Sparrow^{IQ} User Guide

Release 1.1

Table of Contents

1. Introduction

Sparrow[IQ] is a flow analytics solution which provides near real-time visibility of the network traffic. It allows the IT administrator to monitor the network usage based on conversation, application, user, class and more without the requirement of expensive flow-capable routers and switches. Sparrow[IQ] achieves this by listening to all the traffic on the network and generating flow-type data. For example, to monitor all external transactions, it is imperative to make sure that Sparrow[IQ] is deployed at the gateway where all the network traffic passes through.

Sparrow[IQ] also provides the user with various monitoring, alerting and reporting capabilities.

1.1 *Key Features*

1. Flow Analysis dashboard: Customized dashboard provides network usage statistics and easy to follow trends
2. Network traffic usage via various data points such as:
    a. Top Conversations
    b. Top Applications
    c. Top Users/Endpoints
    d. Top Classes of Service
    e. Bandwidth Usage by Rate
    f. Traffic Volume
    g. Overall traffic summary/statistics
3. Single-click drilldown capabilities
4. Flow-based long term reports
5. Custom alert setup for bandwidth and traffic volume
6. Track department-wise usage via IP grouping

1.2 *Requirements Specification*

The Sparrow[IQ] analytics and monitoring solution consists of

- A PC on which Sparrow[IQ] software is installed
- A switch with port mirroring (also known as SPAN) or a Tap to channel the network traffic to the Sparrow[IQ] machine
- A web browser to access Sparrow[IQ]

1.2.1 Hardware Requirements for the Sparrow[IQ] PC

	Minimum System Requirements	Recommended System Requirements
Processor	2+ GHz	2.6+Ghz

RAM	2GB	4GB
Disk space	80GB	100GB
Ethernet interfaces	One interface, if using a switch with port mirroring OR Two Interfaces, if using a Tap with aggregator port OR Three interfaces, if using a regular Tap	

1.2.2 Software Requirements for Sparrow[IQ] PC

Sparrow[IQ] is supported on the following Operating Systems:

- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 7

Sparrow[IQ] also requires:

- Microsoft Visual C++ Redistributable 2008

The Visual C++ Redistributable 2008 package can be downloaded for free from Microsoft's website. Check the installed programs list if the packages are already installed. Note that the multiple versions of the VC++ Redistributable can co-exist on the PC without any impacts.

1.2.3 Virtual Environments

Sparrow[IQ] has been successfully tested on the following virtual environments

Virtual Host Technology	Client OS
VMWare vSphere Hypervisor (formerly ESXi 5.0)	Windows XP, Vista and 7
VMWare Player	Windows XP, Vista and 7

1.2.4 Network Requirements

Sparrow[IQ] requires access to all the network traffic that needs to be monitored. This is achieved by sending a copy of all traffic to the Sparrow[IQ] machine using either a SPAN capable switch (port mirroring) or a network tap.

Port mirroring or *SPAN*- Please check your switch's user manual to verify that the feature exists and follow the specified configuration steps to enable port mirroring to one free port. This is the port that the Sparrow[IQ] PC will be connecting to.

Network Tap - If using a Tap, the input and output ports need to be connected to allow the data to pass through. The Sparrow[IQ] PC is connected to the drop of the Tap where data is copied to. The drops from Tap will be either one or two connections depending on the type of Tap. If it is an Aggregator Tap, only one Ethernet connection will be available; if not there will be two Ethernet connections.

1.2.5 Supported Browsers

The interface to access Sparrow[IQ] is via a standard web browser. Sparrow[IQ] can be accessed from any machine in the network as long as the Sparrow[IQ] PC is reachable. This includes all connected computers, tablets and phones. The following web browsers are supported:

- Firefox 13, 14
- Chrome 20, 21
- Internet Explorer 9
- Safari 5

1.3 *Release Notes*

- Please ensure that the PC does not go into sleep/hibernation mode. Sparrow[IQ] has been observed to consume unnecessary processor cycles when a PC wakes up from sleep/hibernation mode. This issue will be addressed in future release.
- Some Windows machines (especially laptops) have default settings that may disable Ethernet interfaces when a power cord is not connected, in order to save power. Sparrow[IQ] will not be able to collect any data from the interfaces in this case. It is recommended that if such power saving options is enabled on the laptop, the power cord be connected for Sparrow[IQ] to operate.
- Sparrow[IQ] becomes unstable in case of a power cut and cannot be rolled back into a stable state. Sparrow[IQ] will need to be reinstalled (with a loss of old data) to get Sparrow[IQ] working again. This issue will be addressed in the next release.
- If the network cable is physically disconnected and connected to a different switch port while running Sparrow[IQ], data collection may be interfered. Sparrow[IQ] will need to be restarted to return to a normal state.
- All bandwidth gadgets (bandwidth rate and traffic volume) data is delayed by three minutes. The rest of the gadgets provide up to the minute data.
- Mouse-over the pie charts are observed to not present a tooltip to the user when using Internet Explorer 9.
- Wireless interfaces: Wireless interface monitoring is not supported under Windows XP. In Windows Vista and Windows 7, interfaces simply called *Microsoft* will appear in the list. You may use these for monitoring using the wireless interface. Note that an AirPCAP adapter needs to be installed for this to function.

1.4 *Contact Information*

For technical support, contact us at

support@sparrowiq.com

For all other information, contact us at

sales@sparrowiq.com

2. Installation and Licensing

2.1 *Initial Install*

It is recommended that Sparrow^{IQ} be installed on a dedicated PC with a configuration similar to the listed Recommended System Requirements in Section 1.2.1.

One can download a trial or purchase a Sparrow^{IQ} by going to www.sparrowiq.com. The package is an all-in-one solution and will install all the various pieces of libraries and software necessary for Sparrow^{IQ} to run. Double-clicking on the installation package will initiate the standard installation steps of license agreement, target directory etc.

Software requirements for Sparrow^{IQ} include the Microsoft Visual C++ Redistributable 2008 package, which is available for free download via Microsoft's website. Note that multiple versions of the Redistributable package can co-exist in the system.

2.2 *Upgrades*

One can choose to initiate installation of a newer version of Sparrow^{IQ} without uninstalling the older version. Sparrow^{IQ} will remove the older version if found in the system.

Sparrow^{IQ} will automatically retain the existing network data so that the old data (run Reports etc.) with the new updated version is still usable.

2.3 *Licensing*

All versions of Sparrow^{IQ} require a license key. You may obtain one of the following licenses:

1. A Trial license - you only need to specify name and email address.
2. Purchase Sparrow^{IQ}. When purchasing Sparrow^{IQ}, the PC on which it runs has to be identified by a SystemID.

For both the options, an email will be sent to the registered address with a Sparrow^{IQ} license.

	Sparrow^{IQ} Trial	Sparrow^{IQ} Free	Sparrow^{IQ} 7	Sparrow^{IQ} 15	Sparrow^{IQ} 30
Maximum Rate Supported	30 Mbps	7 Mbps	7 Mbps	15 Mbps	30 Mbps
# of concurrent users	1	1	1	2	2
# of user accounts	5	5	5	5	5
Historical Reporting	1 week	-	1 month	2 months	3 months
Max # of Configured Alerts	3	-	3	7	15
Max # of Stored Alerts	30	-	30	50	100

2.3.1 Sparrow^{IQ} Trial License

One can try Sparrow^{IQ} before purchasing for free. Simply register with a valid email address and a Sparrow^{IQ} Trial license will be emailed to the address, with most features enabled and valid for 15 days.

2.3.2 SparrowIQ Free License

Once the trial license expires, SparrowIQ automatically switches to the *Free Mode*. In this mode, only the bandwidth gadget on dashboard is available to use.

2.3.3 SparrowIQ Full License

SparrowIQ is available for different levels of bandwidth support. All SparrowIQ purchases are perpetual licenses.

Note that SparrowIQ is tied to a PC and you will need to provide the SystemID for the purchase. See Section 2.3.4 on details of obtaining the SystemID.

The supported levels of bandwidth are:

1. SparrowIQ 7 – a perpetual license supporting upto 7 Mbps.
2. SparrowIQ 15 - a perpetual license supporting upto 15 Mbps.
3. SparrowIQ 30 - a perpetual license supporting upto 30 Mbps.

Threshold Allowance

Even though the numbers stated above are 7, 15 and 30 Mbps, SparrowIQ provides you with a window of an extra 25% allowance, before SparrowIQ starts dropping packets. So, for SparrowIQ7, the max threshold value is 8.75Mbps, for SparrowIQ15 – the max threshold is 18.75Mbps and for SparrowIQ30 – the max is 37.5Mbps.

Once the sustained bandwidth stays above the real max threshold value, data will be dropped by SparrowIQ.

Bandwidth calculation

The above numbers – 7/15/30 Mbps are tracked and calculated as a *moving average* and not based on instantaneous bandwidth. So, the network bandwidth may spike up for a few seconds or minutes to a higher value, but if the moving average stays below the threshold value, packets will not be dropped.

