WebSpy FlowMonitor 1.0

Installation and User's Guide

Table of Contents

1. About FlowMonitor

WebSpy FlowMonitor is a Windows NT Service that can collect NetFlow data from correctly configured Cisco routers, for the purpose of providing organizations with byte-accurate Internet traffic information.

FlowMonitor consists of two parts:

- FlowMonitor Service (see below)
- FlowMonitor Console (see page 2)

You should install the service on a computer that can receive NetFlow messages from a Cisco router. Then, you will have to configure your routers to send the NetFlow information to this computer. The FlowMonitor service can only be installed on Windows NT, 2000 or XP operating systems.

The FlowMonitor service collects and logs the NetFlow information to files at a specified location. These log files can then be imported into WebSpy Analyzer for detailed analysis. See FlowMonitor Log Format on page 2 for more information about the log files.

The FlowMonitor console provides the user interface for configuring the FlowMonitor service and should be installed on the administrator's computer. Unlike the service, the console can be installed on Windows 98 and Windows ME.

The FlowMonitor console also charts NetFlow traffic in real time to provide timely information when analyzing bandwidth performance.

1.1. About the FlowMonitor Service

The FlowMonitor service captures and logs any Netflow data that is sent to it by a Cisco Router. You need to configure your Cisco router to send NetFlow messages to the service. Many routers can send NetFlow data to the one FlowMonitor service.

By default, the service listens on port 8777 for any incoming Netflow packets and creates log files, which are saved in the Log Folder location specified in the FlowMonitor console. The log files are named using the convention of YYYYMMDD.log, and have a specific structure. See FlowMonitor Log Format on page 2for more information.

You can change any of the service's default settings using the FlowMonitor console. For information on configuring the service, see Configuring FlowMonitor on page 13.

The service can be installed on any workstation or server running Windows NT or above. FlowMonitor's processing requirements are minimal, so installing the service on a server may provide enhanced uptime without affecting network performance. See Installing FlowMonitor on page 4 for more information.

Please note:
The FlowMonitor service cannot be run on Windows 9x operating systems (such as Windows 98 or ME).

1.2. About the FlowMonitor Console

The FlowMonitor console provides the user interface for configuring your FlowMonitor service.

With the console, you can:

- Connect to a FlowMonitor service and configure its parameters
- View the data being received by the FlowMonitor service in real time in the Traffic Over Time graph
- Register both the service and console

You can configure multiple services using a single console. For more information on configuring the FlowMonitor service using the console, see see Configuring FlowMonitor on page 13.

