed. For more information see 'Storage Partitioning'.

#### **Set the date format**

If you know the date format recorded in your log files, set it when importing your logs. This prevents Vantage Giga from automatically detecting the date format which can slow down the speed of importing. When importing logs, and after clicking the Add button on the Input Selection page, simply click the More button to present the date format option. Note: If adding individual log files via Add | Add File, you need add the files, then click the Edit button to access this option.



## Storage Partitioning

By default a storage is partitioned by date. That means that if you drill down by a date, Vantage Giga does not have to read the entire storage to retrieve that information. It only has to look at the partition in the storage for the date you have drilled down into.

However sometimes you don't want to drill down into the Date Summary first. You may want to view a User's data for all dates. In this case, Vantage Giga needs to read the entire storage to get that information. Vantage Giga lets you choose the summary that your storage should be partitioned by.

You can also partition your storage by multiple summaries to further break your storage into more partitions. For example, you can select user and month to create separate partitions for each user's monthly traffic.

You can only choose the partitioning scheme on an empty storage. That is, before you import data, or when a storage has been cleared.

You can choose the partitioning of a storage when importing data for the first time or on the storage properties dialog.

To partition a storage when importing data:

1. Click the **Import Logs** link in the Inputs task pad to launch the Input dialog.
2. Ensure you configure the first three pages, then go to the **Partitions** page of the Input dialog.
3. Select the summaries you would like to partition the storage by.

To partition a storage using the storage properties dialog:

1. Select an existing storage that you have imported data into.
2. Clear the storage by clicking the **Clear** button on the toolbar of the left Navigation bar.
3. Right-click the storage and select **Properties** from the pop-up menu. This launches the storage properties dialog.
4. Click the **Partitioning** tab and check the Summaries you would like to partition your storage by.
5. You will then need to re-import your data by clicking the **Reload all** button in the right hand pane.

*Tip: Choose a summary that you frequently drilldown into that doesn't contain thousands of items. If you have more than 5000 partitions in your storage, importing can be quite slow as for each line in your log file, there is a calculation to work out what partition to file the hit under. Drilling down into anything other than the partitioned summary can also be slow. For example, if you partition your data by Source IPs and URLs you can end up with hundreds of thousands of storage partitions, each with very little data. If you don't drilldown into those partitions, Vantage Giga will have to read every single partition.*

## Import Issues

Occasionally, Vantage Giga encounters issues when importing information from log files.





Issues may occur for several reasons:

- ➔ You may have selected the wrong format for your log files.
- ➔ Your log contains a different date format than what Vantage Giga was expecting
- ➔ The log file format is not supported by Vantage Giga.
- ➔ The log file contains information that does not adhere to the structure Vantage Giga was expecting.

During an import, any issues that are encountered are displayed in the Issues pane at the bottom of the Storages dock.






An import will stop after a certain number total issues or a certain number of consecutive issues are encountered. These values are set in Import Options. The default values are 1000 total issues and 15 consecutive issues.

There are four severity levels of import issue:

Issue Severity Levels		
	Fatal	<p>Fatal issues indicate that nothing could be imported from a log source due to a problem with the log source itself. Fatal Issue example:</p> <ul style="list-style-type: none"> <li>➔ Could not find file.</li> <li>➔ No data stream available.</li> <li>➔ Could not access the input.</li> </ul>
	High	<p>High severity issues indicate a problem with hits in the log source that indicate that data has been imported incorrectly. Changes may need to be made to the import settings to correctly import the file.</p> <ul style="list-style-type: none"> <li>➔ Incorrect data type was returned (e.g. Expected number and found text).</li> </ul>
	Medium	<p>Medium severity issues indicate a problem with hits in the log source that may prevent them being imported, but does not mean the log source has been imported incorrectly. Medium severity issues include:</p> <ul style="list-style-type: none"> <li>➔ Expected n fields, n returned.</li> </ul>
	Low	<p>Low severity issues do not affect the import and can be thought of as informational messages rather than issues. Low severity issues include:</p> <ul style="list-style-type: none"> <li>➔ Couldn't connect to content file (when importing WebSpy Sentinel log files).</li> <li>➔ Automatically changed the date format from D/M/Y to Y/M/D.</li> </ul>

You can perform the following functions using the buttons on the toolbar of the Issues pane:

- ➔ **Dismiss**  
Removes the selected issue from the list

-  **Dismiss All**  
Removes all the issues from the list
-  **Email**  
Launches an email to WebSpy support that includes some system and loader information. Before sending this email to WebSpy Support, export your issues to a review file (\*.islog) using the Review button and attach this file to the email (see below).
-  **Review**  
You can export the list of issues to a review file with the extension \*.islog which can be viewed with any text editor such as notepad. This can be emailed to WebSpy support using the Email button.
-  **Copy**  
Copies the selected issue to the clipboard
-  **Help**  
Launches this help file

## ***Repairing Storages***

If WebSpy Vantage is terminated unexpectedly during an import, the storage can become corrupted. This can result from a lack of available memory, the process being terminated from the Task Manager or a system crash during the import.

Damaged storages are detected automatically and you have the option to repair them. Alternatively, you can manually check a storage and repair it on the Storage properties dialog.

To do this:

1. Click the **Storage Properties** link on the Storages tab.
2. Click on the **Diagnostic** tab.
3. Click **Repair Storage**.
4. Click **OK**.

If your storages are becoming damaged frequently and you are not sure why, please contact [support@webspy.com](mailto:support@webspy.com).

## ***Purging Storages***

The Purge Storage Wizard can assist in managing the log files in your storages by purging data according to date.

To do this:

1. On the Storages tab, click the **Purge Storage** link to launch the Purge Storage Wizard.
2. Select the storages to purge data from and then click **Next**.
3. Select the date range you want to purge.  
The default is 'All data' however you can use the radio buttons to specify a date range, purge data before or after a certain date or purge data older than a specific time period such as 1 month or 7 days.



You can also set up a task to purge storages on a scheduled basis, such as once a month or at an interval that matches your organization's data retention policy.

## Summaries


### *Summaries*

Summaries are the different categories of information that Vantage Giga can produce from the fields in your log file. Summaries include categories such as Users, Site Names, Protocols, Senders, Recipients, and Source Addresses.

Depending on the log file format you are importing, the list of summaries that are returned will vary. The list of Summaries for any given log format is called a Schema.

The Summaries view enables you to analyze these Summaries and drilldown into your imported data to find specific information.

To begin analyzing your data, you need to run an analysis. This launches the Analysis Dialog, which will guide you through the process of selecting the storages, schemas and Summaries to analyze.

Once your analysis is complete, the Summaries are listed on an Overview screen, and clicking a summary displays the underlying information. You can also navigate between Summaries using the Summaries Tree by clicking the  button. You can drilldown further into your data by right-clicking on any hyperlinked item and selecting Drilldown from the pop-up menu.

Any aliases that have been defined for the current summary can be applied by selecting them from the Aliases drop down list at the top of the screen. You can add any item to an alias or profile by right-clicking the item and selecting either the Add to alias or Add to profiles options.

You can also use an extension by right-clicking an item and selecting the Extensions option; your available extensions will be listed in the pop-up menu. You can manage your extensions from the Summary tab in the Options menu.

You can export any Summaries screen to a web document (HTML), word document (DOC), spreadsheet (CSV), and text (TXT) formats, by clicking the Export current view link in the Summaries task pad. You can export all Summaries at any given level by selecting their containing folder in the Summary Tree and clicking the Export all views link in the Summaries task pad.

### ***Running an Analysis***

Running an Analysis is the process of reading the information in your storage and creating Summaries. Summaries can be interactively browsed and filtered using the Summaries dock, enabling you to drilldown into all areas of your network activity.

There are two types of Analyses:

#### **Ad-hoc Analysis**

An Ad-hoc Analysis displays all 'top-level' or 'overview' Summaries that you can drilldown into. When you drilldown, Vantage Giga runs another analysis to retrieve the next group of

Summaries from your storage. This type of analysis is great for interrogating your data on demand, but it is recommended that you only perform Ad-hoc Analyses on relatively small amounts of data, such as a day or a week, as the time it takes to perform each drilldown is affected by the amount of data Vantage Giga needs to analyze.

#### **Template Analysis**

If you know what you want to analyze, such as the top 10 users and the largest file downloads, you can create an Analysis Template that displays just this information, and select it when running an analysis (see 'Running a Template Analysis'). This is effectively the same as running a report, only the results are displayed in the Summaries screen, allowing you to drilldown past what has been defined in your template.

You can select the type of analysis you want to run from the 'Analysis Type' page of the Analysis dialog.

**Try this:** Run an Ad-hoc Analysis:

1. Click the **Summaries** tab at the top of the screen. This takes you to the Summaries dock.
2. Click the **New Analysis** link in the 'Summaries' task pad to launch the Create Analysis dialog.
3. Select 'My Storage' from the 'Storage' list.
4. Select 'Sentinel Web' from the 'Schema' list.
5. Click **Next**.
6. On the 'Analysis Type' page, select the 'Ad-hoc Analysis' radio button and ensure 'Use precalculated analysis if available' checkbox is checked.
7. Click **OK**.

*Note: You can filter the analysis using the Filter page. For more information see Filtering. You can also select the summaries that you want created using the summaries page. For more information see Summary Selection.*

To create a Template Analysis, simply select the Analysis Template you want to run from the 'Template' drop down list on the Analysis Type page. For more information see 'Running a Template Analysis'.

Once your analysis has been run, you can interactively browse your Summaries.

## **Running a Template Analysis**

If you know what you want to analyze, such as the top 10 users and the largest file downloads, you can create an Analysis Template that displays just this information, and select it when running an analysis. This is effectively the same as running a report, only the results are displayed in the Summaries screen, which allows you to drilldown past what has been defined in your template.

*Note: Depending on the number of drilldowns and Summaries in the Analysis Template, Template Analyses may take longer to generate and may initially consume more RAM than Ad-hoc analyses.*

*Before you start: The Instructions below were created using the 'Tutorial' Alias. You should load this Alias to ensure the steps you make match the steps provided. Go to the Aliases dock, click Open Aliases, select Tutorial.Aliases. When prompted with*






*the Merge Alias dialog select 'No', please be aware that this will overwrite your currently open aliases. If you have made any changes to the current aliases that you wish to keep, we suggest you 'cancel' and 'Save aliases' first. This will allow you to restore your aliases at a later time.*

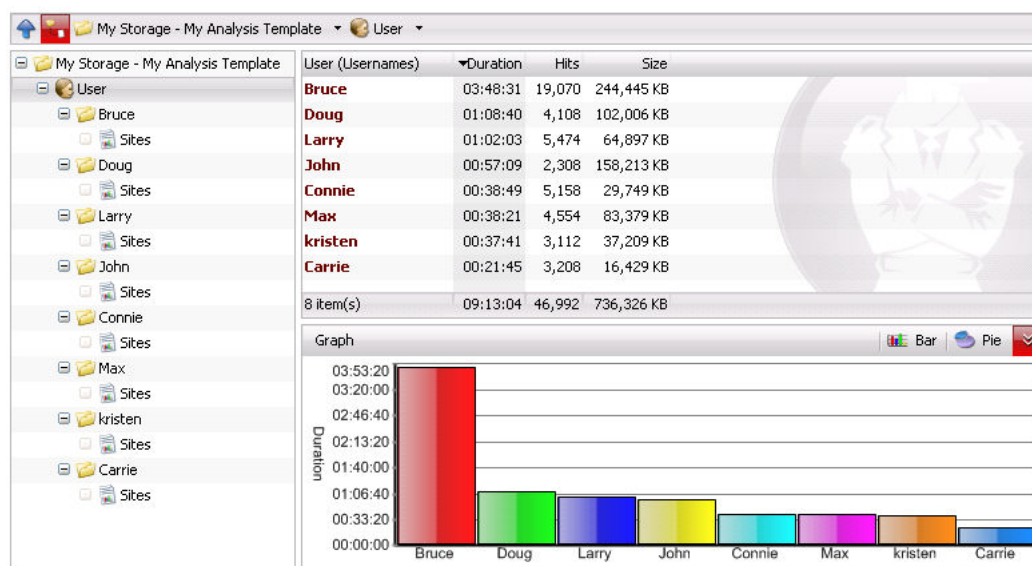
**Try this:** Run an Analysis using an Analysis Template:

1. Click the **Summaries** tab at the top of the screen. This takes you to the Summaries dock.
2. Click the **New Analysis** link in the Summaries task pad. This launches the New Analysis dialog.
3. On the **General** page, enter 'My Template Analysis' in the Name edit box.
4. Check the checkbox next to 'My Storage' in the Storage list.
5. Select 'Sentinel Web' in the Schema list. Click **Next**.
6. Click the 'Template-based Analysis' radio button and select 'My Analysis Template' from the Template drop down list.
7. Click **OK**.

All the summaries defined in 'My Template Analysis' appear in the Summaries dock.