2.3.4 System ID

Each SparrowIQ license is tied to one PC and requires you to identify the PC with a SystemID during the purchase process. To obtain this SystemID, you can use one of the following methods:

- If SparrowIQ is already installed as a trial, launch the Configuration (right-click on SparrowIQ icon in the system tray and select Configuration). The dialog box provided will display the installed PC's SystemID.
- Download and install SparrowIQ and on first run, it will prompt for a license and specify the SystemID of the PC, which can then be used to complete order online.
- Download the 'SystemIDFinder' package from the Support page on www.sparrowiq.com. Once downloaded, run the executable file to obtain the SystemID of the PC.

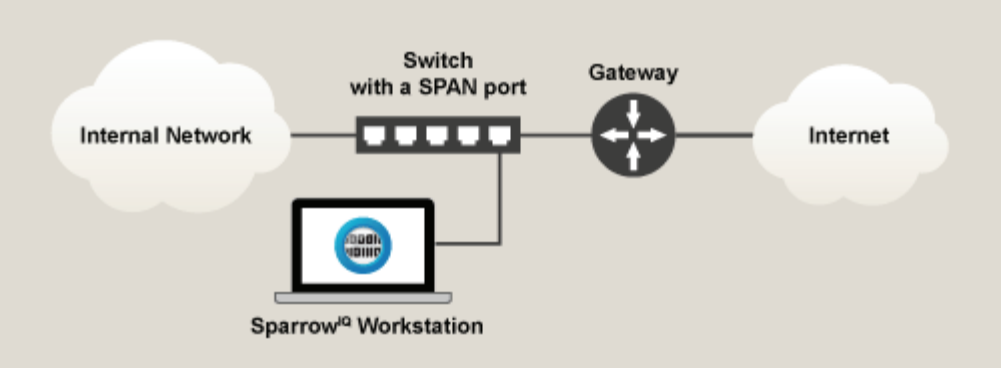
2.4 *Uninstall*

Sparrow[IQ] will prompt you to confirm if you want to remove Winpcap. Winpcap is a library which may be used by other software on the PC. If removed, other software packages may not work which depend on Winpcap.

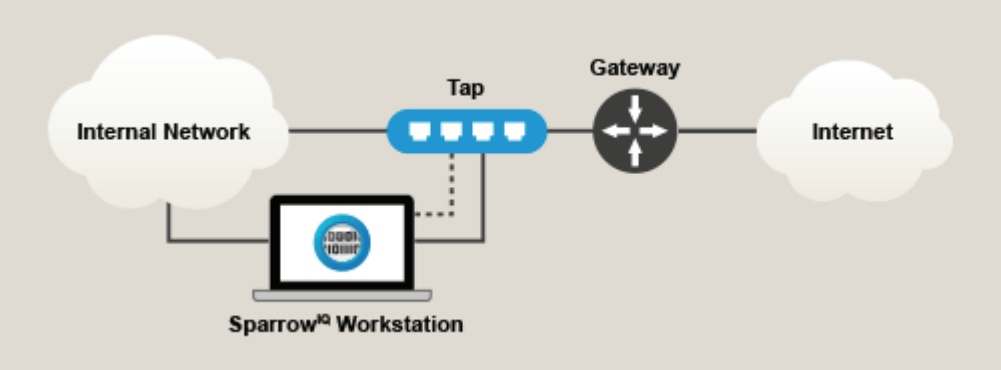
Before removing all files, Sparrow[IQ] will also confirm if the database is to be saved for future updates/access.

3. Deployment

Sparrow^{IQ} requires access to all the network traffic that needs to be monitored. This is achieved by sending a copy of all traffic to the Sparrow^{IQ} machine using either a SPAN capable switch (port mirroring) or a network tap.



3.1 *Deployment using SPAN switch*



3.2 *Deployment using Network Tap*

3.3 *Launch & Access*

To launch Sparrow^{IQ}, select SparrowIQ > SparrowIQ Analyzer from the Windows start menu. On the first startup, it will prompt you for a license key and when entered and confirmed, disappears as an icon into the system tray. Note that it may take a minute or so for all the processes to start up.

To access Sparrow^{IQ} on the same PC, one can either select SparrowIQ > SparrowIQ Viewer from Windows start menu or click on Sparrow^{IQ} Viewer from right-clicking the Sparrow^{IQ} icon in the system tray. This will launch the default web browser and brings up the login screen of Sparrow^{IQ}.

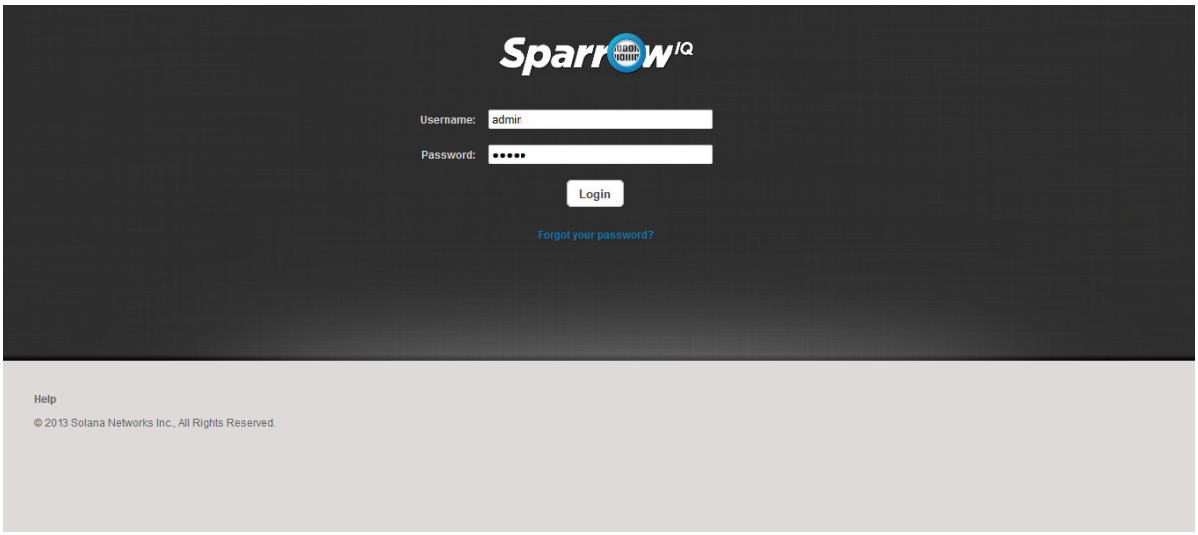
Sparrow^{IQ} can also be accessed from anywhere in the network by specifying the IP address of the Sparrow^{IQ} PC. The default port to access Sparrow^{IQ} is 8000. Please make sure that the access port is not blocked by any firewall in the network.

3.4 *Login*

Once Sparrow^{IQ} is installed and deployed in the network, one can access Sparrow^{IQ} from any machine in the network. Sparrow^{IQ} can be accessed by using a computer, phone or tablet connected to the local network. Enter the IP address and port number of the Sparrow^{IQ} PC on one of the supported web browsers and this will bring up the login page as shown below.

For e.g.: If Sparrow^{IQ} PC is at IP address 192.168.1.100, enter the following in the address bar on the browser.

http://192.168.1.100:8000



Sparrow^{IQ} is shipped with one account – 'admin'. The default login credentials are:

Username: admin

Password: admin

One may choose to change the password anytime by clicking the lock icon in the Users tab under the Settings page. If accessing Sparrow^{IQ} on the installed PC, using the address http://localhost:8000 also works.

A forgotten password can be reset by clicking the "Forgot your password?" link and entering the email address associated with your SparrowIQ account. Instructions will be emailed to the address provided.

Use Case:

"I have decided to give SparrowIQ a try. Can you give me step-by-step instructions to get started?"

This assumes you have the necessary hardware available.

