



WebSpy Vantage 1.0

Getting Started Guide

This document is intended to help you get started using *WebSpy Vantage 1.0*. For more detailed information, please see the *Vantage 1.0* online help. This can be accessed via **Help** | **Contents** on the main menu.

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

Table Of Contents

Overview	3
Importing log files.....	4
Running an Analysis	5
Browsing Summaries.....	6
Applying Aliases	8
Creating Reports.....	9
Generating Reports	10
Creating Tasks	11
End of Tutorial.....	12
Supported Log Files.....	13
Contact WebSpy	14
WebSpy North America	14
WebSpy Europe	14
WebSpy Australia	14
WebSpy Support	14

Overview

Thank you for downloading or purchasing WebSpy **Vantage**

This tutorial will guide you through Vantage'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 Ad hoc Analysis on your storage.
- ➔ Browsing your Summaries
- ➔ Applying Aliases to your Summaries.
- ➔ Creating and Generating reports.
- ➔ Creating and running tasks.

Importing log files

Vantage 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 the list of supported formats, please see the Supported log files topic at the end of this tutorial.

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 FlowMonitor.log included with the application you downloaded. This log file is a WebSpy FlowMonitor Log file and contains information about traffic flowing through Cisco® routers.


Try this: Create a storage:

1. Open Vantage and click **Storages** on the left Navigation bar. This takes you to the Storages dock.
2. Click the **New** button on the toolbar in the left Navigation bar.
3. Enter the name 'My Storage' into the 'Name' edit box. Ensure the 'Import Data into this storage now' checkbox is checked and click **OK**.

The new storage appears in the list on the left hand Navigation bar, and the Input Dialog is launched. The Input Dialog guides you through the process of importing data into your storage.

Try this: Import some log files:


1. On the Input Type page of the Input Dialog, select 'Local or networked files and folders'. Click **Next**.
2. On the Input Specifications page, select the Loader Group 'WebSpy' and the Loader Format 'FlowMonitor'.
3. Set the File Mask to *. Click the browse button next to the 'Path' edit box, navigate to **My Documents\WebSpy\Vantage 1.0\Logs** and click **OK**. This default log file location can be changed in Path Options. Click **Next**.
4. The files contained in the folder you selected appear on the Input Selection page. Check only the FlowMonitor.log file and click **OK** on the Input Dialog.

 **Optimization Tip:** You can get better performance out of Vantage by configuring some of the settings on the Advanced pages of the Inputs dialog. For more information see the Advanced Importing Features topic in the help file.

While Vantage 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 the Precalculated Analysis topic in the help file).

As Vantage imports FlowMonitor.log, you can watch 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 the Import Issues topic in the help file.

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

If any of the log files you have imported are still being written to by your logging device, you can easily import the new hits by clicking the **Import All** button on the toolbar. You can also clear all the imported hits and reload the information from your log files by clicking the **Re-Import All** button on the toolbar.

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 creates 'top-level' or 'overview' Summaries that you can drilldown into. When you drilldown, Vantage runs another analysis to retrieve the next group of Summaries from your storage. This type of analysis takes time to perform each drilldown, but allows you to drilldown into any area of your data. This type of analysis is great for interrogating your data on demand.

➔ **Template Analysis:**

The problem with Ad hoc analyses is that every time you drilldown, you get the full list of summaries and some of those summaries are slow to produce. If you only want to see a specific set of summaries, you can produce an Analysis Template that defines those summaries and drilldowns. When you generate the Analysis Template, all the Summaries and drilldown paths are pre-calculated during the analysis, where as an Ad-hoc analysis only returns the 'top-level' or 'overview' summaries. Once the Analysis has finished and the drilldowns and summaries are displayed, you can drilldown further into summaries that have not been pre-calculated as you can in an Ad-hoc Analysis.

Try this: Run an Ad-hoc Analysis:

1. Click Summaries on the left Navigation bar. This takes you to the Summaries dock.
2. Click the **New Analysis** button on the toolbar in the left Navigation bar. This launches the Create Analysis dialog.
3. In the 'Name' edit box, enter 'My Analysis'.
4. Select 'My Storage' from the 'Storage' list.
5. Select 'FlowMonitor' from the 'Schema' list.
6. Click **Next**.
7. On the Analysis Type page, select the 'Ad-hoc Analysis' radio button and ensure 'Use precalculated analysis if available' checkbox is checked.
8. Click **OK**.

 **Note:** You can filter the analysis using the Filter page. For more information see the [Filtering](#) topic in the help file. You can also select the summaries that you want created using the [summaries](#) page. For more information see the [Summary Selection](#) topic in the help file.

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 the [Running a Template Analysis](#) topic in the help file.

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

Browsing Summaries

Once an Analysis has been run, Vantage 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.