**Try this:** Browse the summaries that were created in the Template Analysis:

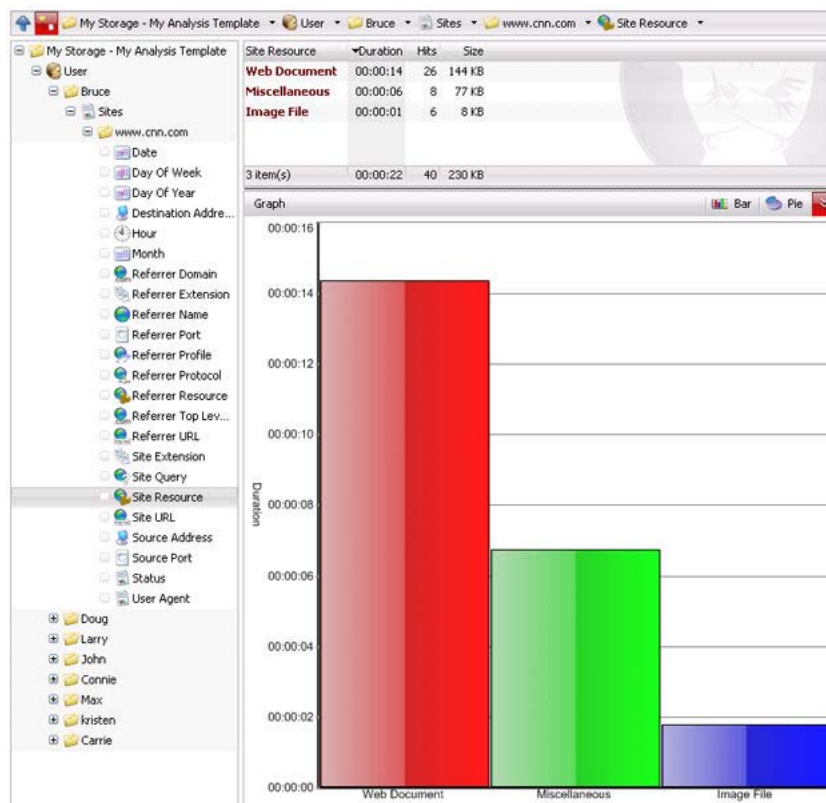
1. Ensure the Summaries Tree is on, by clicking the  button.
2. Click the  next to the Analysis to display the list of generated Summaries. You will notice that only the User Summary has been created and each User has been drilled down into.
3. Click the  next to any of these items in the Summary Tree to view the Sites Summary containing all the visited web sites for that User.



Although Template Analyses only display the precalculated Summaries and drilldowns as defined in the Analysis Template, you can still drilldown into any other Summaries. Vantage Giga will access the storage and retrieve the information for the specific Summary item that you drill down into.

**Try this:** Drilling down into Summaries not present in the Analysis Template:

1. Expand one of the User nodes and click its **Sites** summary in the Summary Tree.
2. Right-click any of the Sites in the right hand pane and select **Drilldown | Site Resource** from the pop-up menu. Vantage Giga will extract the Site Resources for the selected Site from your storage.



### ***Precalculated Analysis***

When Vantage Giga imports data, it also runs an analysis on your data at the same time. This analysis is then saved back into the storage. This means that every time you want to analyze the storage, the first level of Summaries are instantly available

The saved analysis is retrieved by checking the 'Use precalculated analysis if available' checkbox on the Analysis Type page of the Create Analysis dialog. (See 'Running an Analysis').

You may not want to retrieve the precalculated analysis if you have made changes to your Profiles. The Profiles summary is calculated when an analysis is run, so if you make changes to the keywords in your profiles, these changes will not be reflected until you run a fresh analysis. In this case, simply uncheck the 'Use precalculated analysis if available' checkbox to run a new analysis, or re-import your log files to refresh the precalculated analysis.

If you are re-running the analysis, you can save the new analysis back into the storage. This will replace any existing saved analysis in that storage. Simply check the 'Update precalculated analysis in the selected storage' check box.

Precalculated analyses are only used when running an An-hoc analysis on the Summaries screen. They are not used when running Template Analyses, or when running reports on the report screen. If you

never run ad-hoc analyses (if you just run reports or template analyses) you can turn off the analyze on import feature to gain speed when importing.

To turn off Analyze on import:

1. Select **Tools | Options** from the main menu
2. Select the **Import** tab
3. Un-check the 'Analyze data during import' checkbox

If you turn off this feature, Ad-hoc analyses will take longer to generate.

## Summary Selection

You can specify which summaries are automatically created when running an Adhoc Analysis, or when performing an interactive drilldown in a Template Analysis. Limiting the number of Summaries that are created can increase the speed of analysis and drilldowns.

To do this:

1. Click the **Summaries** tab at the top of the screen. This takes you to the Summaries dock.
2. Click the **New Analysis** link in the Summaries task pad. This launches the Create Analysis dialog.
3. Click the 'Summaries' Tab. This tab presents all the Summaries that can be created, as well as the aggregate columns for each of those Summaries.
4. Check the checkbox next to the Summaries and aggregates you would like created.







When the analysis is run, only the Summaries and aggregates you checked are created.

*Hint: The default Summary selection can be automatically altered to only show 'basic' Summaries. To do this, select Tool | Options from the main menu and go to the Summaries tab. Uncheck the 'Include advanced summaries in analyses' checkbox. Basic Summaries are suitable for most reporting and analysis requirements.*

## Summaries created from URLs

Any log format that contains a URL will produce a range of Summaries that can be built from that URL.

For example, the WebSpy Sentinel log format contain two URLs: Site Url and Referrer Url. When running an analysis on the Sentinel Web Schema, the following Summaries are created:

- |   |   |
|---|---|
|  Site Domain           |  Referrer Domain           |
|  Site Extension        |  Referrer Extension        |
|  Site Keywords         |  Referrer Keywords         |
|  Site Name             |  Referrer Name             |
|  Site Port             |  Referrer Port             |
|  Site Profile          |  Referrer Profile          |
|  Site Protocol         |  Referrer Protocol         |
|  Site Query            |  Referrer Query            |
|  Site Resource         |  Referrer Resource         |
|  Site Top Level Domain |  Referrer Top Level Domain |

- ➔ Site URL
- ➔ Referrer URL

The Site Url `http://www.webspy.com/download/index.aspx?key=5:80` will return the following Summaries and values:

- ➔ Site Domain: webspy.com
- ➔ Site Extension: .aspx
- ➔ Site Keywords: 5
- ➔ Site Name: www.webspy.com
- ➔ Site Port: 80
- ➔ Site Profile: My Organization
- ➔ Site Protocol: http
- ➔ Site Query: ?Key=5
- ➔ Site Resource: /download/index.aspx
- ➔ Site Top Level Domain: .com
- ➔ Site URL: `http://www.webspy.com/download/index.aspx?key=5`

*Note: The Profile Summary is not derived directly from the URL. Vantage Giga creates the Profile Summary by profiling the URL.*

## Schemas Explained

A schema is the list of Summaries that Vantage Giga can build given the fields available in any log file. Schemas are also used to separate logically different sets of information from a log file, such as web or email information.

For example, WebSpy Sentinel log files contain both Web and Email information. You can therefore analyze your Sentinel Web schema or your Sentinel Email schema and each schema has a different list of Summaries. These two types of information are separated into different Schemas as because it does not makes sense to drilldown from on into the other. For example, drilling down into email subjects and into web URLs associated with those email subjects does not make sense.

WebSpy produces a product called FlowMonitor that collects NetFlow data from a Cisco® router. These log files contain information regarding the traffic flowing on your router's interfaces. Below is the list of Summaries that make up the FlowMonitor Schema:

- ➔ Date\*
- ➔ Day of Week\*
- ➔ Day of Year\*
- ➔ Destination Addresses
- ➔ Destination AS
- ➔ Destination Port
- ➔ Destination Route Mask
- ➔ Hour\*
- ➔ Input Interface
- ➔ IP Protocol
- ➔ Month\*
- ➔ Netflow Device IP



- ➔ Next Hop IP
- ➔ Output Interface
- ➔ Source Address
- ➔ Source AS
- ➔ Source Port
- ➔ Source Route Mask
- ➔ TCP Flags
- ➔ Type of Service
- ➔ Week of Year\*
- ➔ Year

\* Vantage Giga builds summaries such as Day of Week, Day of Year, Hour and Month from any DateTime field in a log file. Vantage Giga also produces a range of summaries from any URL in a log file (see 'Summaries created from URLs').

For each of these summaries, Vantage Giga also produces the following Aggregate columns.

- ➔ Duration
- ➔ Packets Transmitted
- ➔ Size
- ➔ Hits\*\*

\*\* Hits isn't produced from a field in the FlowMonitor log file, but rather by counting each record for a particular item in the log file. For example, if you drilldown to the Source Address summary, this hits column will display how many log lines (records) were recorded against each Source IP address.

The above FlowMonitor schema is different to the schemas produced from other vendor's log files. Each schema is customized to get the most out of the log file you are importing.

## ***Using Extensions***

Extensions enable you to utilize computer network tools. The available default extensions include ping, nslookup and traceroute.

After you have run an analysis you can right click on any information and select the Extensions menu and run the desired tool.

You can also add extension by clicking Tools | Options and viewing the Summaries tab.

## **Reports**

### ***Reports***

Vantage Giga enables you to produce report documents which you can send to other members of your organization, or archive.

The Reports dock enables you to configure report templates which you can then generate on your open storages. You can also view previously created reports and collate reports using this dock. To access the Reports dock, click the Reports tab at the top of the screen.

You can create three types of reports:

➔ **Analysis Reports**

Analysis Reports enable you to define flexible customized Reports using any of the available summaries in a Schema. You can create an Analysis report with a flat list of Summaries, or specify drilldown paths such as "for each user, show me the top 25 sites". Analysis Reports can be generated as a printable or online report, or viewed in the Summaries dock by running a Template Analysis (see 'Creating an Analysis Template').


➔ **Trend Reports**

Trend Reports utilize statistical functions to calculate trends over time and predict values in the future (see 'Creating Trend Reports').

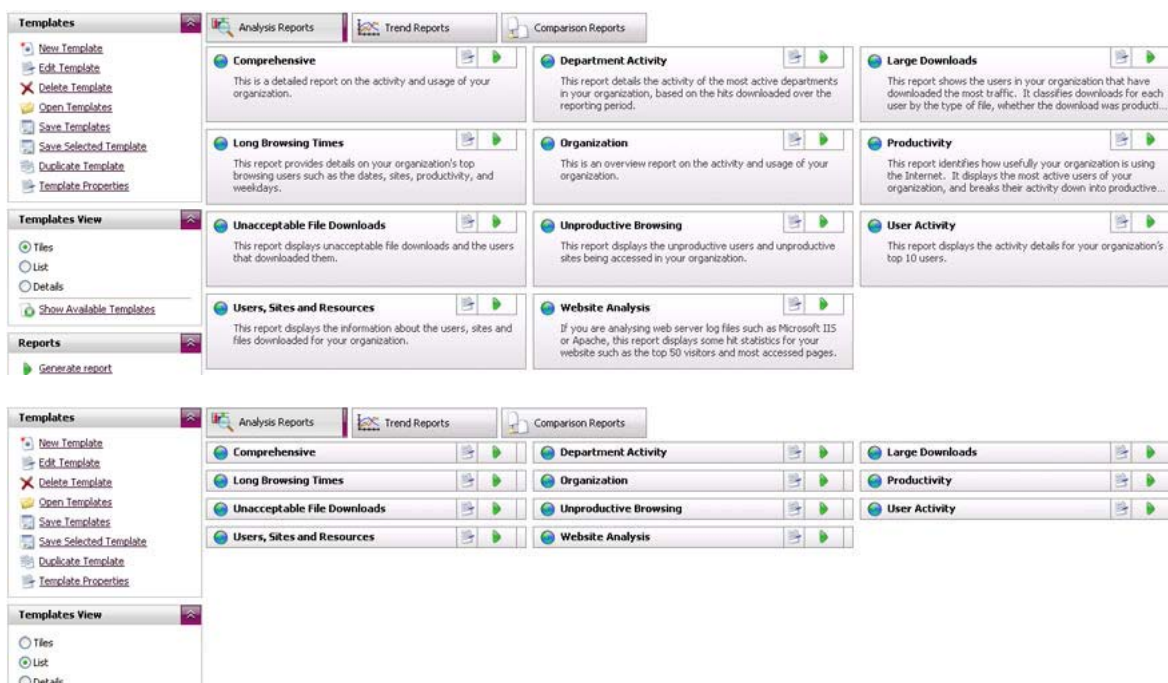
➔ **Comparison Reports**

Comparison Reports enable you to quickly define up to four drilldowns that you want to view. (see 'Creating Reports')

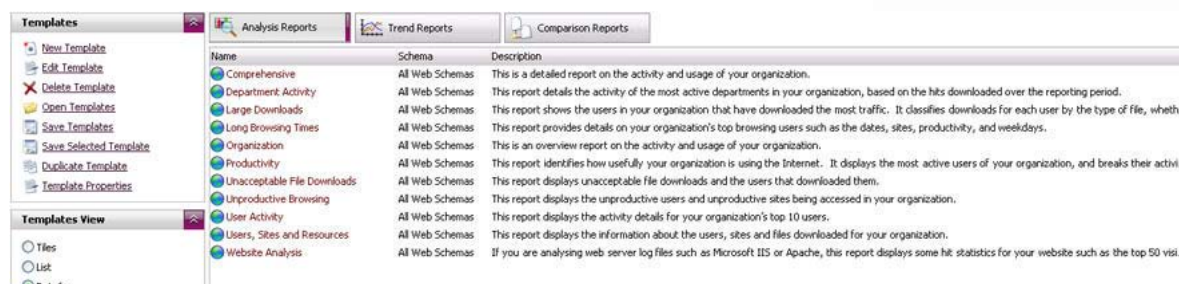
To access each type of report, simply click the corresponding tab at the top of the Reports dock.