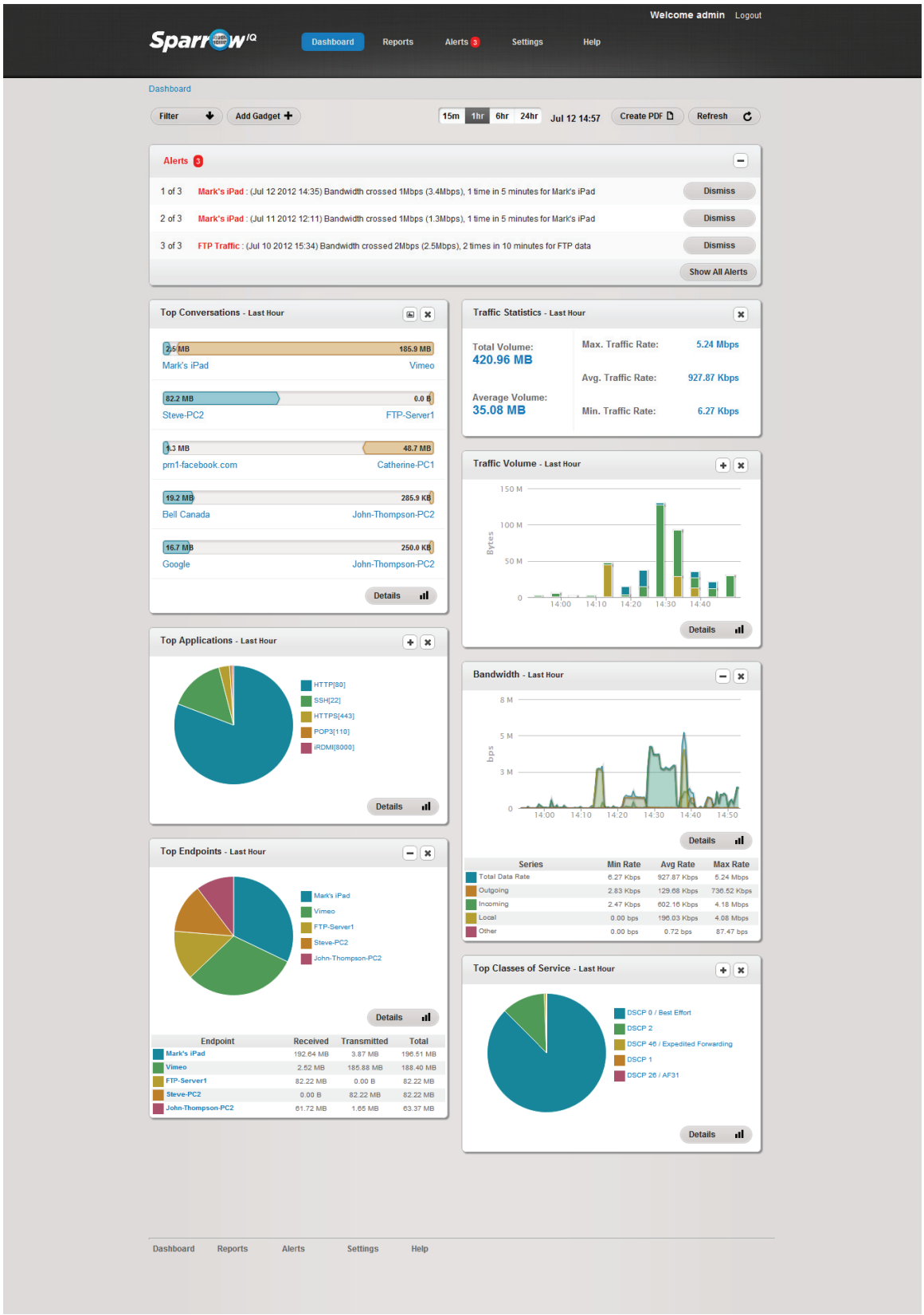
1. Go to SparrowIQ website and sign up for a free trial version. An email will be sent to your registered email address with a trial license.
2. Download and install SparrowIQ on a PC meeting the minimum requirements.
3. Connect the PC to a switch with port mirroring switch (which is configured to mirror traffic to that port) or a Tap with the drops going to the SparrowIQ PC.
4. Start SparrowIQ - Click on SparrowIQ Analyzer under Windows Start menu > SparrowIQ.
5. You will be prompted for a license. Enter the trial license you received via email and click *Validate*.
6. Right click on the SparrowIQ icon in the taskbar and click SparrowIQ Viewer. This will bring up your default web browser and take you to the login page. Enter the following credentials and click *Login*
    - Username: *admin*
    - Password: *admin*
7. Go to the *Settings* > *Probe* page and select the appropriate option and the appropriate interface(s) for your setup - Span or Tap mode, interface selection under each option etc. If changes are made, make sure you click *Save* after the changes.

You are now ready to monitor your network using SparrowIQ. Note that there is a delay of about 3 minutes for the data to show up on the gadgets in the dashboard. If you still do not see any data after the wait, please refer to our Troubleshooting guide.

4. The Dashboard

The extracted data by Sparrow[IQ] is organized so that the following are readily available to the user. If not already added, add a gadget by clicking *Add Gadget*. Gadgets can be dragged and dropped anywhere on the dashboard.

1. Top Conversations
2. Top Endpoints
3. Top Applications
4. Top Classes of Service
5. Bandwidth
6. Traffic Volume
7. Traffic Statistics


Welcome admin Logout
SparrowIQ
Dashboard
Reports
Alerts 3
Settings
Help
Dashboard
Filter
Add Gadget
15m 1hr 6hr 24hr
Jul 12 14:57
Create PDF
Refresh
Alerts 3
1 of 3 Mark's iPad : (Jul 12 2012 14:35) Bandwidth crossed 1Mbps (3.4Mbps), 1 time in 5 minutes for Mark's iPad
Dismiss
2 of 3 Mark's iPad : (Jul 11 2012 12:11) Bandwidth crossed 1Mbps (1.3Mbps), 1 time in 5 minutes for Mark's iPad
Dismiss
3 of 3 FTP Traffic : (Jul 10 2012 15:34) Bandwidth crossed 2Mbps (2.5Mbps), 2 times in 10 minutes for FTP data
Dismiss
Show All Alerts
Top Conversations - Last Hour
2.5 MB
185.9 MB
Mark's iPad
Vimeo
82.2 MB
0.0 B
Steve-PC2
FTP-Server1
1.3 MB
48.7 MB
prn1-facebook.com
Catherine-PC1
19.2 MB
285.9 KB
Bell Canada
John-Thompson-PC2
16.7 MB
250.0 KB
Google
John-Thompson-PC2
Details
Traffic Statistics - Last Hour
Total Volume:
420.96 MB
Average Volume:
35.08 MB
Max. Traffic Rate:
5.24 Mbps
Avg. Traffic Rate:
927.87 Kbps
Min. Traffic Rate:
6.27 Kbps
Traffic Volume - Last Hour
150 M
100 M
50 M
0
Bytes
14:00
14:10
14:20
14:30
14:40
Details
Top Applications - Last Hour
HTTP[80]
SSH[22]
HTTPS[443]
POP3[110]
iRDMI[8000]
Details
Bandwidth - Last Hour
8 M
5 M
3 M
0
bps
14:00
14:10
14:20
14:30
14:40
14:50
Details
Series
Min Rate
Avg Rate
Max Rate
Total Data Rate
6.27 Kbps
927.87 Kbps
5.24 Mbps
Outgoing
2.83 Kbps
129.68 Kbps
736.52 Kbps
Incoming
2.47 Kbps
602.16 Kbps
4.18 Mbps
Local
0.00 bps
196.03 Kbps
4.08 Mbps
Other
0.00 bps
0.72 bps
87.47 bps
Top Endpoints - Last Hour
Mark's iPad
Vimeo
FTP-Server1
Steve-PC2
John-Thompson-PC2
Details
Endpoint
Received
Transmitted
Total
Mark's iPad
192.64 MB
3.87 MB
196.51 MB
Vimeo
2.52 MB
185.88 MB
188.40 MB
FTP-Server1
82.22 MB
0.00 B
82.22 MB
Steve-PC2
0.00 B
82.22 MB
82.22 MB
John-Thompson-PC2
61.72 MB
1.65 MB
63.37 MB
Top Classes of Service - Last Hour
DSCP 0 / Best Effort
DSCP 2
DSCP 46 / Expedited Forwarding
DSCP 1
DSCP 26 / AF31
Details
Dashboard
Reports
Alerts
Settings
Help

The dashboard displays a gadget for each of the stated data points and displays the top 5 values. The data view can also be customized to various timeframes such as 15m, 1h, 6h or 24h.

Pie Charts: Some of the gadgets display the data depicted as a pie chart. The data depicted on dashboard shows the top 5 entries for the metric in question. The pie chart will fill this out to show the relative consumption adding up to 100% to complete the circle.

For e.g., if an endpoint pie chart gadget says that UserA is consuming 40% of data, this only refers in relation to the other four entries shown. The actual data consumed by UserA in the whole network can be seen in the drilldown mode in the Details gadget with an entry "Percentage of All Traffic" – which shows the real percentage.

4.1 *Timeframes*

This allows one to select a timeframe which is applied to all the gadgets on the dashboard. The available options are:

- 15 minutes
- 1 hour
- 6 hours
- 24 hours

4.2 *Filters*

This provides the user with all the configured filters. Filter names will appear in this list when you add and configure Groups - see 0 for details. The application of these filters will change the dashboard gadget's data to match the Group configuration.

Use Case:

"I want to monitor and view all traffic from/to the Finance department"

Assuming Sparrow^{IQ} is configured and running to listen to traffic to departments, including the Finance department.