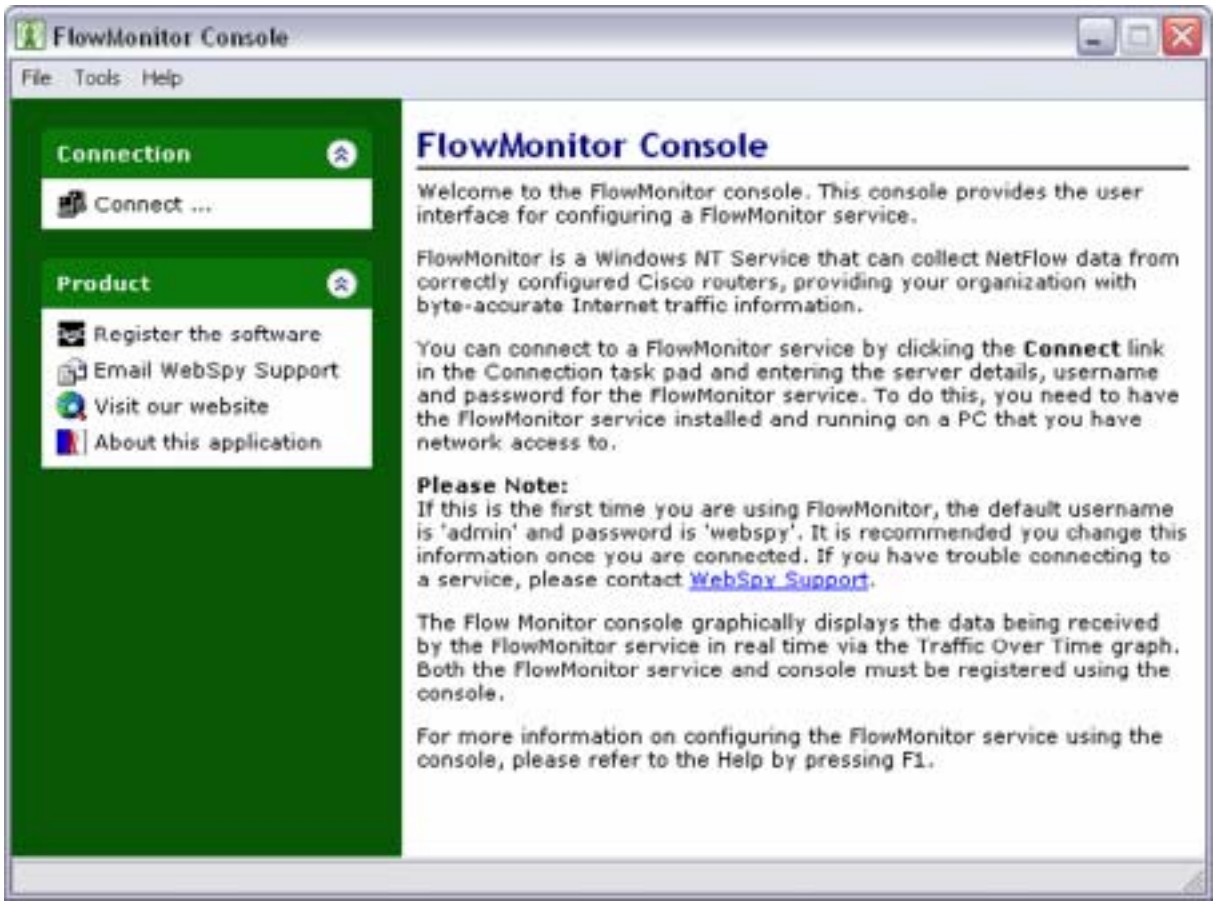

Figure 1: FlowMonitor Console

1.3. FlowMonitor Log Format

The FlowMonitor log file is formatted as ANSI text. Each line is terminated by a CRLF, and each field is separated by a tab.

The field values are as follows:

1 Source IP
2 Destination IP
3 Next Hop IP
4 Input interface

5 Output interface
6 Packets transmitted
7 Bytes transmitted
8 First packet time
9 Last packet time
10 Source port
11 Destination port
12 TCP flags
13 TCP protocol
14 Type of service
15 Destination AS (Autonomous System)
16 Source AS
17 Destination route mask
18 Source route mask
19 NetFlow Device IP (not used by WebSpy Analyzer)

The log files are named using the convention of YYYYMMDD.log and are saved in the Log Folder location specified in the FlowMonitor console.

Because FlowMonitor logs all traffic information, the log files can become quite large. The actual size will depend on the amount of traffic.

1.4. Contact WebSpy

If you have any comments, queries or suggestions regarding any WebSpy products, please forward them to support@webspy.com.

If possible, include in your email the name of the WebSpy product you are using, its version and build number (which can be obtained by selecting **Help | About** from the main menu), the operating system you are using (such as Windows 98, 2000 or XP), and a copy of the log file that is causing issues (if relevant).

If you experience any issues with FlowMonitor, please also include FlowMonitor's Error log and Status log (see page 15).

2. Installing FlowMonitor

When you install WebSpy FlowMonitor, you will first have to determine which computer you should install the FlowMonitor service on. This computer must be running Windows NT or above.

Windows NT 4.0 Workstation
Windows NT Server
Windows 2000 Professional
Windows 2000 Server/Advanced Server
Windows XP Home/Professional

Table 1: Supported Operating Systems

Please note:
The FlowMonitor service cannot be run on Windows 9x operating systems (such as Windows 98 or ME).

Because the service is collecting the NetFlow data, it is important that this computer is available over the entire period you want to collect data. For this reason, you may choose to install the service on a server. The FlowMonitor service has minimal processing requirements, but the log files may consume a significant amount of hard disk space, depending on the amount of traffic passing through the router.

With the FlowMonitor service installed, you will then need to configure your router to send the NetFlow data to the computer. This procedure is described in Configuring Cisco Routers for FlowMonitor below.

Once your trial period has expired, FlowMonitor will stop capturing data unless you purchase FlowMonitor and then register it. See Registering FlowMonitor on page 5 for more information.

2.1. Configuring Cisco Routers for FlowMonitor

You will need to configure your Cisco router so it sends NetFlow data to the FlowMonitor service. You will need to know the IP address of the computer that the service is installed on, and which port the service is set up to listen for the data on.

Before attempting to configure your router, please check that it supports NetFlow. See Routers Supporting NetFlow on page 5 for more information.

To configure NetFlow on the Cisco router you need to perform the following steps:

1 On each interface you want to receive incoming NetFlow packets for you need the following command:
```
(config-if)#ip route-cache flow
```
2 You also need to enter the following global commands:
```
(config)#ip flow-export source <interface number>
(config)#ip flow-export version 5 peer-as
(config)#ip flow-export destination <ip address><port number>
```

Note:
The "ip flow-export destination" needs to have the IP address and port number of the machine running the FlowMonitor service. By default, the

service listens on port 8777 for any incoming NetFlow packets. This port number can be changed, by editing FlowMonitor's Listening Port.

Up to two destinations can be specified by using two 'ip flow-export destination' commands.

For more information on configuring NetFlow on Cisco routers, please consult the relevant Cisco documentation.

2.2. Routers Supporting NetFlow

The following table lists the versions of Cisco IOS software and Cisco Hardware that support NetFlow.