You can either create a custom report for the log format schemas you are reporting on by clicking the **New Template** link in the Templates task pad, or generate one of the many sample reports. Simply click the Generate button  on the selected template (see 'Generating Reports').

To change the view of templates simply click on either Tiles, List or Details under the Templates view task pad.



The image shows two screenshots of the WebSpy interface. The top screenshot displays the 'Reports' dock with three tabs: 'Analysis Reports', 'Trend Reports', and 'Comparison Reports'. The 'Analysis Reports' tab is active, showing a grid of report templates. The 'Templates' task pad on the left includes options like 'New Template', 'Edit Template', 'Delete Template', 'Open Templates', 'Save Templates', 'Save Selected Template', 'Duplicate Template', and 'Template Properties'. The 'Templates View' section has radio buttons for 'Tiles', 'List', and 'Details', with 'Tiles' selected. A 'Generate report' button is visible at the bottom of the Reports dock. The bottom screenshot shows the same interface but with the 'List' view selected in the 'Templates View' section.



*Note:* Some of the sample reports may not be available to generate depending on the schema you are analyzing.

You can also produce a collated report from your existing reports.

## Creating an Analysis Template


An Analysis Template is a way of pre-defining the drilldown paths and Summaries you are interested in analyzing. Once defined, an Analysis Template can be used to generate a Template Analysis on the Summaries screen or to generate a Report such as a Web document or Microsoft® Word document.

**Try this:** Create an Analysis Template:

1. Click the **Reports** tab at the top of the screen. This takes you to the reports dock.
2. Click the **Analysis Reports** tab at the top of the Reports dock to view all existing Analysis Reports.
3. Click the **New Template** button in the left Navigation bar. This launches the Add Template dialog.
4. Enter **My Analysis Template** in the Name edit box.
5. Assuming you still have the storage 'My Storage' open that you created in the topic 'Importing log files', select the Sentinel Web Schema from the Schema drop down list.
6. Select the 'Analysis' radio button and click **OK**.

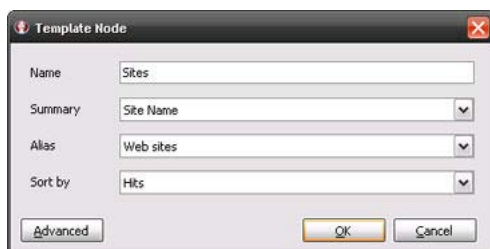
You now need to edit this template to define the information you want to report on.

**Try this:** Configure an Analysis Template to display the Sites Visited for each User:

1. Click the **Edit** button  on the 'My Analysis Template'.
2. You will see one item in the Template called 'My Analysis Template'. Select this item and click the **New Node** link in the Template Nodes task pad.
3. Click the **New Node** button on the toolbar. This launches the Template Node dialog.
4. Enter **User** in the Name edit box.
5. Select 'User' from the Summary drop down list.
6. Select 'Usernames' from the Alias drop down list.
7. Select 'Hits' in the Sort by drop down list.
8. Click **OK**.



9. Ensure the User node is selected and click the **New Node** button on the toolbar to launch the Template Node dialog again.
10. Enter **Sites** in the Name edit box.
11. Select 'Site Name' from the Summary drop down list.
12. Select 'Web Sites' from the Alias drop down list.
13. Select 'Hits' in the Sort by drop down list.
14. Click **OK**.



You now have an Analysis Template that will drilldown into each User and display the Web Sites visited by each one.

*Note: You can also set other properties for each node of your analysis template such as sorting, whether charts are displayed when the template is generated as a report, and filtering (see Filtering).*

You can also click the Advanced button when adding Template Nodes to access further options such as custom columns, charts, and filters. For more information see 'Advanced Analysis Templates'.

Now that you have created an Analysis Template, you can run it in the Summaries dock. This is explained in the next topic 'Running a Template Analysis'. You can also generate it as a printable or online document (see 'Generating Reports').

## **Advanced Analysis Templates**



Creating a simple Analysis Template was described in the topic 'Creating an Analysis Template'. Vantage Giga can create more complex analysis templates using the concepts of multi-key queries and custom aggregate columns.

### **Multi-key queries:**

When running an Ad-hoc Analysis, all the Summaries only have one 'key' column. For example, the Source IP Summary has the key column Source IPs. With Analysis Templates you can create Summaries that have multiple keys, enabling you to group information in customized ways.

**Multi-key Query Example:** You can define a Summary with both the Input Interface and Output Interface Summaries as keys. Each row in the Summary will be a unique combination of Input and Output interfaces enabling you to see the heaviest traffic flows through your router.

To create a Summary with a multi-key query:

1. Click **Reports** on the left Navigation bar. This takes you to the Reports dock.
2. Create a new **Analysis Template**.
3. Select the new Analysis Template in the left Navigation bar and click the **New Node** button in the right hand pane. This launches the Template Node dialog.
4. On the **General** page, Enter 'Multikey query' in 'Name' edit box.
5. Click the  button next to the Summary drop down list. This launches the Custom Summary dialog. This dialog enables you to select more than one Summary or Alias as the keys of the Summary.
6. Check the checkboxes next to Input Interface and Output interface. Each row in the Summary will be a unique combination of Input and Output interfaces
7. Click **OK** on the Custom Summary dialog. This takes you back to the Template Node dialog. Notice that both the Summary and Alias drop down lists are now disabled. To make changes to your Summary or Alias select, click the  button again.

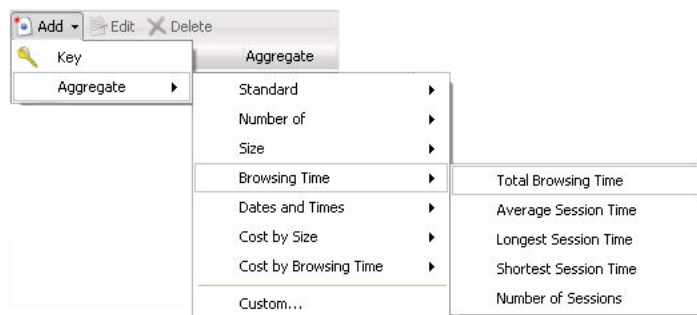
## Custom Aggregate Columns

When running an Ad-hoc Analysis, all the Summaries have a default number of other non-key columns such as packets, size and hits. With Analysis Templates, you can define other columns to display more information per Summary Item.

**Custom Aggregate Column Example:** You can define a custom aggregate column to display the Total Browsing Time.

To create a Summary with a custom aggregate column:

1. Open the Template Node dialog by adding a node to an Analysis Template or editing an existing node.
2. On the General page, ensure the node has a name and a Summary has been selected.
3. Click Add | **Aggregate** | **Browsing Time** | **Total Browsing Time** on the toolbar of the 'Columns' list.



You have now added a column to the summary that will show you the total browsing time.

*Note: The 'Calculate sessions' checkbox performs a session calculation on the selected field, using the aggregate function you selected. This allows you to add columns such as 'Total Browsing Time' or 'Average Browsing Time' to your template node.*

The Custom aggregate option will open the aggregate options dialog. This allows for a manual creation of an aggregate, as opposed to the automated process used through the flow-menu. You may wish to use the Custom aggregate option for when you need the aggregate to calculate the session for a different summary and alias to that of the node.

Once you are satisfied with your Summary and column selection for all nodes in the Template, you can generate the Analysis Template in Summaries or Reports.

## Creating Trend Reports

Trend Reports enable you to analyze fluctuations in Summaries and Summary items over time.

Trend Reports Example: You can plot the number of packets sent and received through each router interface over a period of time, enabling you to see patterns of traffic and make configuration adjustments.

To create a Trend Report:

1. Click **Reports** on the left Navigation bar. This takes you to the reports dock.
2. Click the **New** button in the left Navigation bar. This launches the Add Template dialog.
3. Enter 'My Trend Template' in the Name edit box.
4. Assuming you still have the storage 'My Storage' open that you created in the topic 'Importing log files', select the Sentinel Web Schema from the Schema drop down list.
5. Select the 'Trend' radio button and click **OK**.

You will notice that a new template is added under the 'Trend Reports' folder in the left Navigation bar and it is automatically selected. You now need to configure your Trend Report by adding Trend Elements. Each Trend Element creates a graph or number of graphs displaying Summary Item's activity over time.

To configure your Trend Report:

1. Ensuring 'My Trend Template' is selected in the left Navigation bar, click the **New Element** button on the toolbar of the right hand pane. This launches the Trend Element dialog.
2. On the **General** page, enter 'Department Activity' in the Name edit box.
3. Select 'User' from the Series ID Field drop down list. Select 'Department' from the Alias drop down list. This will create a series on the Trend Graph for each Department. Click **Next**.
4. On the **Time Axis** page, select 'DateTime' from the Time Field drop down list. This is the Field that will be used to chart time on the X-axis (only DateTime Fields are presented in this drop down list).
5. Enter '1' into the Time Unit edit box and select 'Hour' from the drop down list. For each hour in your data, a point will be plotted for each User. Leave the 'Limit chart length and wrap data' checkbox unchecked. Click **Next**.
6. On the **Aggregates** page, check 'Hits' and 'Size' in the Aggregates list.



7. Select 'Hits' in the list and click the **Edit** button on the toolbar. This launches the column Dialog. Click **options**, check the 'Create a separate graph for each value in the Series ID column' checkbox and click. Click **OK**.
8. On the **Trending** tab, select the 'Linear' trend type and forecast forward 24 hours by entering **24** into the Forward spin box.
9. Click **OK** on the Trend Element dialog.

You have now added a Trend Element that will create graphs to display the number of hits and the total size transferred by each Department. For the Hits aggregate, a separate graph will be created for each Department. For the size aggregate, all series will be put on the same graph. A linear trend line will be drawn through each series on each chart and the chart will be extrapolated 24 hours into the future.

*Note: If you do not check the 'Create a separate graph for each value in the series ID column' checkbox in step 7, all the Departments will be displayed as separate series on the one graph for the Hits aggregate.*

Now you have created and configured a Trend Report, you can generate it by clicking the 'Generate Report' button on the toolbar. For more information see 'Generating Reports'.

*Note: You can filter the Trend element using the Filter tab. For more information see 'Filtering'.*


## Generating Reports

Vantage Giga comes with a list of predefined report templates that you can generate. You can also create your own customized report templates.

Reports can be generated in the following formats:

- Web Document (MHT)
- Web Document (HTML, Loose files)
- Microsoft® Word Document (DOC)
- Text Document (TXT)
- Comma Separated File (CSV)

**Try This:** Generate a report:

1. Click the **Reports** tab at the top of the screen. This takes you to the Reports dock.
2. Select the tab that contains the Report Template you want to generate. In this case, select the **Comparison Reports** tab.
3. Select 'My Comparison Report' you created in the previous topic and click the **Generate** button  located on the template. This launches the Generate Report dialog.
4. On the **Storages** Tab, check 'My Storage' that you created in the topic 'Importing log files'. Click **Next**.
5. On the **Format** Tab, click the **Web Document MHT** radio button. This will create an MHT file which is a packaged HTML document. Click **Next**.
6. On the **Publish** Tab, enter 'My Generated Report' in the Name edit box. Check the 'Display the report using the default viewer' checkbox. Click **Next**.
7. Click **OK**.



Vantage Giga then generates the report and opens it using the default viewer for the format you selected in step 5.

Web Document MHT reports can be created as a packaged document (MHT) or as loose HTML, where all the graphics, styles and html pages are contained in a folder. MHT files can only be viewed in Microsoft® Internet Explorer. To view HTML reports in other browsers, generate them as loose HTML.

*Note: You can filter your reports using the Filter tab of the Generate Report dialog. For more information see Filtering. There are also other publishing options for reports such as emailing the report and copying it to a location. For more information, see Report Publishing.*

You can also create a separate report document for each item in a Summary. For example, you can create a separate report for each user or each department in your organization.