1. Identify the Finance department by IP addresses

For e.g., Finance department is configured on subnet 192.168.109.0/24

2. Add a Group.
    a. Go to Settings > Groups
    b. Click on *Add Group* and add details

Name: Finance

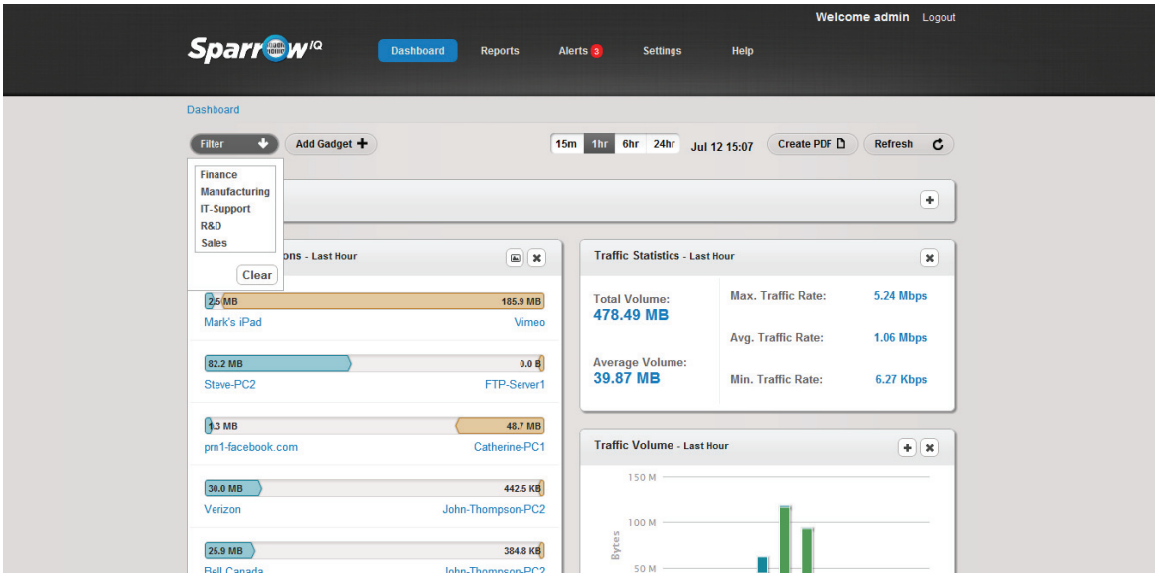
Low IP Address: 192.168.109.1

High IP Address: 192.168.109.255

Enabled: <yes>

    c. Click Save

3. Go back to the dashboard and apply the Filter.
    a. Click on Filter
    b. Select *Finance* from IP Groups list
    c. Click OK



4.3 *Add gadgets*

Sparrow[IQ] by default comes pre-populated with all available gadgets (unless it is in Trial mode). If a gadget is missing from the dashboard, this button displays the gadgets available to add to dashboard.

4.4 *Create PDF*

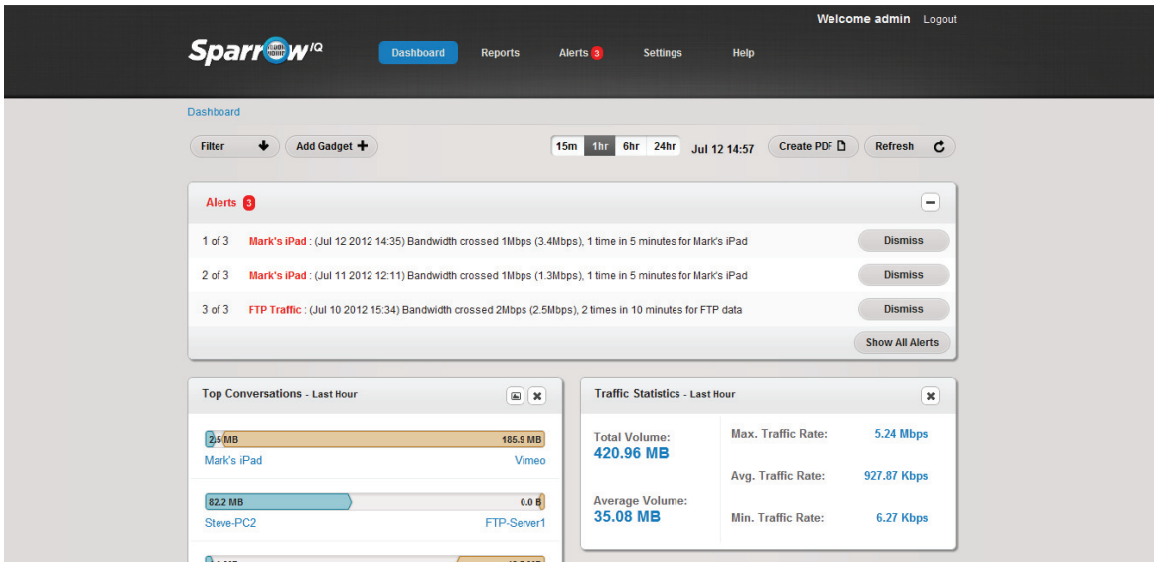
This will create a PDF file of the dashboard with all the gadgets included and download it on the viewing PC for future references.

4.5 *Refresh*

This button forces all gadgets on the dashboard to reload their data from the server.

4.6 *Alerts (gadget on Dashboard)*

This provides a count of number of generated Alerts in the system. In addition, the Alerts gadget on Dashboard displays the latest 4 alerts raised by Sparrow[IQ].

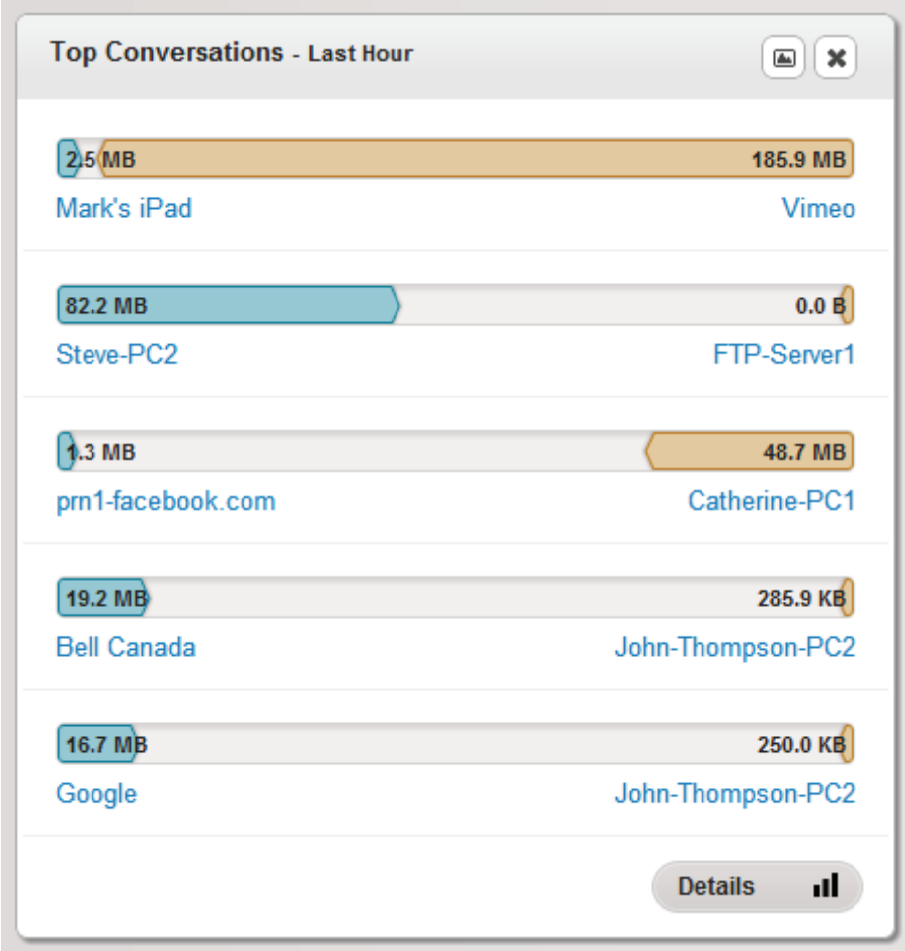


4.7 *Top Conversations*

The Top Conversations gadget displays the top five pair of IP addresses consuming the network bandwidth for the appropriate time period. The IP addresses in each pair are placed next to each other with an indication of the amount of data from each direction. This is the default view of the conversation gadget, but one may change to a pie chart if preferred by clicking on the chart icon on the top-right corner of the gadget.

Clicking on any of the conversations' IP address will take the user into the drilldown mode of the conversation pair. See Section 5 for details on drilldown mode.

Clicking on Details will run a report for the same timeframe as selected on dashboard, but will extend this to show the top 20 entries.



4.8 *Top Endpoints*

The highest traffic generators and consumers are listed in this gadget. This list of IP addresses includes both local and remote endpoints. The default view is to show only the pie chart in this gadget. However, one can get a table view of the data by clicking on the '+' sign on the top-right corner of the gadget. Clicking on Details will run a report to show the top 20 endpoints for the selected timeframe.