Cisco IOS Software Release Version	Supported NetFlow Export Version(s)	Supported Cisco Hardware Platforms
11.1CA, 11.1CC	v1, v5	7200, 7500, RSP7000
11.2, 11.2P	v1	7200, 7500, RSP7000
11.2P	v1	Route Switch Module (RSM), 11.2(10)P and later
11.3, 11.3T	v1	7200, 7500, RSP7000
12.0	v1, v5	1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000, RSM
12.0T 12.0S	v1, v5	1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000, RSM, MGX 8800 RPM, BPX 8600
12.0(3)T and later 12.0(3)S and later	v1, v5, v8	1400*, 1600*, 1720, 2500*,2600, 3600, 4500, 4700, AS5800, AS5300**, 7200, uBR7200, 7500, RSP7000, RSM, MGX8800 RPM, BPX 8650
12.04XE	V1, v5, v8	7100
N/A	v7	Catalyst 5K NetFlow Feature Card (NFFC) Catalyst 6K with MSFC card
12.0(6)S	v8	12000

*Support for NetFlow Export v1, v5, and v8 on 1600 and 2500 platforms is targeted for Cisco IOS software release 12.0(5)T. NetFlow support for these platforms will not be available in the Cisco IOS 12.0 mainline release.

**Support for NetFlow Export v1, v5, and v8 on AS5300 platform is targeted for Cisco IOS software release 12.0(7)XR.

Cisco 1000/1600/2500/2600/3600/4000/AS5800 Series - NetFlow functionality is supported only in Plus images for these platforms.

See the Cisco NetFlow website for more information.

2.3. Registering FlowMonitor

If you do not register FlowMonitor, your trial will run out thirty days after you first use the program. Once your trial has run out, your FlowMonitor services will no longer capture data.

Before you can register FlowMonitor, you will need to purchase the application. To purchase the application, please contact sales@websp y.com. A serial number will then be forwarded to you.

You will need to register the FlowMonitor console, and then use the registered console to unlock all of your FlowMonitor services.

You must perform the registration on the computer you intend to use to run the FlowMonitor console. If you need to transfer the registration to another computer, please contact WebSpy Support.

To register the FlowMonitor console, go to **Tools | Registration Wizard** to launch the Registration Wizard.

There are three parts to the registration process:

1 Requesting an unlock code
2 Entering an unlock code to register your copy of the FlowMonitor console
3 Unlocking your FlowMonitor services, to register your FlowMonitor services

If you have any problems with the registration process, please contact WebSpy Support.

Note:
Your computer must have an active Internet connection to be able to register your software.

2.3.1. Requesting an Unlock Code

Once you have purchased FlowMonitor, you need to request an unlock code to register your copy of the application.

To request an unlock code:

1 Launch the Registration Wizard by choosing **Tools | Registration Wizard** from the main menu of the FlowMonitor console, or by clicking the **Register the software** link in the Product task pad
2 Once the Registration Wizard is open, you need to enter your details into the Registration Details and User Contact Details pages of the wizard
WARNING:
These details are essential for WebSpy Ltd. to generate a successful unlock code for your copy of FlowMonitor. If you do not supply your correct details, WebSpy Ltd. cannot confirm that you have purchased your software, and an unlock code will not be generated for you.
3 After you have entered all your details, the Submission page will show you the progress of your submission
4 If it is successful, you will be able to click **Finish** to complete the wizard

Once the wizard has been completed, an unlock code for the software will be emailed to the address you provided in the User Contact Details page. You will now need to enter your unlock code.

If, for any reason, you need to reinstall FlowMonitor, use the Registration Wizard to request a new unlock code. You will not be able to use your old unlock code. Please contact WebSpy Support if you have any problems registering your software.

2.3.2. Entering your Unlock Code

After you have requested an unlock code, you will receive an email containing that unlock code. This unlock code needs to be entered into the Registration Wizard.

Note:
You can only use an unlock code on the computer you requested it from.

To enter your unlock code:

1 Launch the Registration Wizard by choosing **Tools | Registration Wizard** from the main menu of the FlowMonitor console
2 Copy the unlock code from the registration email
3 On the Enter Unlock page of the wizard paste the unlock code that you copied from the email into the Unlock Code edit box
4 Click **Next**
5 Your unlock code will be verified, and your registration confirmed
6 To close the wizard, click **Finish**

If, for any reason, you need to reinstall FlowMonitor, use the Registration Wizard to request a new unlock code. You will not be able to use your old unlock code.

You can now use the FlowMonitor console to unlock all of your FlowMonitor services.

2.3.3. Unlocking FlowMonitor Services

Once you have registered the FlowMonitor console, you need to unlock each FlowMonitor service.

To unlock a FlowMonitor service:

1 Start FlowMonitor console
2 Connect to the service you wish to unlock
3 Select **Unlock** from the Connection task pad

Note:
Once WebSpy FlowMonitor's trial period has expired, your FlowMonitor services will not capture data unless you register FlowMonitor and unlock each of the services.

3. Using the FlowMonitor Console

The FlowMonitor console provides the user interface for configuring your FlowMonitor service.

With the console, you can:

- Connect to a FlowMonitor service and configure its parameters
- View the data being received by the FlowMonitor service in real time in the Traffic Over Time graph
- Register both the service and console

You can configure multiple services using a single console.

For more information on configuring the FlowMonitor service using the console, see Configuring FlowMonitor on page 13.