Vantage Giga also allows you to create reports that can be collated at a later stage. On the Publish page of the Generate Report wizard you can tag your report as available for collation. Reports that are available for collation are listed on the Collatable Reports tab of the Report Manager.

## Collating Reports

Vantage Giga enables you to produce report documents which can be collated at a later date. When creating a report you can add a tag which will mark the report as collatable. You can view your collatable reports from the Report Manager dock, via the Collatable Reports tab. You will only be able to see reports that have been marked as available for collation.

**Try this:** Generate two collatable reports:

1. On the **Reports** Dock, select **Large Downloads** and click the **Generate report** link
2. Select the storage you created earlier and click **Next**
3. On the **Formats** page, select the **Web Document (HTML, loose files)** format and click **Next**
4. On the **Publish** page, enter a name for the report and check that the 'Make this report available for collation' checkbox is ticked
5. Enter **Large Downloads** as the tag for your report and click **Next**
6. On the **Documents** page, ensure that the 'Create a separate report document for each:' checkbox is marked
7. Select **Month** from the summary drop-down box and select **Months** from the aliases drop-down box
8. Proceed through the wizard and then click **OK** to generate your report

After your report has been generated, click on the Collatable Reports tab in the Report Manager to view your collatable reports. The left hand panel contains a tree listing your tags with the reports templates used to generate collatable reports underneath. When you select a template the collatable reports will be displayed in the right hand panel. You can delete these reports individually by selecting a report and clicking on the delete button, or you can delete all the displayed reports by clicking the clear button.

**Try this:** Collate two reports:

1. On the **Reports** Dock, click **Collate report**



2. Select **Large Downloads** and click **Next**
3. On the **Date Range** page, select Absolute and set the date range to 30/05/07 - 1/06/07 and click **Next**
4. Select the Web Document (HTML, loose files) format and click **Next**
5. On the **Publish** page, enter a document name
6. Select any publishing options you would like and click **Next**
7. Enter your email options if you wish to email the report and click **OK**

You report will now be collated.

## Issues

### Modifying Report Templates

If you generate a range of reports and tag them as collatable, then modify the report template, and generate another range of reports with the same tag, only the latest version of the template will be used in the final collation. If you have deleted a node from a report template, the information generated from that node will not be in the final report.

### Count Distinct Aggregate

Report nodes that contain a column based on the Count Distinct aggregate (such as 'number of sites', 'number of users', etc) cannot be collated. For example, if one collatable report contains a list of users with a 'number of sites' column, such as

User	Number of Sites
John	35
Stef	25
Chris	18

Then the next collatable report contains this information:

Stef	35
Chris	19
John	3

You cannot calculate the number of sites that each user visited as sites could easily be replicated in the reports.

If your report template contains the Count Distinct aggregate, the values for that column in the final collated report will be 0. A warning is displayed when you tag a report for collation that contains a count distinct aggregate.

### Average Aggregate

For columns based on the 'Average' aggregate, the values in the final collated report will be the average of these.

For example, if a report with:



User	Average Size	Average Browsing Time
John	15MB	00:09:00

is collated with a report where the values are:

User	Average Size	Average Browsing Time
John	80MB	00:06:00


Then the values in the final report will be 47.5MB and a browsing time of 00:07:30.

These figures are slightly different than the values in a report generated on the original data.

## Report Publishing

Once you have Created a report template, there are various publishing options you can configure when generating the report. Report publishing options are selected on the Generate Report dialog.

To access the Generate Report dialog:





1. Click the **Reports** tab at the top of the screen. This takes you to the Reports Docks.
2. Click the **Generate** button  on any of the available Report templates.

The Storages, Formats, and Filters tabs enable you to specify the storage to report on, the output document format and any filters respectively.

*Note: If you select HyperText Markup Language document on the Format tab, you can also choose to generate the report as Loose HTML files. This will create a HTML file as well as a folder containing all the resources the report requires, such as graphics, styles and other HTML pages. This option is useful if you want to view the report in a browser other than Internet Explorer, as MHT files are not currently supported by any other browser.*

Most other publishing options are selected on the Publish page of the Generate Report dialog.

The Publish page has the following options:

-  **Document Name**  
The 'Document Name' text box defaults to the name of your Report Template, however you can rename it as desired each time you generate the report.
-  **Prefix with the current date**  
You can prefix the current date to the report name each time it is generated. This is useful to create a document with a unique name if you are creating the same report each day.
-  **Create a separate document each for each top level summary item**  
Instead of creating one document containing all data, you can create separate documents for each summary item. For example, you can create a separate report document for each user, or each department.
-  **Display the report using the default viewer**  
If this option is selected, once the report is created, it will automatically launch in the default

viewer, such as Internet Explorer, Microsoft® Word or Excel. Leave this option unchecked if you want the report to be created, but want to view it at a later stage.

➤ **Copy the report to a location**

All reports are saved into the folder defined in Location Options. You can use this option to copy the report to another location if you wish such as an intranet site.

➤ **Compress the report using ZIP**

On the Publish Tab you also have the option to Compress the report using ZIP. This option when checked will compress the generated report and any associated files into one zip file.

The Email tab of the Generate Report dialog enables you to send the report via email to any specified email address.

To send the report by email:

1. Click the **Email** page of the Generate Report dialog
2. Check the 'Send the report(s) by email' checkbox
3. Enter the email addresses you want the report to be emailed to in the 'To', 'Cc' and 'Bcc' edit boxes. You can enter multiple email addresses separated with a comma or semi colon.
4. Enter the subject line for the email in the 'Subject' edit box. This defaults to the name of your Report Template.

You will need to configure some options such as your SMTP server for the emailing functionality to work. Simply click the Email Options... button to do this (see 'Email Options')

Once you are satisfied with all your Report publishing options, click OK on the Generate Report dialog to generate the report.

## **Report Documents**

When generating reports, you can create a separate report document for each item in a selected summary or alias. For example, if you have created an alias to group your organization's traffic into Departments, you can create a separate activity report for each Department. You can then send these reports to the managers of each department.

To create a separate document for each item in a summary or alias:

1. Launch the Generate Report dialog on the Reports dock (see 'Generating Reports').
2. Click the **Documents** page and check the 'Create a separate report document for each item in:' checkbox.
3. Select the Summary that you want to create a separate document for. For example, selecting 'Source Address' will create a separate document for each Source Address in your storage.
4. Select any aliases you want to apply. For example, you can configure a Subnet alias to group IP addresses into locations. Selecting the Subnet alias will create a separate document for each of your locations or Subnets.
5. It is often useful to limit the number of documents being created by specifying a 'having' criteria. For example select packets in the Column drop down list, select the Top N radio button and enter 10 into the edit box. This will limit the number of reports to '10'. That is, the top 10 summary items that have transmitted the most packets.



6. Once you have made your selections on the **Documents** tab, and the other pages of the Generate Report dialog have been configured appropriately, click **OK**.

The report documents will be named in the format [Report Name] (Summary Item). For example 'My Analysis Template (London)'.

## **Sessions and Browsing Time**

Vantage Giga enables you to calculate sessions on any summary. This allows you to view a user's Total browsing time or Average browsing time.

Browsing Time is calculated by looking at the date/time stamp of each hit in a log file, and then grouping the hits into 'sessions'. Whether a hit falls into a particular session or not is based on a special 'threshold time'. The default session threshold time in Vantage Giga is 5 minutes, but you can change this in Tools | Options | General.

If two hits are written to the log file within five minutes of each other, they are grouped into the same session. If another hit is made within five minutes of the second hit, this too is added to the same session. If there is a break of more than five minutes with no hits made, then the previous session is 'closed off'. A new session is started when the next hit is made.

The total time of one session is calculated as the time between the first and last hits of the session. You can add an aggregate column in an [Analysis Template](#) to display the Sum, Average, Minimum or Maximum session times for any summary item (such as users, departments or user agents).

To add a browsing time column to an Analysis Template node:

1. Create an Analysis Template (see 'Creating an Analysis Template')
2. Add a new node to the analysis template by clicking the **New Node** link in the Template Nodes task pad.
3. Select the summary you want to display browsing time for, such as 'Users' from the Summary drop down list.
4. Click the **Advanced** button. This launches the Advanced Template Node dialog.
5. On the General page click **Add | Aggregate | Browsing Time | Total Browsing Time** on the toolbar of the 'Columns' list.
6. If the summary you selected in step 3 is different to the summary that sessions should be calculated for, double click the Total Browsing Time aggregate to display the aggregate options dialog, then check the 'For' check box and select the summary that session should be calculated for, along with any aliases.  
*View example: If you selected Departments in step 3 (Users aliased by Departments), most departments are likely to have one long session as at least one person in the department will be browsing at any given time. What you want is browsing time to be calculated as the sum of each individual User's browsing sessions within each department. You would therefore select the Users summary here on the Aggregate dialog.*
7. Click **OK**.

The new browsing time column appears in the 'Column' list. You can use this column on the other pages of the Analysis Template dialog for charting, sorting and filtering.



*User browsing example: If a user browses to a website and then walks away from their computer for an hour, no time will be added to that user's browsing time while they are away from their PC. Only the initial 2 seconds to open the website and download the resources will be added to their browsing time. Note: Time may be added to their Browsing Time if the website they have opened has self-refreshing banner ads or tickers.*

Browsing Time should not be confused with Download Time. Download Time is the time taken to download a resource from the web site. Total Download time is the sum of the Download Times for all the resources downloaded by a user or from a site.

## Aliases

### Configuring Aliases

Aliases enable you to provide an alternative name for a Summary item or group of Summary items.

For Example: By applying the 'Subnets' alias to your Source IP Address Summary, you can group your Source IP Addresses according to your organization's subnets. Alternatively you can apply the 'Websites' alias to view the resolved Site names instead of IP addresses.

You can quickly alias any Summary item using the Quick Alias function in the Summaries dock.

To use the Quick Alias function

1. Click the **Summaries** tab at the top of the screen. This takes you to the Summaries dock.
2. Drilldown into a summary and right-click on a Summary item you want to alias. This launches the Quick Alias dialog.
3. Select **Add to alias** from the pop-up menu.
4. Select the alias you want to add the Summary item to from the 'In Alias' drop down list.
5. Enter the desired display name for the Summary item in the 'As' edit box.
6. Click **OK**.

The Summary item will now be displayed as the name you entered in step 5 above. If this is not the case, ensure you have applied the alias by selecting the appropriate alias in the Aliases task pad.

You can also configure your aliases manually using the Aliases dock.

There are two types of aliases:

#### **String Aliases**

String Aliases can convert any Summary item into a meaningful display name as long as the summary item exactly matches an item in an alias group.

#### **IP or Subnet Aliases:**

IP or Subnet Aliases can only be applied to Summary items that are IP addresses. An IP or Subnet alias can contain subnet expressions as alias items, such as 192.168.0.0\24. Using binary arithmetic, an IP or Subnet alias evaluates whether an IP address belongs to any of its configured subnets and aliases the IP addresses appropriately.

To add a String alias:

1. Click the Aliases tab at the top of the screen. This takes you to the Aliases dock.
2. Click the New Alias link in the Aliases task pad.
3. Enter a name and a description for the alias.
4. Select whether you want the alias to apply to another alias or to a summary:
  - ➔ **Applying to another alias**

You can apply String aliases to other Aliases. For example, if you have first configured an alias that groups IP addresses into Subnets, you can apply an alias to that list of Subnets to further group them into Departments or Locations. To apply the alias to another alias, select the 'Use alias relationships' radio button and select the alias from the drop down list.
  - ➔ **Applying to a summary**

If you want to apply the alias directly to a Summary, select the 'Apply alias to selected summaries' radio button and select the schema that contains the summaries you want to apply the alias to from the 'Schema' drop down list. Select the summaries you want to apply the alias to and click the left arrow button to move them to the list on the right.
5. If you want to group all Summary items that do not match any of your alias groups into a single name, check the 'Group unresolved into a single name' checkbox and enter the name you would like to use, such as 'Miscellaneous' or 'Unknown'.
6. If you want to use Wildcard characters when adding items to the alias, such as \* and ?, check the 'Use wildcard matching' check box.
7. Click OK.

To add a Subnet or IP alias:

1. Click the **Aliases** tab at the top of the screen. This takes you to the Aliases dock.
2. Click the **New subnet Alias** link in the Aliases task pad.
3. Enter a name and a description for the alias.
4. Select the schema that contains the summaries you want to apply the alias to from the drop down list. Select the summaries you want to apply the alias to and click the left arrow button to move them to the list on the right.
5. If you would like to group all Summary items that do not match any of your alias groups into a single name, check the 'Group unresolved into a single name' checkbox and enter the name you would like to use, such as 'External' or 'Unknown'.
6. Click **OK**.

Once an alias has been added, you need to groups and add items to the alias. See 'Adding alias groups and items'.

### ***Adding alias groups and items***

Once an alias has been added (see 'Configuring Aliases'), you need to add alias groups to the alias, and Summary items to the alias groups. If you apply aliases, when browsing Summaries or generating reports, any Summary item that matches an item is displayed with its corresponding group name.