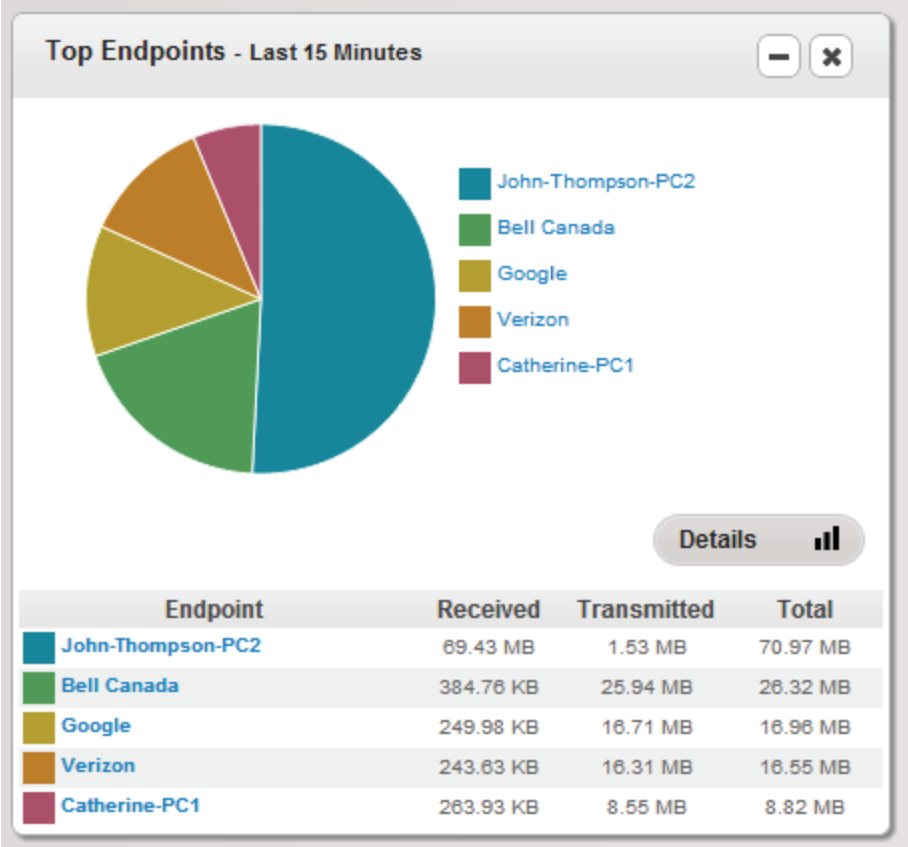
Use Case:

"I want to give a name to an unresolved IP address" or "The name resolution is incorrect and I want to change that" or "I want to shorten that name"

Sparrow^{IQ} will display names whenever they are resolved, but sometimes it is possible names aren't configured properly or display a very long name which needs to be shortened. To do this, Sparrow^{IQ} provides you to override the name used for an IP address

1. Go to Settings > Name Mapping
2. If name already exists (resolved) in the table view, click on the first column in the table and enter your preferred name.
3. If name does not exist, click *Add Entry* and a new field will be added to the table where you can specify the IP address and the preferred name.
4. After each column is edited, click on the little checkmark button next to the entry to validate and confirm.

All references in Sparrow^{IQ} will use the preferred name you just specified.



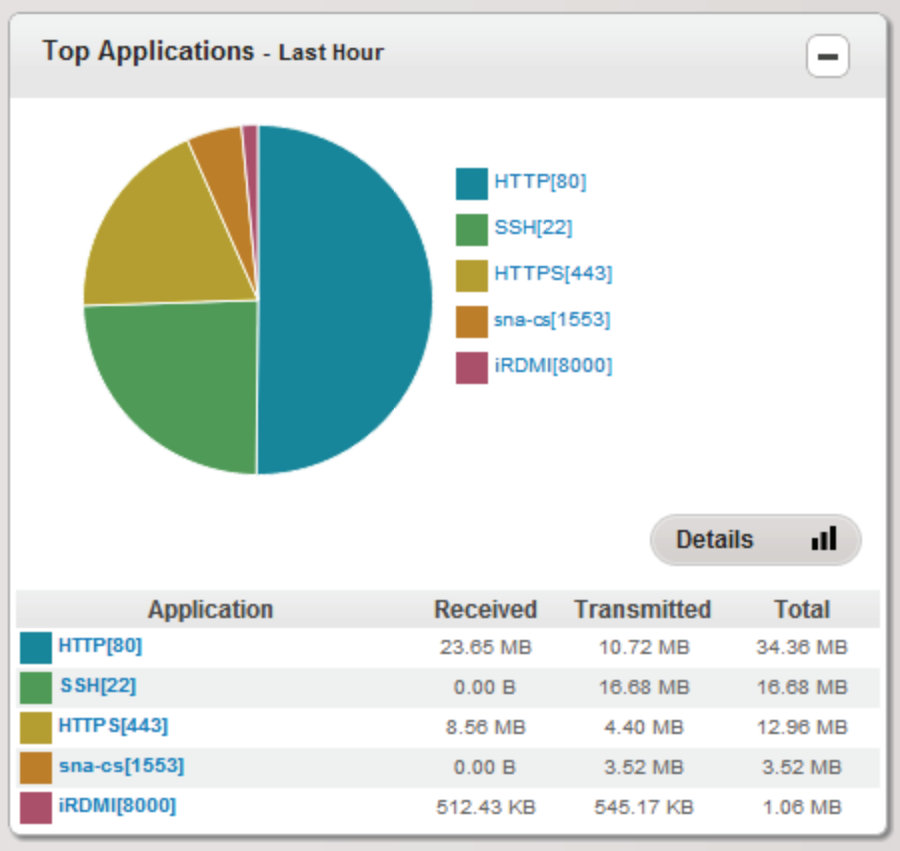
4.9 *Top Applications*

This gadget lists the top 5 applications that are generating/consuming traffic in the network. The default view hides the table view which can be accessed by clicking on the '+' sign on the top-right corner of the gadget.

Unknown Port: Sparrow[IQ] maps traffic source or destination port numbers up to port # 50,000. However, some applications use high port numbers which are not defined or reserved with the IANA port number list. Sparrow[IQ], in this case, identifies this traffic as *Unknown.*

Port 0: Any traffic without TCP or UDP as the transport layer protocol is marked as Port # 0.

In order to add a new port number please refer to 8.5.

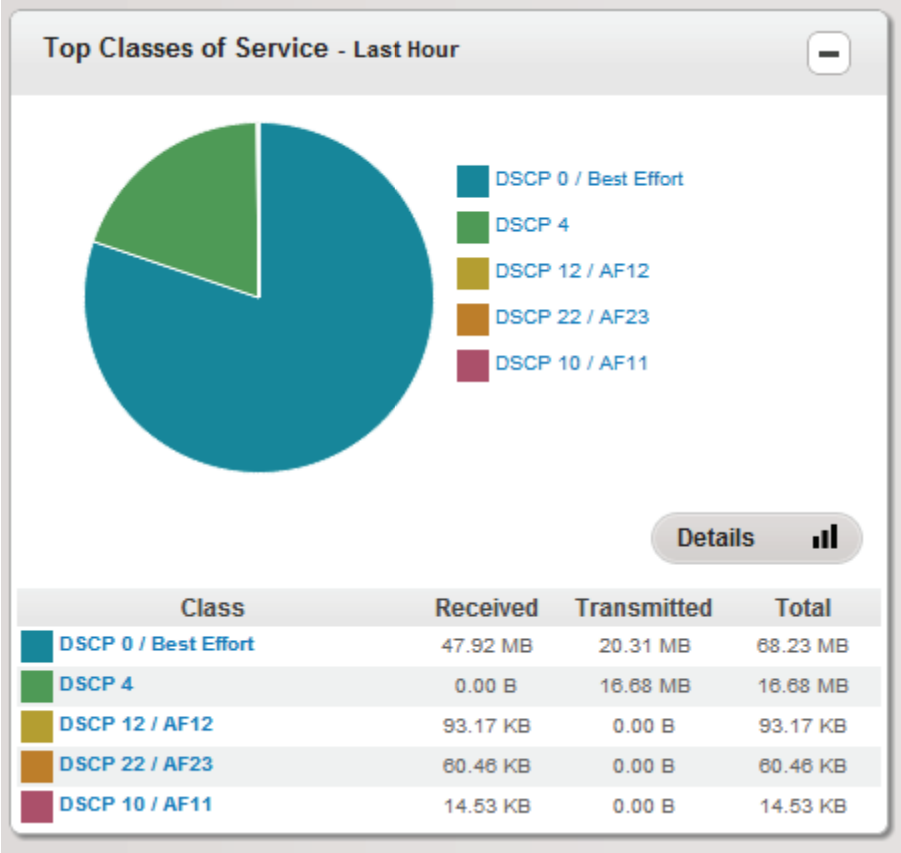


Application	Received	Transmitted	Total
HTTP[80]	23.65 MB	10.72 MB	34.36 MB
SSH[22]	0.00 B	16.68 MB	16.68 MB
HTTPS[443]	8.56 MB	4.40 MB	12.96 MB
sna-cs[1553]	0.00 B	3.52 MB	3.52 MB
iRDMI[8000]	512.43 KB	545.17 KB	1.06 MB

4.10 *Top Classes of Service*

This gadget lists the top 5 classes of service that are generating/consuming traffic in the network. The default view hides the table view which can be accessed by clicking on the '+' sign on the top-right corner of the gadget.

In order to add new classes of service please refer to 8.6.