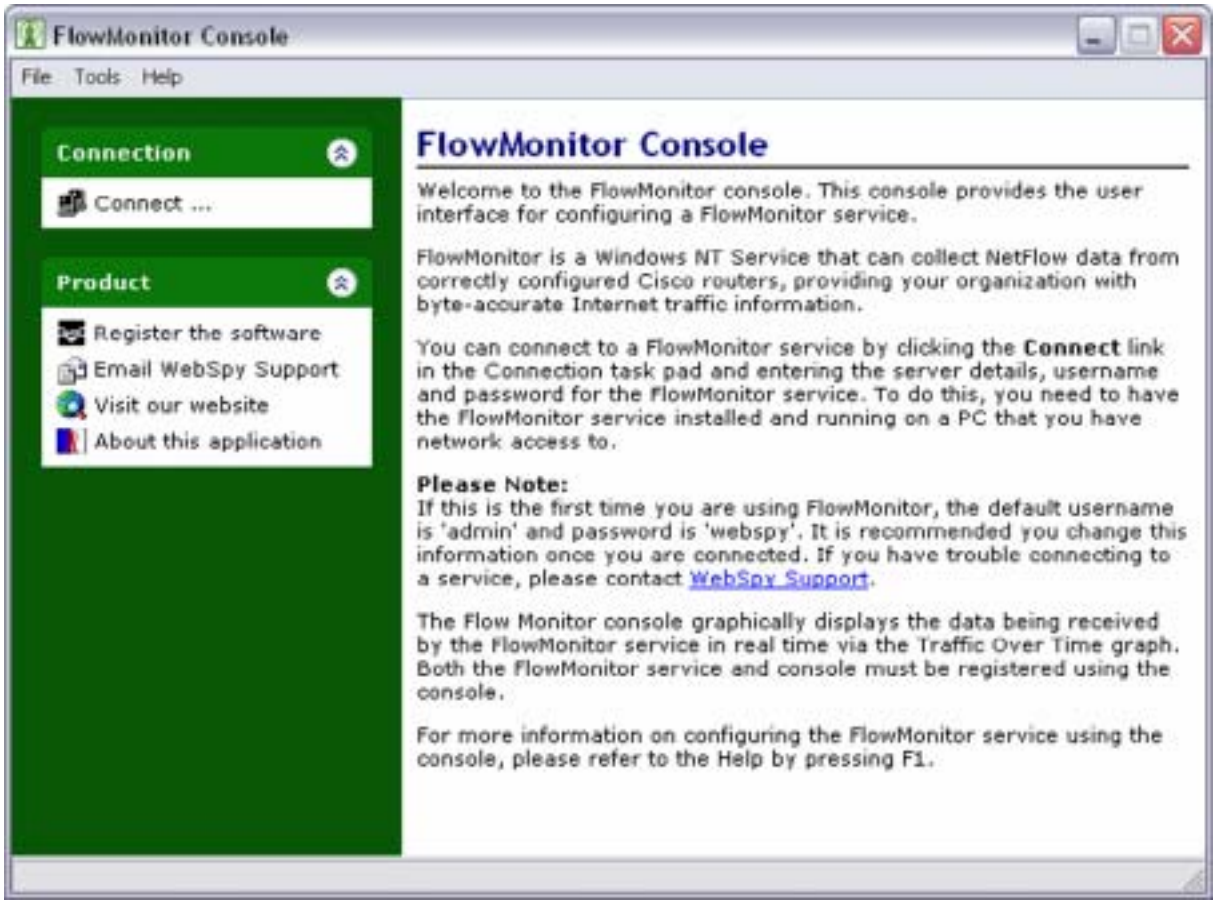

Figure 2: FlowMonitor Console

3.1. Connecting to a FlowMonitor Service

The FlowMonitor console enables you to connect to a FlowMonitor service so you can configure its parameters.

You can connect to a FlowMonitor service by clicking the **Connect** link in the Connection task pad and entering the server details, username and password for the FlowMonitor service.

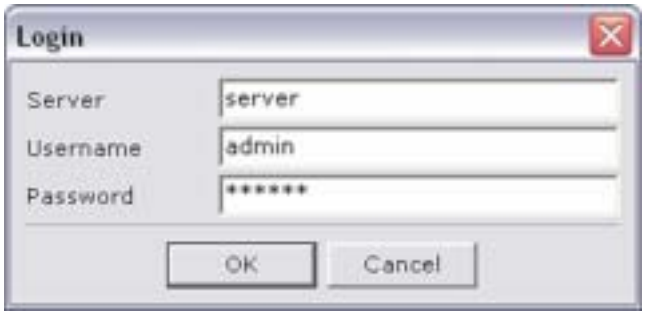

Figure 3: Login dialog

If this is the first time you have connected to the FlowMonitor service, the default username and password is:

Username: admin

Password: webspy

It is recommended that you change this information once you are connected. If you have trouble connecting to a service, please contact WebSpy Support.