The right-hand pane displays the list of summaries for the schema you analyzed. Each summary is hyperlinked. Notice that the same list of summaries appears in the left Navigation bar. Clicking a hyperlinked summary takes you to the corresponding summary in the tree on the left. So you can simply use the tree on the left to navigate between summaries as desired.


ⓘ 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. This is because it does not make sense to drilldown into these items as the drilldown will take time, 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. Click the Source Address Summary by clicking the Summary in the left Navigation bar. All the source IP addresses in your storage are displayed in the right hand pane. The number of Hits, Packets transmitted and Size of data transmitted are also displayed. The bottom right hand pane charts the top 25 items in the Summary.
2. Click the 'Packets transmitted' 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 source IP address with the most number of packets transmitted:

1. Click the source IP address at the top of the list. Vantage performs a drilldown and retrieves all the Summaries that pertain to that IP address.
2. Once the drilldown is complete, all the generated Summaries are listed underneath the IP address in the left Navigation bar. Click the  next to the IP address 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 left Navigation bar. 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 Output Interface for a specific Next Hop IP address using the right-click Drilldown function:

1. Go to the Next Hop IP Summary by clicking this Summary in the left Navigation bar.
2. Right-click on the first IP address in the list and select **Drilldown** from the pop-up menu.
3. Select the Output Interface Summary from the sub-menu.

Vantage then performs a drilldown into the first Next Hop IP in the list and displays the Output Interface 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 in the left Navigation bar 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 a Source IP Address:

1. Click the Source Address summary in the left Navigation bar.
2. Enter '192.168' into the Find edit box at the top of the list and click the **Find** button. All the IP addresses that include the values 192.168 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.

 **Tip:** *As more drilldowns are performed, Vantage uses more RAM. You can monitor the CPU and RAM usage in the Status bar at the bottom of the screen. If Vantage is using too much RAM, you can right-click any drilldown in the left Navigation bar and select Remove from the pop-up menu. This frees some memory for use by other applications. You can display these Summaries again by right-clicking in the left Navigation bar and selecting 'Show cached summaries'.*

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 IP addresses contained within your Source IP Address Summary, you may want to group them into your organization's subnets, or show hostnames instead.

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

Try this: View the list of sample aliases:

1. Go to the Aliases dock by clicking Aliases in the left Navigation bar.
2. Select an alias in left Navigation bar 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 Summaries in the left Navigation bar.
2. Ensuring you have the 'My Analysis' Analysis open, select the Destination Port Summary in the left Navigation bar.
3. Click the **Aliases** drop down list in the toolbar and select 'Port Names'. All the Destination Ports are now represented by Port Names. Any Destination Ports that do not match a Port 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 from the **Aliases** button on the toolbar. If no Aliases can be applied to a particular Summary, the **Aliases** button is disabled.

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

Creating Reports

Vantage 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 and generate reports as well as manage any existing reports. To access the Reports dock, click **Reports** in the left Navigation bar.

Report templates are listed in the left Navigation bar and templates are configured in the right hand pane. At bottom of the screen is the Reports Manager pane that lists all the generated reports.

You can create three types of 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.

➤ **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 an Template Analysis (see the Running a Template Analysis topic in the help file).

➤ **Trend Reports**

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

Try this: Create a quick Comparison report:

1. Click **Reports** in 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. Type 'My Comparison Report' in the Name edit box.
4. Select 'FlowMonitor' from the Schema drop down list.
5. Select the 'Comparison' radio button and click **OK**. A new Comparison Report Template is added under the Comparison Reports folder in the left Navigation bar. Ensure this Template is selected.
6. Check the '1' check box in the right hand pane to enable the options for the first drilldown.
7. Select TCP Protocols from the Summary drop down list and select TCPIP Protocols from the Alias drop down list. Leave the Filter edit box empty and Select Packets Transmitted from the Order By drop down list.
8. Check the '2' check box to enable the options for the second drilldown.
9. Select 'Destination AS' from the Summary drop down list and select Packets Transmitted from the Order By drop down list. Leave the Alias drop down list set to none and the Filter edit box empty.

You have now configured a Comparison Report to drilldown into TCP Protocols and display all the Destination AS' (Autonomous Systems) 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 the Running a Template Analysis topic in the help file) you can use it to generate a printable or online document (see Generating Reports).

Generating Reports

Vantage 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:


- ➔ HyperText Markup Language (HTML)
- ➔ Microsoft® Word Document (DOC)
- ➔ Text Document (TXT)

Try This: Generate a report:

1. Click **Reports** on the left Navigation bar. This takes you to the Reports dock.
2. Select the Report Template you want to generate in the left Navigation bar. In this case, select the 'My Comparison Report' you created in the previous topic.
3. Click the **Generate Report** button in the right hand pane. 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 HyperText Markup Language radio button. Leave the 'Generate as loose HTML files' unchecked. 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 then generates the report and opens it using the default viewer for the format you selected in step 5.