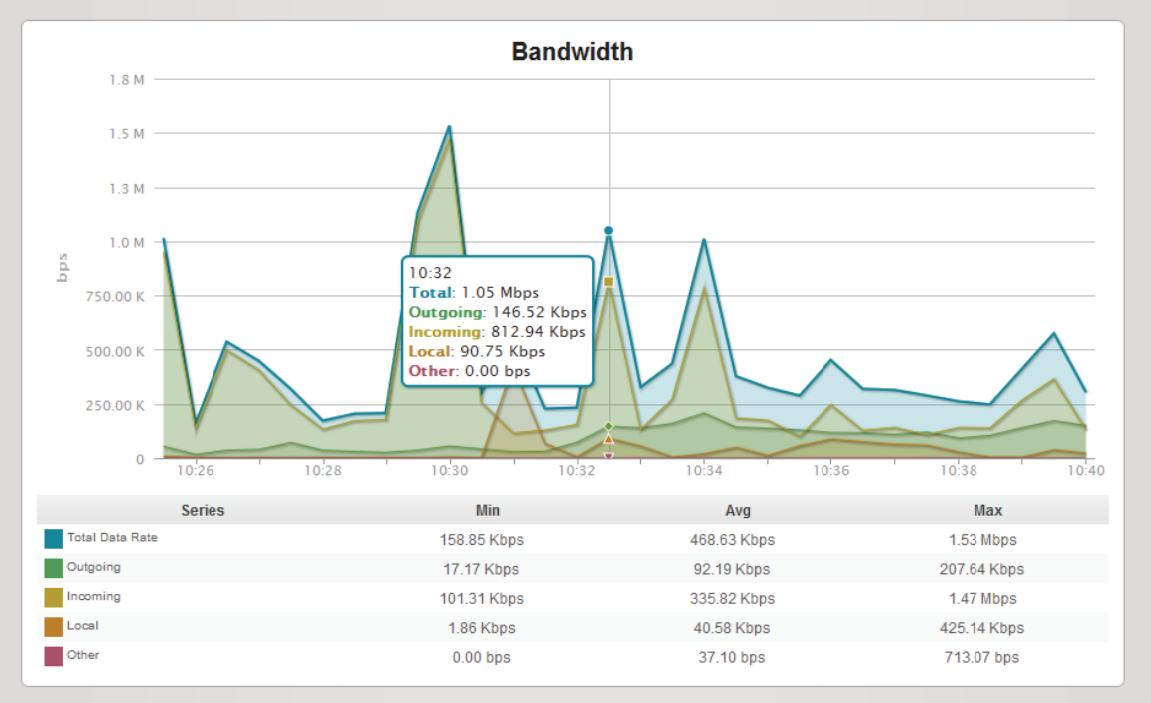
4.11 *Bandwidth Rate*

The bandwidth rate gadget displays the measured overall bandwidth as measured at the gateway (or wherever Sparrow^{IQ} is deployed).

The default view displays only the overall bandwidth trend, but more series can be enabled by selecting *Gateway Monitoring* under Settings > Internal Addresses. You can also specify internal gateways and enable display of local traffic. This will result in multiple series of line graphs on the dashboard.

Clicking on the '+' on the top-right corner of the gadget will display the Total Transferred data rates. If Gateway Monitoring and local traffic options are enabled, Sparrow^{IQ} will display a view of the breakdown of incoming, outgoing, local and other traffic. Incoming and outgoing refer to the traffic going into and out of the configured subnet(s). Local refers to traffic moving around within the subnet itself.

Note that the bandwidth rate gadget has a delay of up to 3 minutes.



Series	Min	Avg	Max
Total Data Rate	158.85 Kbps	468.63 Kbps	1.53 Mbps
Outgoing	17.17 Kbps	92.19 Kbps	207.64 Kbps
Incoming	101.31 Kbps	335.82 Kbps	1.47 Mbps
Local	1.86 Kbps	40.58 Kbps	425.14 Kbps
Other	0.00 bps	37.10 bps	713.07 bps

Use Case:

"Total Bandwidth is informative, but I need more and a breakdown of bandwidth direction"

With Sparrow[IQ], you can enable internal traffic monitoring and this will provide you with a breakdown to internal, incoming and outgoing traffic statistics.

1. Go to Settings > Internal Addresses
2. Select Gateway Monitoring
3. Select Show Local Traffic
4. Configure to add local subnet configuration.

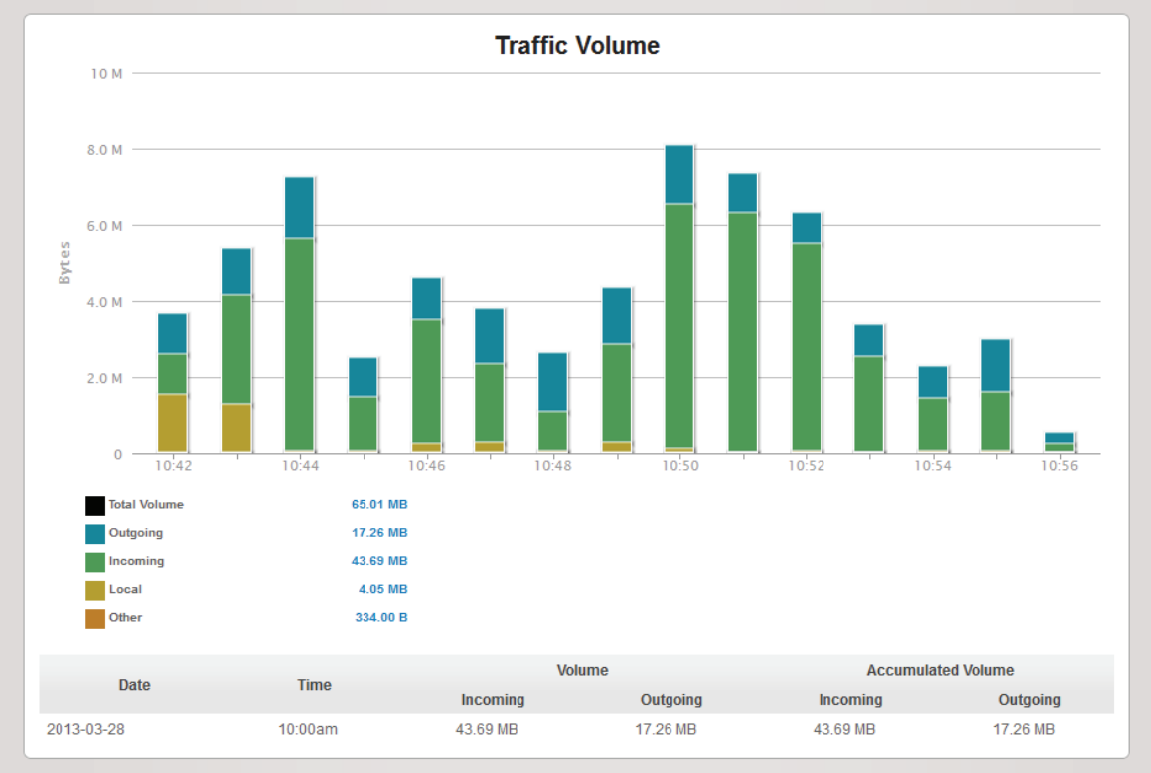
For e.g., if local subnet is 192.168.1.0 and subnet mask is 255.255.255.0, add the line to Subnet Mask # 1: *192.168.1.0/24*

5. Click *Save*

The bandwidth and traffic volume gadgets on the dashboard will now contain multiple graph components displaying Incoming, Outgoing, Local and Other traffic.

4.12 *Traffic Volume*

The Traffic Volume gadget displays the volume of traffic in the network. If Gateway Monitoring has been enabled and configured as explained in the previous section, the traffic volume is broken down to display the different sections of incoming, outgoing, local and other traffic. Clicking on the '+' on the top-right corner of the gadget will display the Total Transferred data volumes.



Date	Time	Volume		Accumulated Volume	
		Incoming	Outgoing	Incoming	Outgoing
2013-03-28	10:00am	43.69 MB	17.26 MB	43.69 MB	17.26 MB

4.13 *Traffic Statistics*

The traffic statistics gadget summarizes the Total and Average Volume in addition to the Minimum, Average and Maximum bandwidth rates for the specified time period.

5. Drilldown

Sparrow[IQ] makes drilldown simple and intuitive. Drilldown is a mode where the user can view all data associated with one reference point.

For e.g., if the user is interested in viewing all information related to UserA, clicking on UserA on the dashboard will take the user to the drilldown mode and show all data related to UserA. In drilldown mode for an Endpoint/User, the user would see:

- Details on the user such as aliases and associated groups (if configured)
- Total bandwidth sent and received by that user
- Bandwidth consumed by the user as a percentage of total network traffic
- Bandwidth rate information in bits per second
- Bandwidth rate information in packets per second
- Traffic volume information
- Top applications used by the user
- Top conversations carried out by the user

As on the dashboard, this can be customized to view the data for various timeframes such as 15m, 1hr, 6hrs and 24hrs.

Note that the drilldowns are always one level deep. If the user drills down to an Endpoint, say UserB and then clicks on an Application, say HTTP, this will take the user to the drilldown of the application HTTP for the whole network and is not a drilldown of HTTP traffic specific to UserB. This is the same if a user drills down HTTP from Top Application gadget on the dashboard.