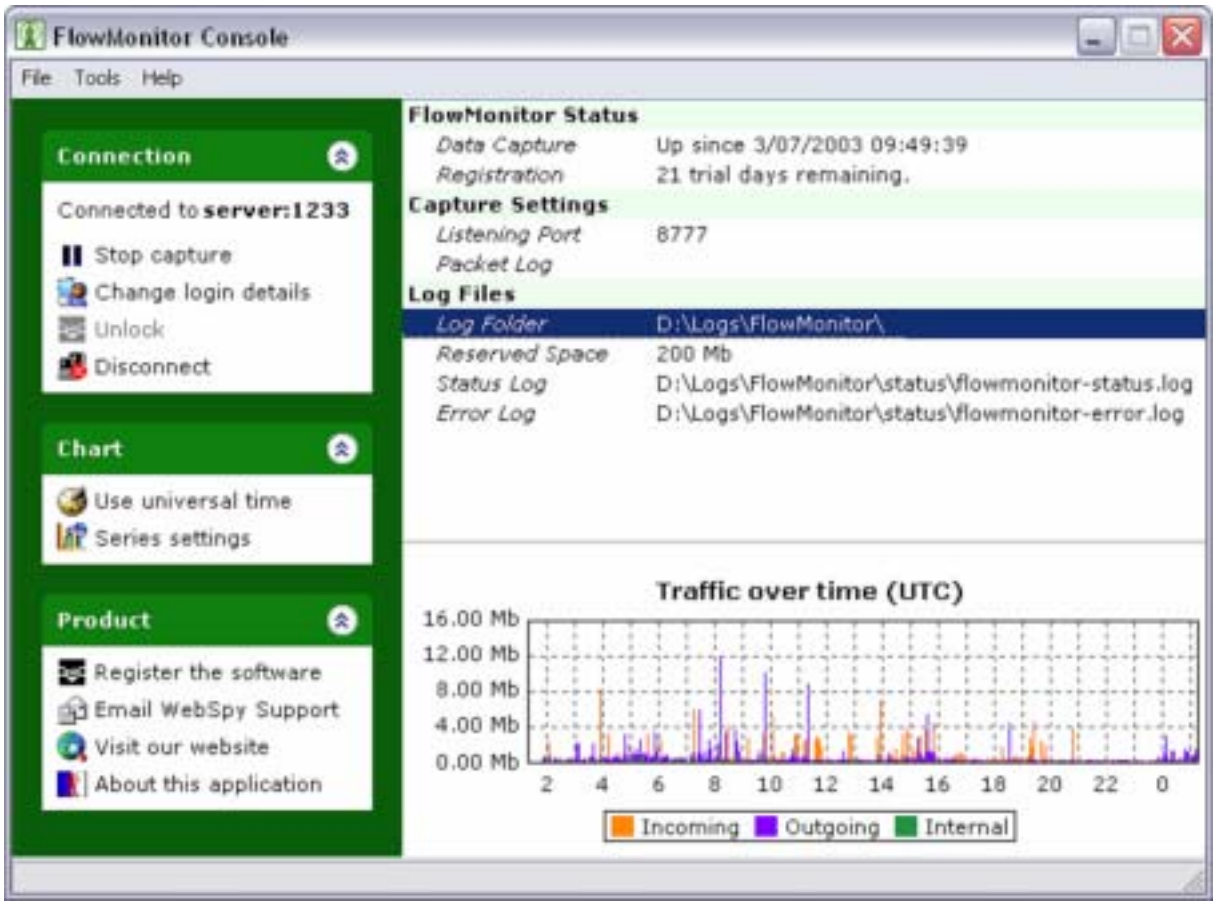

Figure 4: FlowMonitor Console, connected to service

Once you are connected, you can disconnect from the service and connect to another FlowMonitor service that you may be running elsewhere.

3.2. Disconnecting from a FlowMonitor Service

Once you are connected to a FlowMonitor service, you can disconnect at any time by clicking the **Disconnect** link in the Connection task pad.

This enables you to connect to other FlowMonitor services without closing the FlowMonitor console.

3.3. Updating Login Information

Once you are connected to a FlowMonitor service, you can change the login information (username and password) at any time. It is recommended that you do this when you login to each service for the first time using the default login of 'admin' and password of 'webspy'.

To change the login information of a FlowMonitor service:

1 Connect to the FlowMonitor service using your existing username and password
2 Click the **Change login** link on the Connections task pad
3 Enter your new username and password, and retype the new password to confirm it
4 Click **OK**

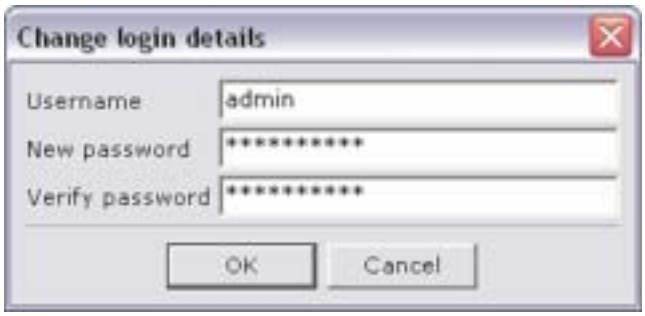

Figure 5: Change login details dialog

You may want to do this on a regular basis to prevent unauthorized personnel from guessing your password and changing the configuration.