For Example: The IP Protocols alias has an alias group called 'ICMP' and the Summary item assigned to it is '1'. When you apply the IP Protocols alias when browsing Summaries or generating reports, 'ICMP' will be displayed wherever the Summary item '1' is encountered.

To add groups and items to an alias:

1. Click the **Aliases** tab at the top of the screen. This takes you to the Aliases dock.
2. Select the Alias in the list that you want to add groups or items to.
3. Click the **Add Group** button in the Groups task pad.
4. Enter the desired alias group name in the 'Key' edit box. This is the name that will be substituted for any matched Summary items.
5. Click the **Add** button on the toolbar.
6. Enter the Summary item you want to add to this alias group. If the Alias is an IP or Subnet Alias, you can enter a subnet expression in the format <Network Address>\<Network bits> such as 192.168.0.0\24 (this is the same as the subnet 192.168.0.0 with the subnet mask 255.255.255.0). If the Alias is a String alias, you can use the wildcard characters \* and ?.
7. Click **OK**.

You can also use the Unassigned List to help add items to your alias groups. The Unassigned List displays all the Summary items that do not match any of the alias' groups. You can then drag these Summary items to the appropriate alias group.

To add items to alias groups using the Unassigned List:

1. Select the alias in the list that you want to add groups or items to (See 'Configuring Aliases').
2. Click the **Show unassigned** link in the Groups task pad. Using your list of Open Storages, Vantage Giga retrieves the Summary items that do not match any of the items in the selected alias' groups.
3. Once the Unassigned List has been built, simply drag items from the unassigned list to the appropriate alias group.

You can also add an item in the Unassigned List to a new group by right-clicking the item in the unassigned list and selecting Add as new group. If you have selected more than one item in the Unassigned List, you can add each one to a separate group by selecting Add as multiple groups from the pop-up menu. This adds new alias groups with the same name as the Summary item, that can then be renamed.

## Applying Aliases

When browsing your Summaries, you may want to group items together or represent some Summary items with more meaningful names. It is possible to perform these functions using Aliases.

For example, if you are viewing the Users contained within your User Summary, you may want to show the users actual name, or a shorten name to what is actually contained in the summary.

Some example Aliases are provided with the Vantage Giga install file you downloaded.

*Try this:* View the list of sample aliases:



1. Go to the Aliases dock by clicking the **Aliases** tab at the top of the screen.
2. Select any alias on the left to view the Alias Groups and Items in the right hand pane. The Alias Group is the name that will be displayed when any of the Group's Items match a Summary Item. Configuring this list of Aliases is explained in the topic 'Configuring Aliases'.

Any of these aliases can be applied to your Summaries in the Summaries dock using the Apply Aliases button on the toolbar in the right hand pane.

**Try this:** To apply Aliases to your Summaries:

1. Return to the Summaries dock by clicking the **Summaries** tab at the top of the screen.
2. Ensuring you have the 'My Storage' Analysis open in (created in the topic 'Running an Analysis'), select the **User Summary** in the Summary Tree.
3. Select 'Departments' in the Aliases task pad. All the Users are now represented by Department Names. Any Users that do not match a Department Name are grouped into the 'Unknown' Alias Group.

Aliases only apply to specific Summaries. This is configured on the Aliases dock and is explained in the topic 'Configuring Aliases'. When browsing your Summaries, only Aliases that apply to the Summary you are viewing can be selected in the Aliases task pad.

Once an alias has been applied, you can drilldown into it as you can with any other Summary item.

## Using Wildcards

A Summary item needs to exactly match an item in an alias group for it to be represented by the group. Defining your aliases can therefore be a time consuming task.

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

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

A wildcard is a special character that represents information that is allowed to change from hit to hit.

Wildcard example: If you want to alias all hits to your company's web site, 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 web site will therefore be associated with the alias you are defining.

There are two types of wildcard characters in Vantage Giga:

### **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.

*Asterisk: \*@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.

*Question Mark: john?webspy can represent john@webspy, john.webspy, and john-webspy*



*Important: The use of wildcards can slow performance when browsing your data in Summaries and producing reports, especially when analyzing a large volume of data.*

For Wildcards to function correctly, you must set the 'Use wildcard matching' option on the Alias' configuration dialog (see 'Configuring Aliases').

## **Importing user names from your network**

User names in your log files may be in an unfriendly format, such as MYDOMAIN\user007. You may wish to translate these into more readable names, and you may have the information to do this already on your network. So, how can you import this information into Vantage Giga?

There are two main ways to import user names into Vantage Giga:

-  Using the simple Import from Windows domain dialog
-  Using the more flexible Import from LDAP dialog.

*Note: The Import from LDAP functionality is complex, and will require some experimentation. An LDAP browsing tool, such as Microsoft's® ADSIEdit, may be useful.*

If neither of these methods suits the data in your log file, you may be able to get data from your network into a CSV file, and open this file using the Open button on the Aliases dock. For information on the format of this CSV file, export one of your current aliases to a CSV file using the Export to CSV button and examine it's contents.

To import user data from a Windows domain:

1. Select the **Aliases** tab from the top of the screen.
2. Click the **Import from Windows domain** button in the toolbar at the top of the left Navigation bar. This launches the Import Windows Users dialog.
3. Select a domain controller. Usually, you can choose the 'Use the primary domain controller' option.
4. Select an alias to import user names to. If you have an alias called Usernames, this would be a good choice.
5. Select an alias to import user groups to. If you have an alias called Departments, this would be a good choice.

*Note: only aliases that are based on the user names alias you selected will appear in this list. If there are no aliases in this list, and you want to import departments, then click Cancel, double-click your desired departments alias, click 'Use alias relationship', and select your user names alias in the drop-down.*

6. Click **OK**.



Your user names alias should now contain a list of friendly user names, and their corresponding unfriendly names and email addresses. Your departments alias should contain a list of all the groups on your Windows domain, and a list of users belonging to those groups.

*Note: When you use your departments alias, Vantage Giga can show each user as being in at most one group, so you may wish to delete some of the items that have been imported into your departments alias, leaving only the genuinely useful ones. For example, if you have a group called 'All Users', containing a list of all users, this is unlikely to be useful so you should delete it.*

You may also need to ensure that your Usernames alias is bound to the appropriate summaries. To do this, double-click your Usernames alias, and check the list of summaries it applies to. Add and remove summaries as necessary.

To import data from an LDAP directory:

1. Select the **Aliases** tab from the top of the screen.
2. Click the **Import from LDAP** button in the right pane. This launches the import from LDAP dialog.
3. On the **Aliases Selection** page, select the alias that you would like to import to. Click **Next**.
4. The **Object Selection** page enables you to choose what you want to import from your LDAP directory. You can either select Import Windows Users, which uses a pre-defined LDAP query, or you can set up your own LDAP query (this requires a knowledge of LDAP query syntax, which is beyond the scope of this document.) Click **Next**.
5. The **Group Creation** page controls how items in your alias will be named.
  - If you select 'Use the container's name', then an object in your LDAP tree whose parent is 'Users' would be imported to an alias item called 'Users'.
  - If you select 'Use a property of the container', then you must enter the property to use, such as 'canonicalName', or 'name', or 'ou'.
  - If you select 'Create groups based on the name of the object', then an object in your LDAP tree called 'CN=John Smith' would be imported to an alias item called 'John Smith'.
  - If you select 'Create groups based on a property of the object', then you must enter the property to use, such as 'sAMAccountName', or 'user', or 'cn'.

Click **Next** once you have made your selection on the Group Creation page.

6. On the **Alias Items** page, select what you would like to be imported within each alias item. If you would like the account name and email address for each object imported, then check the 'Import the object's Windows account and mail attributes' (these are the same values you get in the simpler Import from Windows domain dialog explained above). If your logs have user account names prefixed with a domain name, then check 'Prefix the account name with the default domain'. If you would like other values from the LDAP object imported (such as sn, userPrincipalName, etc.) add them to the list.

*Note: If you haven't checked Import the object's Windows account and mail attributes and you haven't added anything to the list, nothing will be imported into your alias items.*

Click **Next**.

7. On the **Advanced** page, you can specify a server to be queried or use the default. You can specify a sub-part of the LDAP tree to search, or use the whole tree. For the sub-tree (or whole



tree) that you've selected, you can specify that the search should go all the way to the leaves of the tree, or only to immediate children.

8. Click **OK**.

The import should then commence and your alias will be populated with a list of items and values for those items.

## Resolving IP Addresses

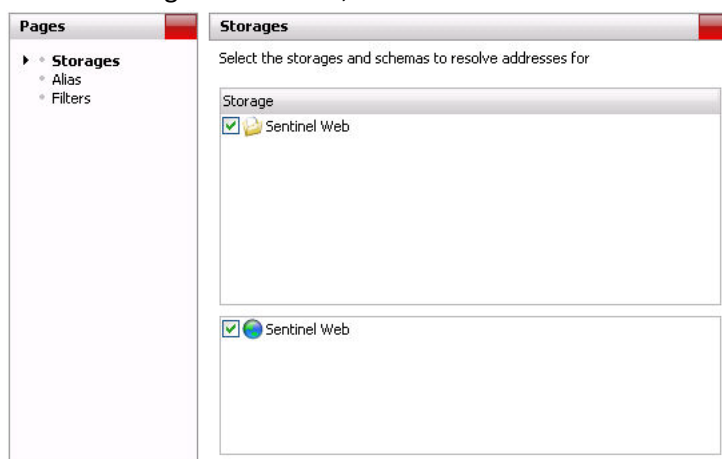
Vantage Giga has the ability to resolve IP addresses to fully qualified domain names. This helps make the information that is presented in Reports more useful.

Instead of changing the IP addresses to domain names in your storages, Vantage Giga uses aliases to display domain names in your Reports. In order to resolve IP addresses to domain names, you need to specify an alias to resolve them into.

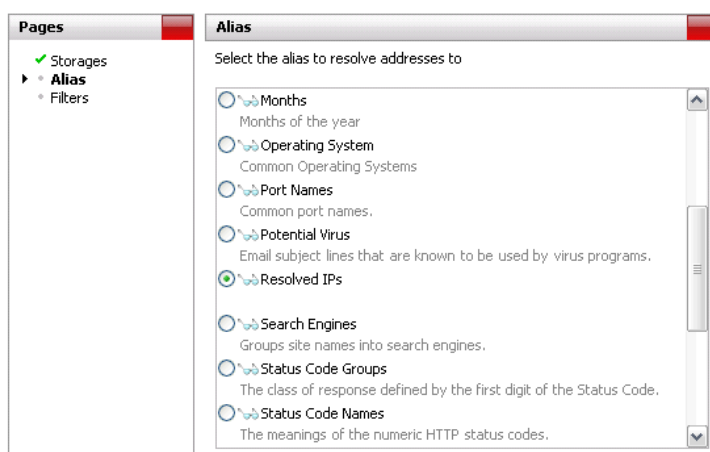
You can resolve all IP addresses at once, or only the IP addresses at a certain summary level. Resolving all IP addresses can take some time, depending on the amount of data in your current analysis. Drilling down into a Summary level such as 'Sites', reduces the number of IP addresses that need to be resolved, and increases the speed of the resolving process.

To resolve all IP addresses:

1. Select the **Aliases** tab from the top of the screen.
2. Click the alias group that you want to resolve IP addresses into, such as 'Usernames' or 'Sitesnames'.
3. Click the **Resolve IPs** link in the Aliases task pad on the left, this will open the Resolve IPs Wizard.
4. Select a Storage and schema, click **Next**.



5. Select the Alias you wish to resolve the IPs into, click **Next**.



- Filters can be added to the Resolve IP function if needed. Click **OK** to complete the wizard.

To resolve IP addresses at a specific summary level:

- Select the **Summaries** tab from the top of the screen.
- Ensure an analysis has been run and you can view summaries
- Select a summary such as site or user addresses that displays IP addresses that you want to resolve
- Click the **Resolve <summary name> IPs** link in the Advanced task pad to open the Resolve IP Addresses dialog
- Select an alias from the drop-down list to resolve the IP addresses into
- Click **OK** to start resolving the IP addresses

Vantage Giga will contact a Domain Name System Server (DNS Server) to attempt to find out the domain name of each IP address.

Vantage Giga will create alias groups using the domain name and add the IP addresses as item to the groups. Your computer must be connected to the Internet for this to work. Any IP addresses that cannot be resolved will remain listed as an IP address, while IP addresses that have been resolved will appear as fully qualified domain names.

*Note: If your network uses DHCP (Dynamic Host Configuration Protocol), resolving IP addresses is not recommended. This is because the computers in your organization may be given a new IP address each time users log on, or when the lease time on the IP address expires. In this situation, your usernames will be invalid if users have logged off and on again since the log file was recorded.*

Resolving IP addresses may take some time. To stop resolving IP addresses at any time, click the Stop button next to the Location bar.