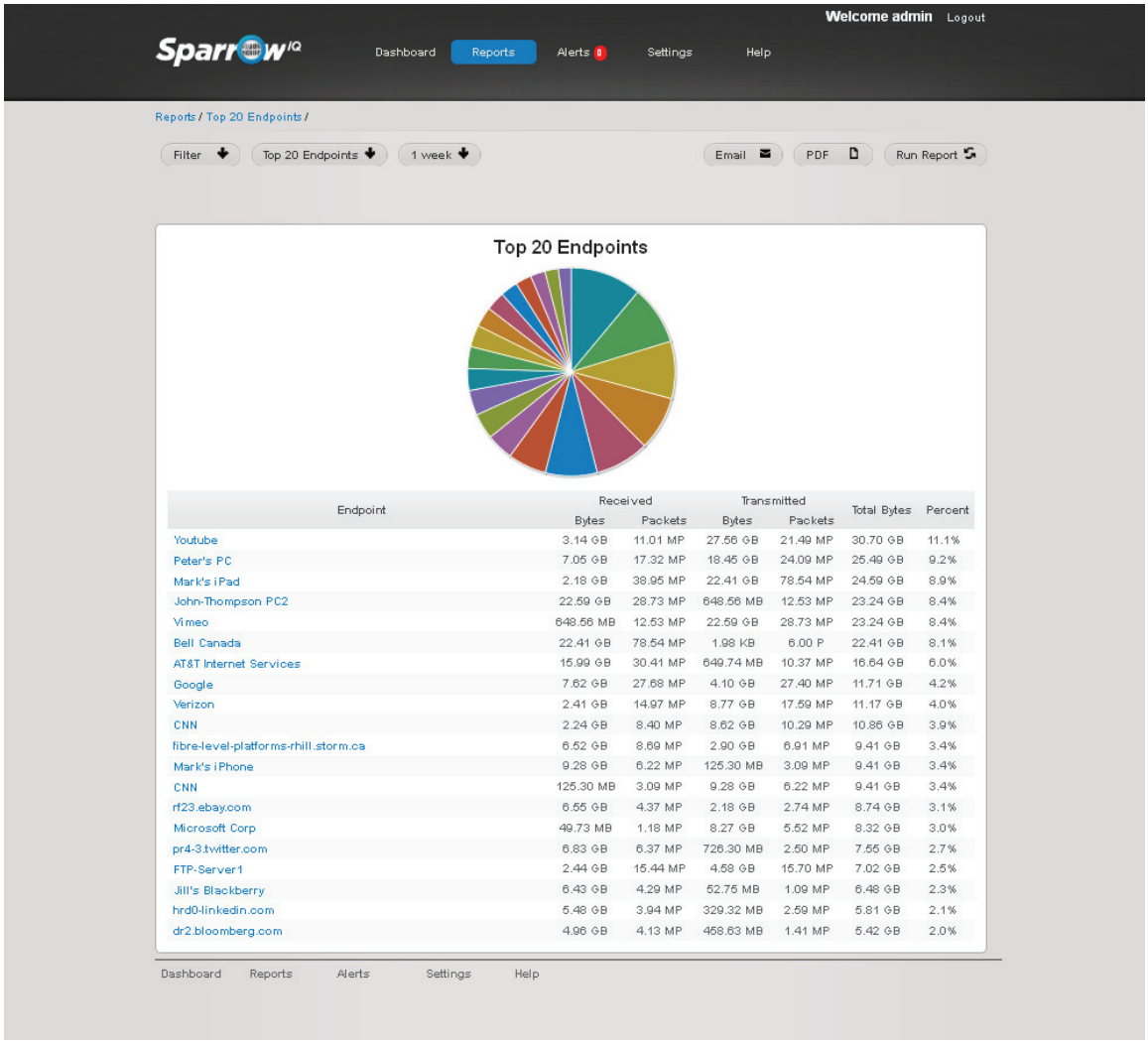

Welcome admin Logout
SparrowIQ
Dashboard
Reports
Alerts 4
Settings
Help
Dashboard / Endpoint: 192.168.1.53
Filter
15m 1hr 6hr 24hr Jul 13 09:30
Create PDF
Refresh
Details - Last Hour
Hostname: Mark's iPad
IP Address: 192.168.1.53
Group: IT-Support
Total Transmitted Traffic: 36.99 MB
Total Received Traffic: 48.10 MB
Percentage of All Traffic: 63.62%
Traffic Volume - Last Hour
30 M
20 M
10 M
0
Bytes
08:30 08:40 08:50 09:00 09:10 09:20
Details
Series Min Avg Max Total
Total Volume 6.55 KB 7.09 MB 24.00 MB 85.09 MB
Outgoing 1.62 KB 3.08 MB 12.53 MB 36.99 MB
Incoming 4.86 KB 4.01 MB 20.69 MB 48.10 MB
Local 0.00 B 0.00 B 0.00 B 0.00 B
Other 0.00 B 0.00 B 0.00 B 0.00 B
Bandwidth - Last Hour
750.00
500.00
250.00
0
pps
08:30 08:40 08:50 09:00 09:10 09:20
Series Min Rate Avg Rate Max Rate
Total Data Rate 0.00 pps 31.97 pps 604.37 pps
Outgoing 0.00 pps 15.45 pps 204.67 pps
Incoming 0.00 pps 16.52 pps 400.30 pps
Local 0.00 pps 0.00 pps 0.00 pps
Other 0.00 pps 0.00 pps 0.00 pps
Top Applications - Last Hour
HTTP[80]
SSH[22]
HTTPS[443]
sna-cs[1553]
iRDMI[8000]
Details
Application Received Transmitted Total
HTTP[80] 23.65 MB 10.72 MB 34.36 MB
SSH[22] 0.00 B 16.68 MB 16.68 MB
HTTPS[443] 8.56 MB 4.40 MB 12.96 MB
sna-cs[1553] 0.00 B 3.52 MB 3.52 MB
iRDMI[8000] 512.43 KB 545.17 KB 1.06 MB
Bandwidth - Last Hour
8 M
5 M
3 M
0
bps
08:30 08:40 08:50 09:00 09:10 09:20
Details
Series Min Rate Avg Rate Max Rate
Total Data Rate 3.73 bps 187.53 Kbps 4.79 Mbps
Outgoing 0.80 bps 81.52 Kbps 2.23 Mbps
Incoming 1.33 bps 106.01 Kbps 4.72 Mbps
Local 0.00 bps 0.00 bps 0.00 bps
Other 0.00 bps 0.00 bps 0.00 bps
Top Conversations - Last Hour
268.9 KB 19.9 MB
Mark's iPad Vimeo
16.7 MB 318.6 KB
prn1-facebook.com Mark's iPad
3.7 MB 12.2 MB
Mark's iPad Mail Server
806.4 KB 8.5 MB
Bell Canada Mark's iPad
571.5 KB 2.7 MB
Mark's iPad SparrowIQ
Details
Top Classes of Service - Last Hour
DSCP 0 / Best Effort
DSCP 4
DSCP 12 / AF12
DSCP 22 / AF23
DSCP 10 / AF11
Details
Class Received Transmitted Total
DSCP 0 / Best Effort 47.92 MB 20.31 MB 68.23 MB
DSCP 4 0.00 B 16.68 MB 16.68 MB
DSCP 12 / AF12 93.17 KB 0.00 B 93.17 KB
DSCP 22 / AF23 60.46 KB 0.00 B 60.46 KB
DSCP 10 / AF11 14.53 KB 0.00 B 14.53 KB
Dashboard Reports Alerts Settings Help

6. Reports

Reports give the user a more in-depth view of the network by reporting on various metrics, including long term timeframes. The following are available:

1. Executive Summary
2. Traffic Usage Summary
3. Bandwidth
4. Traffic Volume
5. Top 20 Applications
6. Top 20 Conversations
7. Top 20 Classes of Service
8. Top 20 Endpoints
9. Top Application Detailed
10. Top Conversation Detailed
11. Top Endpoint Detailed

Each of the above reports can also be generated for pre-defined IP-Groups.



Reports are available in the following timeframes.

- 15 minutes
- 1 hour
- 6 hours
- 24 hours
- 1 week
- 1 month
- 2 months
- 3 months

Data older than 3 months is purged automatically.