3.4. Starting and Stopping FlowMonitor

You can start and stop FlowMonitor from capturing NetFlow data at any time by clicking the **Stop capture / Start capture** link in the Connections task pad.

You do not need to manually stop data capture when making configuration changes to the FlowMonitor service.

Each time you stop and restart the FlowMonitor service, the 'Up since..." value will be updated. This value is displayed on the Data Capture row in the FlowMonitor Status section of the FlowMonitor console. It is also recorded in the Status log.

3.5. Using the Traffic Over Time Chart

As FlowMonitor captures NetFlow traffic, the amount of data captured is displayed graphically on the Traffic over time chart at the bottom of the FlowMonitor console.

This graph gives you a quick reference to the times that network traffic is heavy. Time is displayed on the horizontal axis, with traffic size displayed on the vertical axis.

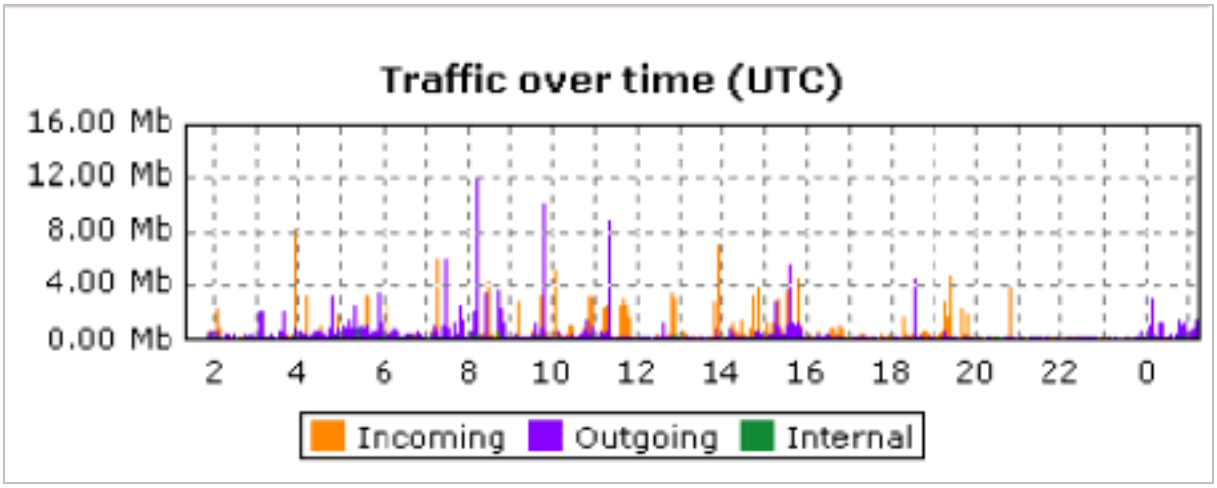

Figure 6: Traffic over Time Chart

Traffic over time can be displayed using Coordinated Universal Time (UTC), or using your local time settings. You can change between these two settings by clicking the **Use local time / Use universal time** link in the Chart task pad.

Two NetFlow datasets exists for every NetFlow configured interface pair on a router (one dataset for incoming data, and another for outgoing data).

A separate series is displayed on the Traffic over time chart for each NetFlow dataset. You can change the display options for each dataset, such as the series name (caption), color, and style (column or line). For more information see Changing Series Settings.

3.6. Changing Series Settings

A separate series is displayed on the Traffic over time chart for each NetFlow dataset.

Two NetFlow datasets exists for every NetFlow configured interface pair on a router. There is one dataset for incoming data, and another for outgoing data.

If you have three interfaces, IfOne, IfTwo and IfThree, you will have 6 NetFlow datasets:
- Data flowing from IfOne to IfTwo
- Data flowing from IfOne to IfThree
- Data flowing from IfTwo to IfOne
- Data flowing from IfTwo to IfThree
- Data flowing from IfThree to IfOne
- Data flowing from IfThree to IfTwo

You can change the display options for each dataset, such as the series name (caption), color, and style (column or line).