*Note: You can also determine the site name for a site IP address yourself by right-clicking the IP address and selecting Browse from the pop-up menu. This will launch your default web browser and open the site. You can then add the site to your Site name aliases.*




## ***Troubleshooting Aliases***

If you have added new items to your aliases, you may accidentally cause hits to be assigned to the wrong alias. This is due to conflicts in your alias definitions.

To remove conflicts from your aliases:

1. Go to the Aliases dock by clicking the **Aliases** tab at the top of the screen.
2. Click the **Troubleshoot aliases** link to open the Troubleshoot Aliases dialog.

This dialog will scan your aliases for conflicts such as:

-  **Exact duplicates**  
The same item in two different aliases.
-  **Partial duplicates**  
Part of an item in two different aliases.
-  **Superfluous includes**  
Part of an item duplicated in an alias.

Once the scan has finished, a list of conflicts will be displayed. You can choose how to resolve each one.

To do this:

1. Select the conflict
2. Click on the **Resolve** button to launch the Resolve dialog
3. Choose your desired way to resolve the conflict
4. Click **OK**

## Filtering

### Filtering

Filtering options are presented in many areas throughout Vantage Giga. Filters allow you to exclude information you are not interested in importing, analyzing or reporting on.

For Example: If you are analyzing internal network traffic only, you can filter out all IP addresses that do not belong to one of your organization's subnets.

Filters can be defined in two ways:

- ➔ Using the graphical filter editor.
- ➔ Typing a manual filter expression.

To define a filter using the graphical filter editor.

1. Click the 'Graphical filter editor' radio button.
2. Click the **Add** button on the toolbar and select **Field value filter** from the pop-up menu. This launches the Filter Values dialog.
3. Select the Summary you want to filter from the Summary drop down list.
4. Select any Aliases you want to filter by from the Aliases drop down list. This will populate the list at the bottom of the dialog with the selected alias' list of alias groups.
5. Select either the Include or Exclude radio buttons depending on whether you want to include or exclude your selection of summary items.
6. If you do not have an alias selected, click the **Display Known** button on the toolbar to retrieve the list of summary items from your open storages. You can also add unknown values to the list by clicking the **Add** button on the toolbar, typing a value and clicking **OK**. For example, if you are filtering IP addresses to only include your organization's subnets, type your internal subnet range such as 192.168.0.0\24.
7. Check the items in the list that you want to use in the filter and click **OK**.

You can also define date and time filters using the Graphical filter editor. Click the Add button on the toolbar of the Graphical filter editor and select either Date filter, Relative date filter, Day of Week filter or Time filter. Each option will launch it's own easy to use dialog to help you configure these filters.

To define a filter by typing a filter expression:

1. Click the 'Manual filter expression' radio button.
2. Type an expression using the WebSpy filter expression language.

*Tip: Use the graphical filter editor first as this will build a filter expression for you. You can then edit this expression to define more complex filters by clicking the 'Manual filter expression' radio button.*

*Important: If you have defined a filter by typing a filter expression, clicking the 'Graphical filter editor' radio button will reset your typed filter expression.*



When defining reports, you can also filter on top N, bottom N, values greater than or values less than, using Having filters.

## Filter Expression Language

If you need to define a complex filter that cannot be defined using the graphical filter editor, you can define a manual filter using WebSpy's filter expression language.

To access this option, click the 'Manual filter expression' radio button on any filter options dialog.

A filter expression consists of one or more Boolean expressions, connected with either an "and", "or" or an "xor" (exclusive or).

Filter Expression Example: [IPProtocol] == 6 AND [Size] > 100M

A filter expression can include the following types of values:

### Field Names

Field names are enclosed in square brackets, e.g. [Name]. The list of legal field names depends on the schema you are using.

### DateTimes and TimeSpans

DateTimes and TimeSpans are wrapped in braces, e.g. DateTime: {16/05/2005 10:53:12}. A DateTime value may exclude the time eg {16/05/2005}. A TimeSpan adheres to the format d.hh:mm:ss e.g {30.1:30:00}. A TimeSpan may exclude either the day or the time e.g. {1:30:00} or {30}.

### Strings

String literals are wrapped in quotes, and can include a quote mark by prefacing it with a backslash, e.g. "Hello", or "Say \"Hello\"."

### Numbers

Numbers can be followed by K, M or G to represent Kilobytes, Megabytes or Gigabytes. Numbers with one of these size modifiers can include a decimal point, e.g. 1.5K

### IP Addresses and Subnets expressions

IP addresses can be represented by a subnet expression in the format <network address>/<network bits> such as 192.168.0.0/24.

## Operators

Math and Comparison operators are used when defining functions.

The following operators are available:

		Strings	Numbers	DateTimes	IP Addresses
Math Operators					
+	Add	Concatenates two strings: "ab" + "cd" = "abcd"	Sums two numbers: 1 + 2 = 3.	Adds a Timespan to a DateTime: {16/06/2005 10:35:01} + {30}	NA



				Adds a Timespan to a Timespan: {10:35:01} + {01:00:00}	
-	Subtract	NA	Subtracts a number from another number: 3 - 1 = 2	Subtracts a Timespan from a DateTime: {16/06/2005 10:35:01} - {30}	NA
/	Divide	NA	Divides a number by another number: 10 / 5 = 2	NA	NA
*	Multiply	NA	Multiplies two numbers: 2 * 2 = 4	NA	NA
%	Mod	NA	Divides two numbers (floating points rounded to integers) and returns only the remainder: 19 % 6.7 = 5	NA	NA
<b>Comparison Operators</b>					
== or =	Equals	Returns true if two strings are equal: "abcd" == "abcd"	Returns true if two numbers are equal: 4.1K == 4.1K	Returns true if two DateTimes are equal: {16/06/2005 10:35:01} == {16/06/2005 10:35:01}	Returns true if two IP Addresses are equal: 192.168.1.63 == 192.168.1.63
!= or <>	Not Equal	Returns true if two strings are not equal: "abcd" != "bcda"	Returns true if two numbers are not equal: 4.1K != 3.9G	Returns true if two DateTimes are not equal: {16/06/2005 10:35:01} != {16/06/2006 10:35:01}	Returns true if two IP Addresses are not equal: 192.168.1.63 != 192.168.1.30



				10:35:01}	
<	Less Than	NA	Returns true if the first number is less than the second number: 5 < 7	Returns true if the first DateTime is before the second DateTime {16/06/2005 10:35:01} < {16/06/2006 10:35:01}	NA
<=	Less Than or Equal To	NA	Returns true if the first number is less than or equal to the second number: 5 <= 5	Returns true if the first DateTime is before or equal to the second DateTime {16/06/2005 10:35:01} <= {16/06/2005 10:35:01}	NA
>	Greater Than	NA	Returns true if the first number is greater than the second number: 7 > 5	Returns true if the first DateTime is later than the second DateTime {16/06/2005 10:35:01} > {16/06/2003 10:35:01}	NA
>=	Greater Than or Equal To	NA	Returns true if the first number is greater than or equal to the second number: 7 >= 7	Returns true if the first DateTime is later than or equal to the second DateTime {16/06/2005 10:35:01} >= {16/06/2005 10:35:01}	NA
in	In	Returns true if a substring is	Returns true if a number is in a list:	NA	Returns true if an IP address is in a



		present in another string: "bc" in "abcd"  Returns true if a string is in a list: "bc" in ["ab", "bc", "cd"]	6 in [1, 2, 5..9]		range: [Source IP] in [192.168.0.0 .. 192.168.0.255] or [Source IP] in 192.168.0.0/24
like	Like	Returns true if a string is similar to another string: "abcd" like "ab*" or "abcd" like [a-z]	NA	NA	NA

Add brackets and spaces to taste, e.g.  $(1 == 1)$  and  $3 - (2 - 1) == 2$

## Functions

You can also define certain functions using the WebSpy expression language such as extracting only the year from a DateTime field, or aliasing a string.

The following functions are available:

Functions		
Function	Syntax	Example
Alias	Alias(alias, value)	Alias("Computer Names", 192.168.0.4)  Returns the aliased value for 192.168.0.4 as defined in the Computer Names alias
Profile	Profile(url)	Profile("http://www.webspy.com")  Returns the profile for the url http://www.webspy.com.
Length	Length(string value)	Length("abcd")  Returns 4
Date	Date(DateTime value)	Date(16/06/2005 10:55:36)  Returns 16/06/2005

Year	Year(DateTime value)	Year(16/06/2005 10:55:36) Returns 2005
Month	Month(DateTime value)	Month(16/06/2005 10:55:36) Returns 6
Day Of Month	DayOfMonth(DateTime value)	DayOfMonth(16/06/2005 10:55:36) Returns 16
Day Of Week	DayOfWeek(DateTime value)	Returns a number ranging from 0 to 6 representing Sunday to Saturday. DayOfWeek(16/06/2005 10:55:36) Returns 4.
Day Of Year	DayOfYear(DateTime value)	DayOfYear(16/06/2005 10:55:36) Returns 167
Week Of Year	WeekOfYear(DateTime value)	WeekOfYear(16/06/2005 10:55:36) Returns 24
Time	Time(DateTime value)	Time(16/06/2005 10:55:36) Returns 10:55:36
Hour	Hour(TimeSpan value) or Hour(DateTime value)	Hour(16/06/2005 10:55:36) or Hour(10:55:36) Returns 10
Md5	Md5([Fieldname])	md5([Username])  Returns an md5 string in place of the Username. This is useful for anonymising data in reports such as usernames or IP addresses.
Minute Of Day	MinuteOfDay(TimeSpan value) or MinuteOfDay(DateTime value)	MinuteOfDay(16/06/2005 10:55:36) or MinuteOfDay(10:55:36) Returns 655



Minute Of Hour	MinuteOfHour(TimeSpan value) or MinuteOfHour(DateTime value)	MinuteOfHour(16/06/2005 10:55:36) or MinuteOfHour(10:55:36)  Returns 55
Now	Now()	Now()  Returns the current DateTime.

Filter Expression Examples	
Description	Syntax
All values in the year 2005	Year([DateTime]) == 2005
All values between the first of May and the First of June 2005.	[DateTime] >= {01/05/2005} and [DateTime] <= {01/06/2005}
All values from 1st May 2005 until today.	[DateTime] >= {01/05/2005} and [DateTime] <= Now()
All values in the past 30 days	[DateTime] > (Date(NOW()) - {30}) and [DateTime] <= Date(NOW())
All values in the subnet alias group "California".	Alias("Subnets", [SourceIP]) == "California"
All values in the Subnet alias groups California and Washington.	(Alias("Subnets", [Source IP]) in ['California', 'Washington'])
All values in the Subnet 192.168.0.0/24	[SourceIP] in 192.168.0.0/24

## Having Filters

When defining Reports, you have the ability to apply filters. There are two types of Filters: Hit Filters (explained in 'Filtering') and Having Filters.

With Having filters, you can filter a report to show only the top or bottom items or items with values greater or less than a certain amount.

Having Filter Example: You can create a having filter to show only the 10 users that have downloaded the most data, or the IP addresses that have transmitted over 1GB of data.



You can specify Having filters wherever the 'Having' tab appears on a dialog.

To specify a Having filter:

1. Select the column you want to base the having filter on.  
For example if you want to see the 10 users that have transmitted the most number of packets, select 'Packets' in the column drop down list (the list of available columns differ depending on the schema you are reporting on).
2. Select your criteria by selecting the 'Top N', 'Bottom N' or 'Value' radio buttons, and enter or select the values to filter on.

## Profiles

### *Profiles*

Any log format that contains a URL will produce a range of Summaries including the 'Profile' Summary (see 'Summaries created from URLs'). Vantage Giga creates the Profile summary by 'Profiling' the URL. Profiling is the process of categorizing the URL based on keywords it contains.

*Note: The Name of the Profile summary is preceded by the name of the URL field, such as 'Site Profile' or 'Referrer Profile'.*

A profile is a collection of keywords that are matched against the names of the sites and downloaded resources. There are two lists of keywords defined on the **Profiles** dock; 'includes' and 'excludes'.

Vantage Giga searches through each URL for 'includes' keywords. As soon as it finds a keyword, it will check for any 'excludes' keywords for that profile. If there are no 'excludes' keywords, then the URL is assigned to that profile. If there is an 'excludes' keyword, the hit is checked for 'includes' keywords in the next profile.

Profile matching example: If a site name contains 'computershop', it will be assigned to the computer profile not the shop profile, since the keyword 'computer' comes before the keyword 'shop', assuming that the URL has no excluded words from the computer profile.

Vantage Giga comes with its own list of default profiles, and you can add, edit or delete profiles and keywords to suit your organization's Internet usage patterns. For example, you may want hits to your organization's intranet to be profiled under the 'My Organization' profile.

A URL that does not contain any keywords will be assigned to the Miscellaneous profile. Approximately 20-35% of URLs will be assigned to this profile when using the default profiles that come with Vantage Giga. The percentage of URLs assigned to the Miscellaneous profile declines as you develop and refine your own profiles.