Hypertext markup language (HTML) 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 the Filtering topic in the help file. There are also other publishing options for reports such as emailing the report and copying it to a location. For more information, see the Report Publishing topic in the help file.*


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. For more information see the Report Documents topic in the help file.

Creating Tasks

Most actions you can perform in Vantage 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 **Tasks** in the left Navigation bar. This takes you to the tasks dock.
2. Click the **New** button on the toolbar in the left Navigation bar. This launches the Task Options dialog.
3. On the General page, enter a name for your task such as 'Weekly network usage report task'.
4. Check the 'Run task using Windows Task Scheduler' check box and enter the Windows user name that you want the task to run as, for example 'mydomain\john.citizen'. Click the **Set Password** button to enter the password for this user name.
5. Click **Next**.
6. On the Schedule page, 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.
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:

8. Select the task you created in the left Navigation bar.
9. Click the **Add** button in the right-hand pane and select the action you want to run.
10. The action will appear in the list in the right-hand pane and will include a number of sub-actions. For example, the 'Import logs into new storage' task action has two sub-actions: 'Select location' and 'Configure input'.
11. Double-click each sub-action to configure them.
12. 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** button on the toolbar. This is a good way to test that the task is working as you expect.
13. 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.

End of Tutorial

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

If you require more information, please visit the WebSpy web site at www.webspy.com. You can also WebSpy Support by emailing 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.

Supported Log Files

Vantage 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.

Vantage currently supports the following log file formats:

- ➔ 3 Com (3 Com Firewall)
- ➔ 8e6 (R2000, R3000)
- ➔ Apache HTTP Server (Access Log)
- ➔ Astaro (Astaro Native Log, Astaro Native Syslog)
- ➔ Avirt (MS Proxy Log Verbose)
- ➔ Bintect VPN (VPN 25)
- ➔ BlueCoat (Proxy SG Common, Proxy SG Squid Native, Proxy SG W3C)
- ➔ BlueReef Virtual Server (Squid Native)
- ➔ CacheXpress (CacheXpress Squid Log)
- ➔ CCProxy
- ➔ CheckPoint Firewall-1
- ➔ Cisco Cache Engine
- ➔ Cisco Systems Inc (IOS Firewall, IOS Firewall IDS)
- ➔ ClearSwift (MailSweeper)
- ➔ ContentKeeper
- ➔ CProxy
- ➔ CSM (Blocking Log, Proxy Log)
- ➔ DansGuardian
- ➔ iPrism (Monitor Log, RT Log, Security Log, Syslog, Syslog v4)
- ➔ JBoss (JBoss Common Log)
- ➔ Microsoft Exchange (5.5, 2000, 2003)
- ➔ Microsoft Internet Connection Firewall
- ➔ Microsoft IIS (Native, NCSA, W3C)
- ➔ Microsoft ISA (Firewall Native, Firewall W3C, Proxy Native, Proxy W3C)
- ➔ Microsoft ISA
- ➔ MIMESweeper (MailSweeper)
- ➔ NetCache (Common, W3C)
- ➔ NetScreen (10, 3, 50)
- ➔ Novell BorderManager (Common Log, Connection Log, Extended Log)
- ➔ Novell GroupWise (Text Log)
- ➔ Novell (iChain W3C Log)
- ➔ Novell Volera (Text Log, W3C)
- ➔ Research Machines (RM) (RM SmartCache)
- ➔ ServGate (Event Log, Mail Filter Log, Security Log, Traffic Log, Virus Log, VPN Log, Web Filter Log)
- ➔ SonicWall (Native)
- ➔ Squid (Common Log, N2H2 Log, Native Log)
- ➔ Squid Proxy (Common Log, N2H2, Native Log)
- ➔ St Bernard Software (IPrism Monitor Log, IPrism RT Log, IPrism Security Log, IPrism Syslog, IPrism Syslog v4)
- ➔ WatchGuard
- ➔ WebSpy (FlowMonitor and Sentinel)

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.

Contact WebSpy

WebSpy North America

(Servicing North and South America)

Suite 202
137 7th Ave West
Kirkland, Washington 98033

Toll free: 888-862-4403
Phone: +1 425-828-4400
Fax: +1 425-828-7115
Email: sales@webspy.com

WebSpy Europe

(Servicing Europe, Middle East and Africa)

3rd Floor, Unit 19
Angel Gate
326 City Road
London, EC1V 2PT

Phone: +44 (0) 207 239 7500
Fax: +44 (0) 207 239 7539
Email: europesales@webspy.co.uk

WebSpy Australia

(Servicing Australia, Asia and the Pacific)

Level 3 Mercury House
33 Richardson 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

WebSpy Support

To contact WebSpy Support, please email support@webspy.com or visit our support page at www.webspy.com/contact/support.aspx