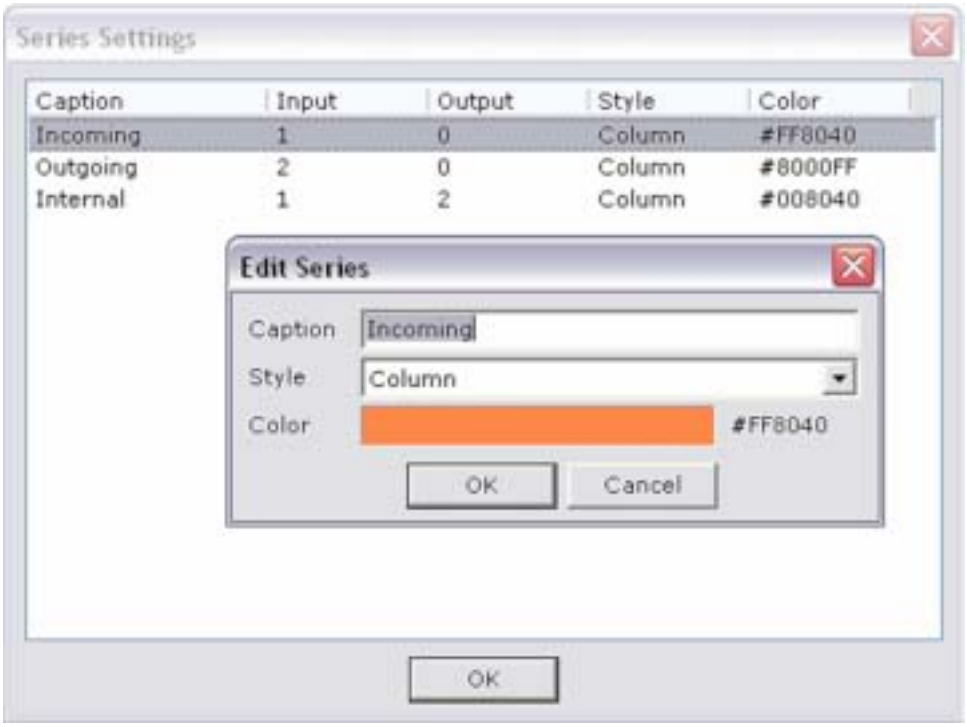

Figure 7: Edit Series Settings dialog

To change the series settings for a NetFlow dataset:

1 Connect to the FlowMonitor service that you want to edit
2 Click the **Series Settings** link on the Chart task pad
3 Double click the NetFlow dataset that you want to change the series settings for. This displays the Edit Series dialog.

Please note:
NetFlow datasets have values representing the input and output router interfaces. These values are the SNMP interface identifiers for your router's interfaces. You can discover which SNMP interface identifiers represent each of your router's interfaces using a SNMP application that enables you to query your router's interfaces.

4 On the Edit Series dialog, you can enter an identifier for the NetFlow dataset into the 'Caption' edit box. You can also select whether the NetFlow dataset is represented as a column or line chart. The color of the NetFlow dataset on the Traffic over time chart can also be changed by either typing a new value into the edit box, or clicking in the box to launch the Color picker dialog.
5 Click **OK** on the Edit Series dialog once you have made all your changes
6 Click **OK** on the Series Settings dialog to return to the FlowMonitor console and view how the new series settings are displayed on the Traffic over time chart
7 If you want to keep these settings, you will need to save them before you disconnect from the FlowMonitor service.

4. Configuring FlowMonitor

The FlowMonitor service is configured using the FlowMonitor console application. To launch the FlowMonitor console, select the **FlowMonitor Console** shortcut in the WebSpy program group in your Start menu.

On the FlowMonitor console, there are three headings:

- FlowMonitor Status
- Capture Settings
- Log Files

Under the FlowMonitor Status heading, the current capture and registration settings are displayed.

Using the FlowMonitor console, you can configure parameters that relate to the capture of data, as well as log file settings.

There are two settings that you can edit that relate to the way FlowMonitor captures data:

- Listening Port, which is the port that FlowMonitor uses to listen for NetFlow messages coming in from a Cisco router
- Packet Log, which is the location of a file that stores the raw binary NetFlow information, if required for troubleshooting

The following Log File settings can be edited:

- Log Folder
- Reserved Space
- Status Log
- Error Log

When you make any changes to a service's configuration, you will need to save the settings before you disconnect from the service, or your changes will be lost.

4.1. Saving Changes

Once you make a change to a FlowMonitor service's configuration (see Configuring Flow Monitor) you will need to save the changes.

When you save changes, the FlowMonitor service will stop, make the changes, and restart. This will reset the 'Up since' value and the chart in the FlowMonitor console.

To save your configuration changes click the **Save changes** link in the Connection task pad.

Figure 8: Save Changes link

You can also cancel any changes you have made since the last save to keep your previous settings.

4.2. Cancelling Changes

You can cancel any changes you have made to the FlowMonitor service's configuration since the last save to keep your original settings.

Figure 9: Cancel Changes link

To cancel changes and restore all settings to what they were since the last save, click the **Cancel changes** link in the Connection task pad.

4.3. Changing the Listening Port

The Listening Port is the port that FlowMonitor uses to listen for NetFlow messages coming in from a Cisco router. By default, the Listening Port is 8777; however, you may want to change the port number if it conflicts with another application you are running.

> **Please note:**
> If you change the Listening Port, you will also need to configure the Cisco router to send NetFlow data to this new port number.

To edit the Listening Port:

1 Connect to the FlowMonitor service that you want to change the Listening port for
2 Double click the Listening Port row on the FlowMonitor console
3 Enter the new value for the Listening Port
4 Click **OK**
5 If you want to keep these settings, you will need to save them before you disconnect from the FlowMonitor service

See also Configuring Cisco Routers for FlowMonitor.

4.4. Changing the Packet Log

The Packet log is a file that stores the raw binary NetFlow information that the Cisco router sends. It is unlikely that you will need to use this log file; however, FlowMonitor provides you with a location to store this information for troubleshooting and debugging purposes.