To add a profile:

1. Click the **Profiles** tab at the top of the screen. This takes you to the Profiles dock.
2. Click the **New Profiles** link in the Profiles task pad to launch the New Profile dialog.
3. Enter a name and description for the Profile and click **OK**.



4. The profile you created appears in Profiles list. The Includes and Excludes keyword list appear next to it. Ensure the profile you created is selected and use the buttons on the toolbars on the Includes and Excludes lists to add, edit and delete keywords.

Run an analysis to re-categorize your URLs with the changes you made. The results of the profile matching can be seen in Summaries or Reports by looking at the appropriate 'Profiles' Summary.

*Tip: Profiling URLs can slow down an analysis. If you do not want to analyze profiles, turn off all the Profile Summaries by un-checking the Summaries on the Create Analysis dialog (see Summary Selection).*

## **Troubleshooting Profiles**

If you have added lots of new keywords to your profiles, you may accidentally cause hits to be assigned to the wrong profile. This is because of conflicts in your keywords lists.

To remove conflicts from your profiles:

1. Go to the Profiles dock by clicking the **Profiles** tab at the top of the screen.
2. Click the **Troubleshoot profiles** link to open the Troubleshoot Profiles dialog

This dialog will scan your profiles for conflicts such as:

- ➔ **Exact duplicates**  
Same includes keyword in two different profiles.
- ➔ **Partial duplicates**  
Part of an includes keyword is in two different profiles.
- ➔ **Overriding excludes**  
An excludes keyword that will mean any hits matched by an includes keyword will be excluded from the profile.
- ➔ **Superfluous include/excludes**  
Part of a keyword is duplicated in a profile's includes or excludes keywords.

Once it has finished scanning, it will display a list of conflicts. You can choose how to resolve each one.

To do this:

1. Select the conflict
2. Click on the **Resolve** button to launch the Resolve dialog for that conflict
3. Choose the appropriate way to resolve the conflict
4. Click **OK**

## Tasks

### Creating Tasks

Most actions you perform in Vantage Giga can be set to run automatically as part of a task. Importing data and running reports can therefore be done overnight, ready for you in the morning.

To create a task:

1. Click the **Tasks** tab at the top of the screen. This takes you to the tasks dock.
2. Click the **New Task** link in the Tasks task pad. This launches the Task Options dialog.
3. On the **General** page, enter a name for your task such as 'Weekly network usage report task'. Click **Next**.
4. On the **Schedule** page, check the 'Run task using Windows Task Scheduler' check box. The 'Key' that is displayed can be used to identify the Windows Job that gets created.
5. Select when you would like the task to run. For example, Start: 01/05/2005 at 06:00:00, Recurrence: Weekly - every 1 week on Fridays. Click **Next**.
6. On the **Authentication** page, enter the Windows user name and password that you want the task to run as, for example 'mydomain\john.citizen'.
7. Click **OK**.

*Tip:* You can receive notification each time your task runs, by configuring the task to send results to an email address using the 'Send task results by email' option on the General page.

Now that you have created a task, you can add actions to the task.

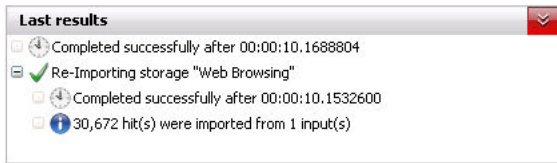
To add actions to a task:

1. Select the task you created in the Tasks list.
2. Click the **Add Action** button in the right-hand pane and select the action you want to run.
3. The action will be added to the Actions list and will include a number of sub-actions. For example, the 'Run a comparison or analysis report' task action has two sub-actions: 'Select template' and 'Configure report'.
4. Double-click each sub-action to configure them.
5. Once you have added all the actions you want the task to run, and configured all the sub-actions, you can run the task by clicking the **Run Task** link in the Tasks task pad. This is a good way to test that the task is working as you expect.
6. Once you are happy with your task, you can leave it to run as scheduled.

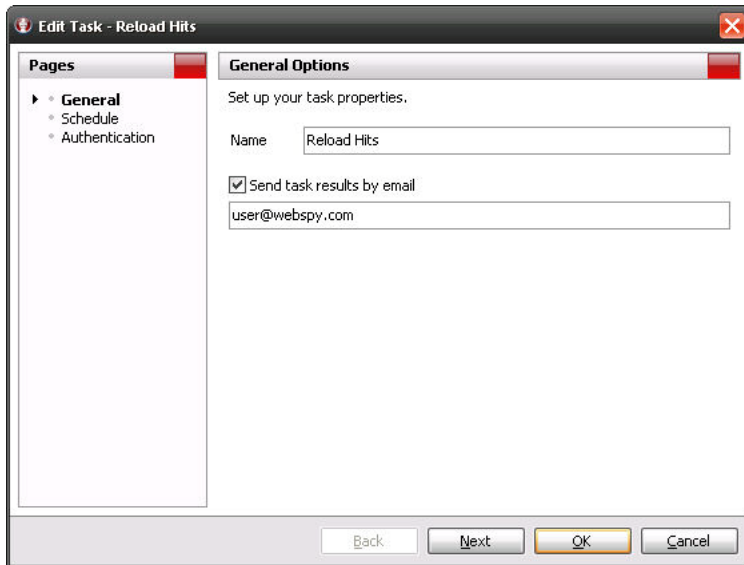
*Tip:* Tasks are not only useful for running actions at convenient times, but also for setting up batch jobs. For example, if you always want to run a set of 10 reports, you can configure a task that runs these reports, and simply click the 'Run Task' button when you want to generate those reports. This is much more convenient than generating each report one by one. On the Task Options dialog, uncheck the 'Run task using Windows Task Scheduler' check box' so that the task doesn't try to run at a scheduled time.

Once completed, task results are displayed in the Last Results section of the selected task.





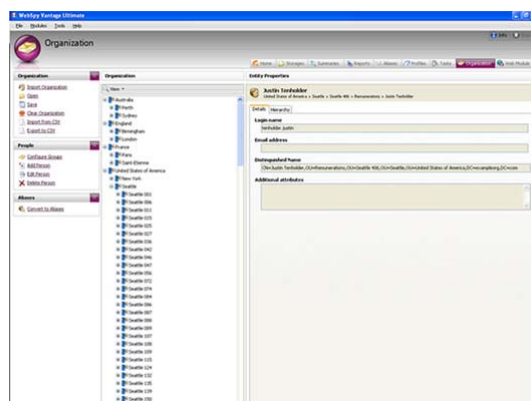
These results can also be sent by email. This option can be found on the General page of the task options, accessed via Edit Task.



## Organization

### *Organization*

The Organization dock enables you to create users and organize them into multi-level groups representing your organizational structure. Users are mapped to information in your log files, enabling effective reporting on any organizational unit. To access the Organization dock, click the Organization tab at the top of the screen.



You can add the users and groups that represent your organizational structure in a number of ways:

- ➔ **Import Organization**  
Imports your organizational structure from an LDAP or LDIF directory server
- ➔ **Import from CSV**  
Imports your organizational structure from a CSV file
- ➔ **Add Person**  
Manually adds a user
- ➔ **Configure Group**  
Manually adds a group

You can manage your organizational structure via a range of options:

- ➔ Export to CSV
- ➔ Clear Organization

You can also use your organizational structure to create aliases.

### *Importing your Organization*

Using the Import Organization option you can add users within your organization and sort them into the desired groups in the same process.

WebSpy recommends that you use an LDAP Browser (such as Softerra's free LDAP Browser) to verify which attributes to use to import user's login details, email addresses and so on.

To do this:

1. Click **Import Organization**

2. On the **Directory server** page, select your directory type and server and enter your username and password to authenticate with your domain controller then click **Test**. Click **Next** after you have successfully connected to your directory server.
3. On the **Source** page, enter a Root Distinguished Name to search for users within (for example, 'dc=mydomain, dc=com'). The LDAP search query is defaulted to a query that returns 'users', however you can change this if necessary. Click **Next**.
4. On the **User details** page fill out the form with the attributes you intend to use for Display name, Email address, Login name and Manager. You can also enter a prefix or suffix for the login names.

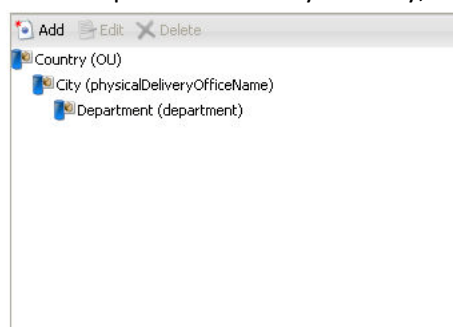
*Note:*

*Additional Attributes:*

*Use the 'Additional Attributes' section to specify any extra information you need to import into the user to map them to the various ways they are identified in your log files. For example, if users are identified by a UserID in your log files, import the UserID attribute from your directory server into the Additional Attributes section.*

*You can use a large range of information as attributes, including IP addresses and subnet masks.*

5. On the **Grouping** page you can setup how your member groups are structured. For example it could be by Country, City, and Department.



To add a group:

1. Click the **Add** button
2. Enter the name of the new group
3. Enter the name of the attribute in your directory server which best contains the groups information
4. Select the source node at which the desired attribute is located in relation to the user node
5. Click **OK**
6. The option **Convert Organization to Aliases after import**, located at the bottom of the grouping page, will automatically create new aliases for each grouping level. You can then apply these aliases in your reports and filters.
7. On the **Merging** page, select how your directory server information should be merged with your existing organizational structure.
 

*Note: When merging, only users that have previously been added from your LDAP/LDIF directory will be affected. Users that have been manually added will not be affected.*
8. Click **OK** to complete the wizard and begin the import

Once the import is complete you will see your Organization tree displayed. You can use the 'View' drop-down list at the top of the Organization tree to display your groups, or your manager/subordinate hierarchy.

## Importing and Exporting CSV Files

Using the Import from CSV option you can add users within your organization and sort them into the desired groups in the same process.

To do this:

1. Click **Import from CSV**.
2. Navigate to the csv file that contains your organizational structure.
3. Select how the information from your csv file should be merged with your existing organizational structure.

*Note: When merging, only users that have previously been added from your CSV file will be affected. Users that have been manually added will not be affected.*

4. Click **OK** to complete the wizard and begin the import.

Once the import is complete you will see your Organization tree displayed. You can use the 'View' drop-down list at the top of the Organization tree to display your groups, or your manager/subordinate hierarchy.

You can also save your organizational structure to a CSV file.

To do this:

1. Click **Export to CSV**.
2. Enter a name for your file.
3. Click **OK** to finish.

## CSV File Format

WebSpy supports CSV file formats that:

- ➔ List your grouping structure  
i.e. Country/City/Branch/Department
- ➔ Contain a unique identification for each individual  
i.e. CN=Cyril Margheim, OU=Acquisition, OU=Perth 950, OU= Perth, OU=Australia, DC=exampleorg, DC=com
- ➔ Link a unique manager identification to each individual  
i.e. CN=Glendora Martensen, OU=Acquisition, OU=Perth 950, OU=Perth, OU=Australia, DC=exampleorg, DC=com

Grouping	Country/City/Branch/Department					
Name	Unique	ManagerUnique	Group	Login	Email	Additional
Cyril Margheim	CN=Cyril Margheim,OU=Acquisitio	CN=Glendora Mart	Australia/Perth/Perth 950/Acquisition	margheim.cyril		
Gabriel Kuennen	CN=Gabriel Kuennen,OU=Acquisiti	CN=Glendora Mart	Australia/Perth/Perth 950/Acquisition	kuennen.gabriel		
Doyle Barer	CN=Doyle Barer,OU=Acquisition,O	CN=Glendora Mart	Australia/Perth/Perth 950/Acquisition	barer.doyle		
Latia Nipp	CN=Latia Nipp,OU=Acquisition,OU:	CN=Glendora Mart	Australia/Perth/Perth 950/Acquisition	nipp.latia		
Laure Rindels	CN=Laure Rindels,OU=Acquisition,	CN=Glendora Mart	Australia/Perth/Perth 950/Acquisition	rindels.laure		

## ***Manually Creating your Organization***

If you do not have access to a directory server or CSV file to automatically import your organizational structure, you can manually create your groups and users.

### **Adding Groups**

The 'Configure Groups' option allows you to manually create user groups. These groups should reflect your organizations structure, for example Country, City, and Department.

To do this:

1. Click **Configure Groups**
2. To add a new organization group click **Add**
3. Enter the name of the new group and click **OK**
4. Use the Up and Down Arrows to rearrange your groups as required

Add any additional ways a group can be identified in the Attributes section. For example if you have a range of IP addresses (subnet) for each branch location of your organization, you can add this information in the Attributes section and then use a custom expression when generating reports.

### **Adding People (Users)**

The 'Add Person' option allows you to add individual users to your organization tree.

To do this:

1. Click **Add Person**
2. Enter the display name for the user in the first entry box
3. Enter their Login name and email address
4. Add any additional ways the user can be identified through log files in the **Additional attributes** section such as IP addresses, computer names, and authenticated usernames
5. The **Hierarchy** tab allows you to specify whether the user has either a manager or subordinates or both

Once you have added a user you can edit that person's details or delete them from the organizational structure by using Edit Person and Delete Person respectively.

## ***Deleting your Organization***

To remove your organizational structure, including all users and groups:

1. Click **Clear Organization**.  
A popup box will appear asking you to confirm the deletion.
2. Click **Yes** to delete your organizational structure

## ***Converting to Aliases***

Once you have created your organizational structure you can choose to automatically create aliases based on hierarchical grouping that you have constructed in your organization tree.

Aliases are used to translate information associated with specific users and groups into a more useful form. This means that a user's or web site's name can be viewed instead of its IP address, or a type of file rather than the file extension.

Clicking on Convert to Aliases will add each organizational group as an alias on the Aliases dock.

*Note: If you do not have any groups in your organizational structure then clicking the button will have no effect.*

## Options

### *General Options*

The General tab of the Options dialog enables you to configure settings that are general to the application.

To access General options:

1. Select **Tools | Options** from the main menu to launch the Options & Settings dialog
2. Click the **General** tab

This tab enables you to configure the following options:

 **Units of size**

Size fields throughout the application can be displayed in Bytes (B), Kilobytes (KB), Megabytes (MB), or Gigabytes (GB). Select the unit of size you would like to use from the 'Units used to display size of data' drop down list. You can also select 'Auto' which appends KB, MB, or GB after each size field.\

 **Time format**

Time fields in the application can be displayed in Milliseconds, Seconds, Hours, h:m:s or h:m:s.ms.. Select the format you would like to use from the 'Units used to display time drop down list.

 **Default application priority**

You can set a change the application priority for Vantage Giga so Windows will devote more or less time to running it. Note: Setting a higher priority to Vantage Giga will slow down other processes running on your computer.

 **Toolbar text options**

This option changes whether text is displayed in addition to icons on the toolbars throughout the Vantage Giga

 **Session Threshold**

This option controls how long a user needs to stop browsing for before their session is considered 'finished' (see 'Sessions and Browsing Time')

 **Check for updates on start**

This option controls whether Vantage Giga should check the web for updates each time it starts.

 **Show latest news**

This option controls whether the latest news section is displayed on the home screen.

### *Import Options*

The Import tab of the Options dialog enables you to configure settings related to importing log files.

To access Import options:

1. Select **Tools | Options** from the main menu to launch the Options & Settings dialog
2. Click the **Import** tab

This tab enables you to configure the following options:



#### **Ignore importing issues**

When importing data into a storage, issues may be encountered. If this option is checked, Vantage Giga will continue importing log files regardless of how many issues are encountered.

#### **Stop importing once this many consecutive issues are raised**

You can configure the number of consecutive issues that can be encountered before the import is terminated. The default number of issues is 15. This can be changed by entering a new number in the 'Stop importing once this many consecutive Issues are raised' edit box.

#### **Stop importing once this many issues are raised**

In addition to the number of consecutive issues, you can also configure the total number of import issues that can be encountered before terminating an import. The default is set to 1000. This can be changed by entering a new number in the 'Stop importing once this many Issues are raised' edit box.

#### **Analyze data during import**

When Vantage Giga imports data, it also runs an analysis on your data at the same time. This analysis is then saved back into the storage. This allows ad-hoc analyses to be instantly available when using the 'use precalculated analysis' feature, but slows import speed. You can therefore turn this feature on or off depending on the way you use Vantage Giga (see 'Precalculated Analysis').

## **Summaries Options**

The Summaries tab of the Options dialog enables you to configure settings related to the Summaries dock.

To access Summaries options:

1. Select **Tools | Options** from the main menu to launch the Options & Settings dialog
2. Click the **Summaries** tab

This tab enables you to configure the following options:

#### **Include advanced summaries in analyses**

All schemas have certain Summaries that are considered 'basic'. That is, they are considered more useful for meaningful analyses than other more 'advanced' Summaries. You can select whether to generate all the Summaries, or only the basic Summaries by default when running an analysis. To generate all Summaries, check the 'Include advanced summaries in analyses' checkbox.

#### **Hide Summaries with only one item**

You can automatically remove Summaries that contain only one item from the list of Summaries created when you run an analysis. To do this, check the 'Hide Summaries with only one item' checkbox. Summaries containing only one item will be removed from the Summaries Tree, however you can still view their information in the overview information that is displayed when you select a folder node in the tree.

#### **Show Descriptions under summaries instead of beside them**

This option changes the position of each Summary's description when you select a folder node in the Summaries Tree.

This tab also allows you to manage your extensions.



## Report Options

The Reports tab of the Options dialog enables you to configure settings related to the look and feel of your generated reports.

To access Reports options:

1. Select **Tools | Options** from the main menu to launch the Options & Settings dialog
2. Click the **Reports** tab

This tab enables you to configure the following options:

### **Web (HTML)**

This option enables you to set a style sheet (CSS) for your web reports. Vantage Giga comes with a list of different stylesheets you can use, and if you're familiar with CSS, you can edit the existing files or create your own to suit your purposes. Simply save the style sheet in the Styles sub-folder in Vantage Giga's installation folder and select it here. All future report that you generate will use your new style sheet.

### **Word**

This option enables you to set a WordML style sheet to be used with Word Reports. If you're familiar with WordML style sheets you can edit the existing file or create your own to suit your purposes. Simply save the style sheet in the Styles sub-folder in Vantage Giga 's installation folder and select it here. All future report that you generate will use your new style sheet.

### **Report Cover Image**

This option enables you to customize the image displayed on the cover page of all your Web and Word reports. This is useful for inserting your company's logo into your reports.

### **Company Name**

The company name is displayed on the cover page of all your reports. Change this to your organization's name.

### **Cover page text**

This option enables you to insert your own text into the cover page of your reports. You can use variables such as %company% to insert the company name (defined above) into the text.

### **Chart Colors**

Choose from a list of preset color options to change the coloring of charts.

## Color Options

You can customize the colors Vantage Giga uses.

To access Color Options:

1. Select **Tools | Options** from the main menu to launch the Options & Settings dialog
2. Click the **Colors** tab

To adjust the colours Vantage Giga uses, simply drag the Hue, Saturation, Luminance, Contrast and Highlight intensity sliders to suit. You can also have the application randomly select a different colour each time it starts by checking the 'Random on start' checkbox. To reset to the default colours, click the Defaults button.



## ***Path Options***

Vantage Giga uses a number of folders to store information. These folders are created automatically when the program is installed.

Folder locations are displayed on Paths tab of the Options dialog.

By default Vantage Giga creates a folder in 'My Documents\WebSpy\Vantage Giga 2.1' where all user files, such as storages and reports, are stored. You may like to change some of these locations, such as the storages location, to somewhere more appropriate.

To access Location Options:

1. Select **Tools | Options** from the main menu to launch the Options & Settings dialog
2. Click the **Locations** tab

To modify a folder path:

1. Click the hyperlink on the name of the path you want to modify. This launches a Browse dialog.
2. Navigate to the location of the desired folder.
3. Click **OK**.

The new path to the folder will be displayed in the Paths tab.

## ***Email Options***

Vantage Giga can email reports to specified recipients each time a report is generated. Emails are sent using SMTP and requires some configuration for it to work. These options are set on the Email tab of the Options dialog.

To access Email Options:

1. Select **Tools | Options** from the main menu to launch the Options & Settings dialog
2. Click the **Email** tab

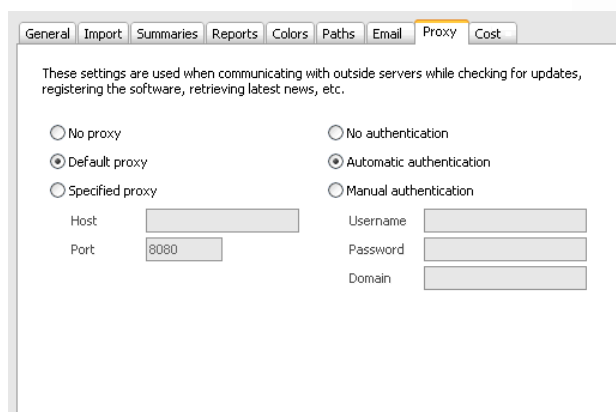
To configure your SMTP options:

1. Enter your SMTP server name into the 'SMTP Server' edit box. You may need to obtain this information from your system administrator or Internet Service Provider.
2. Enter the port number into the 'SMTP server port' edit box (This is usually 25 for SMTP).
3. Enter your email address into the 'Your email address' edit box. This is the email address that will appear in the 'From' field for each report sent by email.
4. If your SMTP server does not accept unauthenticated requests, you can specify your authentication details by checking the 'Login to my SMTP server' checkbox and entering your details.

## ***Proxy Options***

Proxy settings and authentication information, used by Vantage Giga to connect to outside servers, can be set in the Proxy tab.





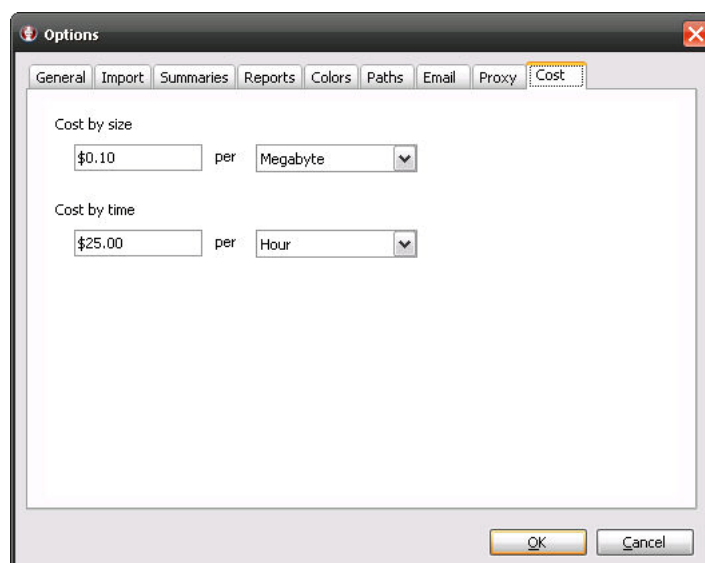
**Default proxy:** Uses current connection settings found within Internet options.

**Automatic authentication:** Uses your Windows log on credentials from the current session.

*Note: Default proxy and Automatic configuration is recommended.*

## Cost Options

The Cost options dialog allows you to associate a monetary value to file size or session time.



Cost by size and Cost by time values are used for calculating the aggregates, Cost by Size and Cost by Browsing Time.

See the Custom Aggregates Column section in 'Advanced Analysis Templates' for information on adding aggregates.

## Module Options

The Modules tab enables you to show or hide the main application tabs in WebSpy Vantage Giga. You can use this tab to simplify the user interface if you never use certain areas of the application.

## ***Performance Options***

If you are running Vantage on a multi-core machine or a machine with multiple CPUs, Vantage can take advantage of the extra CPUs resources to improve the speed of importing and reporting. The Performance tab enables you to configure the multi-processing options.

 **Use multi-processing**

This checkbox turns on multi-processing support.

 **Maximum concurrent threads**

This setting indicates how many threads Vantage should use when processing records.

WebSpy recommends setting this to twice the number of CPUs or logical cores in your machine. For example, if you're running on quad core machine, set this value to 8. If you're running a machine with two quad core CPUs set this value to 16.

 **Show performance statistics on the status bar**

These options display the appropriate performance indicator in Vantage's status bar. Storage throughput displays the number of records written to or read from the Storage per second.

Using multi-processing only increases the speed of certain tasks, such as importing multiple log files or generating side-by-side summaries in reports. Other tasks such as importing a single log or generating drilldown summaries will not benefit from multi-processing.

## Contact WebSpy

### WebSpy North America

*(Servicing North and South America)*

Columbia Center  
701 5<sup>th</sup> Ave, Suite 4200  
Seattle, Washington 98104

Toll free: 888-862-4403  
Phone: +1 206-262-7763  
Fax: +1 206-708-6113  
Email: [sales@webspy.com](mailto:sales@webspy.com)

### WebSpy Europe

*(Servicing Europe, Middle East and Africa)*

Westbourne House  
14-16 Westbourne Grove  
London, W2 5RH

Phone: +44 (0) 207 313 5730  
Fax: +44 (0) 207 313 5731  
Email: [europesales@webspy.com](mailto:europesales@webspy.com)

### WebSpy Australia

*(Servicing Australia, Asia and the Pacific)*

Level 3  
9 Colin Street  
West Perth, Western Australia 6005

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

### WebSpy Support

To contact WebSpy Support, please email [support@webspy.com](mailto:support@webspy.com) or visit our support page at [www.webspy.com/contact/support.aspx](http://www.webspy.com/contact/support.aspx)