You are able to edit the location and file name of the Packet log. The log is saved on the computer that the service is running on.

To edit the location and file name of the Packet log:

1 Connect to the FlowMonitor service that you want to edit
2 Double click the Packet Log row on the FlowMonitor console
3 Enter the new UNC path for the packet log e.g. C:\FlowMonitor\logs\packetlog.log
4 Click **OK**
5 If you want to keep these settings, you will need to save them before you disconnect from the FlowMonitor service

> **Please note:**
> If no file name is specified, this raw information will not be logged. NetFlow information will still be logged to the specified Log Folder.

Another data capture setting that you can edit is the Listening Port (see above).

4.5. Changing the Log Folder

FlowMonitor stores NetFlow information in the Log Folder location. The files created in this location can be imported into WebSpy Analyzer for analysis.

The log files are created with the default naming convention of YYYYMMDD.log. This naming convention and log file structure cannot be changed.

You can change the Log Folder to store these log files in a more convenient location.

To change the location of the Log Folder:

1 Connect to the FlowMonitor service that you want to edit
2 Double click the Log Folder row on the FlowMonitor console
3 Enter the new UNC path for the Log Folder. You do not need to specify a file name.
4 Click **OK**
5 If you want to keep these settings, you will need to save them before you disconnect from the FlowMonitor service

4.6. Changing the Reserved Space

As FlowMonitor continually logs NetFlow data, the Reserved Space setting prevents FlowMonitor from filling up hard disk space. If the Reserved Space is not set, logged NetFlow data will eventually fill up the computer's hard disk, and cause other applications running on the same computer to fail.

FlowMonitor will stop logging data when the amount of free hard disk space reaches the value specified in Reserved Space.

To change the Reserved Space value:

1 Connect to the FlowMonitor service that you want to edit
2 Double click the Reserved Space row on the FlowMonitor console
3 Enter the new value in Megabytes (MB) for the Reserved Space. For example, entering 300 sets the Reserved Space to 300MB. Enter an appropriate value for your system.
4 Click **OK**
5 If you want to keep these settings, you will need to save them before you disconnect from the FlowMonitor service

When the Reserved Space is reached, the FlowMonitor service will stop capturing NetFlow data, and write an error message to the Error log and display the error on the FlowMonitor console. The service will not be able to capture data again until you free hard drive space and restart the service.

Because FlowMonitor logs all traffic information, the log files can become quite large. The actual size will depend on the amount of traffic monitored.

4.7. Changing the Status Log

The Status log records the activity of the FlowMonitor service,:

- When it was last shut down
- When it was last started
- The operating system it is running on

- Its current registration status

You can change the location of FlowMonitor's Status log to store it in a more convenient location. You can also change the file name of the Status log.

The log is saved on the computer that the service is running on.

To change the location and file name of the Status log:

1 Connect to the FlowMonitor service that you want to edit
2 Double click the Status Log row on the FlowMonitor console
3 Enter the new UNC path for the Status log
4 Click **OK**
5 If you want to keep these settings, you will need to save them before you disconnect from the FlowMonitor service

Figure 10: Edit dialog

4.8. Changing the Error Log

The Error log keeps a record of any problems that FlowMonitor encounters and is useful for troubleshooting. The log is saved on the computer that the service is running on.

You can change the location of FlowMonitor's Error log to store it in a more convenient location. You can also change the file name of the Error log.

To change the location and file name of the Error log:

1 Connect to the FlowMonitor service that you want to edit
2 Double click the Error log row on the FlowMonitor console
3 Enter the new UNC path for the Error log
4 Click **OK**
5 If you want to keep these settings, you will need to save them before you disconnect from the FlowMonitor service

5. Glossary

Autonomous System

Internet (TCP/IP) terminology for a collection of gateways (routers) that fall under one administrative entity and that cooperate using a common interior gateway protocol (IGP).

Error log

The Error log keeps a record of any problems that FlowMonitor encounters and is useful for troubleshooting. The log is saved on the computer that the service is running on.

Interface

A router's connection to a network. Interfaces can be configured to use certain protocols and addresses.

Listening Port

Each application program that needs to communicate over Internet Protocol (IP) is associated with a unique port number, which represents a logical channel or channel endpoint in a communications system. For example HTTP (web) data is associated with port 80, SMTP (email) data is associated with port 25.

NetFlow

NetFlow is a Cisco proprietary protocol that helps measure network and application resource utilization. It works by capturing specific information about the data that passes through routers that can then be analyzed and reported on.

The information captured is "byte accurate" and excellent for determining the amount of information sent and received for billing purposes.

UNC Path

A UNC path describes the location of a volume, directory or file. The path is not dependent on the relative location of the machine where the file or folder is actually stored.

UNC is an acronym for Universal/Uniform Naming Convention.

Examples:

- \\servername\c$\flowmonitor\logs
- C:\Data\Logs

WebSpy Analyzer

A range of products from WebSpy that enable you to load a wide variety of log files, including the FlowMonitor format, and provides the ability to conduct detailed analysis on the loaded information.

6. Index