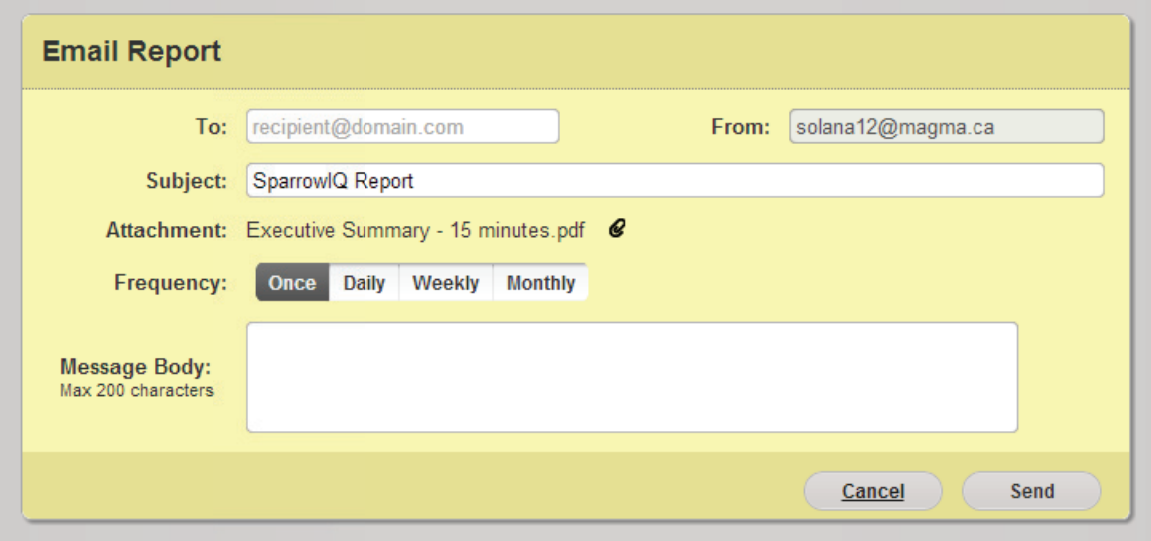
Note that some time periods may not be available based on the license type.

6.1 *Email and PDF Reports*

The "Run Report" button is used to generate reports once the type and duration have been selected. Once generated, the user may save a PDF version of the report, or choose to email a PDF version to a given address.

To save a PDF version of a report, simply click the "PDF" button. After a few moments, you will be prompted to save a PDF file to the desired location.

Reports can be either emailed immediately or scheduled to be emailed periodically until canceled. Before reports can be scheduled for email, SMTP credentials must be configured. See section 8.9 for details. To email the report, click the "Email" button, fill out the form, and click Send.



The fields of the form are:

- To – recipient's email address.
- From – email address provided during SMTP configuration.
- Subject – subject line on the generated email.
- Attachment – generated name for the attachment.
- Frequency – How often the report will be generated and emailed. Weekly and Monthly selections allow the user to select the day on which reports are sent.
- Message Body – Optional body text for the generated email with maximum of 200 characters.

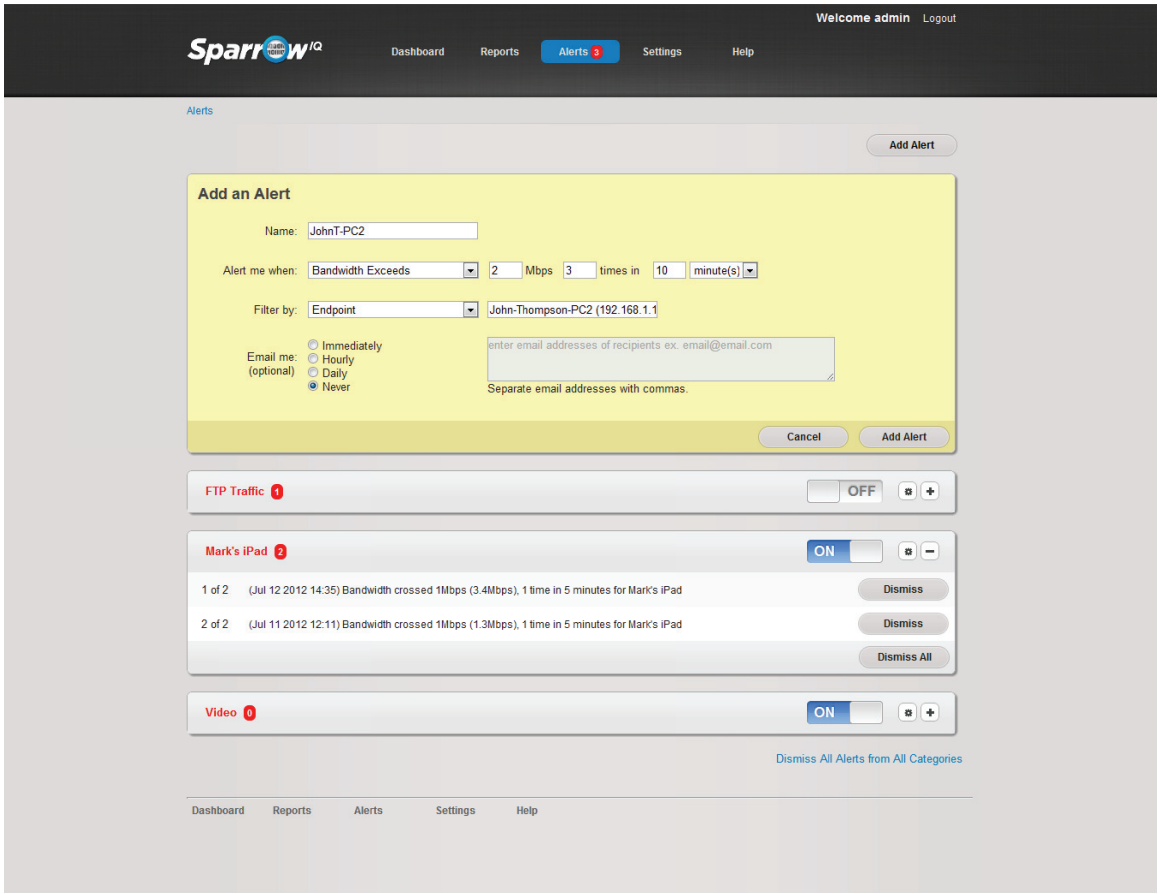
Reports will be generated and emailed at midnight on the selected day. In order to see the list of scheduled emails, and to cancel any previously scheduled reports, see section 8.11.

It is imperative that the user mentions correct email address.

7. Alerts

Alerts can be configured to be generated based on custom threshold values. The available fields are:

- Name: This specifies the name of the alert
- Alert Type: Metric used to monitor/generate the alert. Available options are – Bandwidth Exceeds in Mbps and Traffic Exceeds in MB.
- Value, Occurrence and Period: These fields specify the value, count of occurrences and the time period to use for the alert generation. The time period specified configures a trailing sliding window. For a specification of *x minutes*, the bandwidth or traffic alerting mechanism monitors and tracks the data for the trailing *x minutes* at any given point in time.
- Email: Specifies whether to email when the alert is triggered and if yes, the frequency of emails. Note that for this feature to work, the *Email Setup* fields on the *Settings* page (which configures the outgoing mail server settings) have to be configured.
- Filter Type and Value: The alerts can be specified with filters to be generated for specific Applications, IPs, IP-Groups or Classes of Service (CoS). For the selected filter, Sparrow^{IQ} provides the list of available options



Use case:

"I want to know when the SSH traffic bandwidth in my network exceeds 2 Mbps 3 times per hour and want to receive a daily summary email when that happens"

Sparrow^{IQ} allows you to setup custom alerts with ease. To setup the alert just defined above,

1. Go to *Alerts*
2. Click Add Alert
3. Enter the following details:
    a. Name: SSH*Alert*
    b. Alert me when: *Bandwidth Exceeds, 2* Mbps, *3* times, in *1* hour
    c. Filter by: Application SSH (22)
    d. Notify me: *Daily*
    e. Email me: <youremailaddress>
4. Click *Save*

Make sure that the alert is turned ON – this should be indicated by the slider for the SSH*Alert* on the Alerts page.

You may need to configure email authentication for the outgoing emails in order to receive emails. This can be achieved by specifying your mail settings in *Settings* > *Email Setup*

Use Case:

“I set my alerts with values 1 times in 5 minutes and yet I see alerts every minute. Why?”

The alerting mechanism on SparrowIQ uses a sliding window of a timeframe set in your configuration. So, in this use case, it checks if there are any new alerts in the last 5 minutes and when it finds one, it flags an alert event.

To further illustrate, if you set an alert for bandwidth threshold crossing 1Mbps 1 time in 5 minutes at 12:30pm. Assuming your bandwidth is constantly above the 1Mbps threshold, an event will be generated every minute after 12:30pm. At 12:31, it checks if there were new events in the past 5 minutes (from 12:26-12:31) and marks that as an event. Following minute, again it sees a new event taking place between 12:27 and 12:32, thus generating an alert.

8. Settings

This section lists and details the Settings available and configurable to the Sparrow[IQ] user. Multiple tabs are available under the Settings page.

8.1 *System Status*

This lists some of the system details and can act as a first step in debugging any problems you may face if Sparrow[IQ] doesn't behave as intended.

This section displays the following information:

1. Number of flows processed in last cycle
2. Sparrow[IQ] version information
3. License information - Maintenance and update expiry date
4. System information such as OS, processor, memory and interface details

This section will also list the modules present in Sparrow[IQ] and show the current state of the module.

1. Node Controller – is responsible for managing the other processes and services that exist on the machine and provides naming services for IPC modules.
2. Analyzer – this is the heart of the Sparrow[IQ], which handles most of the work and performs network data processing and analysis.
3. Web Server – provides the web interface to Sparrow[IQ]. This process handles all external connections and interactions.
4. Probe Service – this is the listening module, which parses the incoming network traffic.
5. Database Service – this module stores the network data and handles all database related services.

8.2 *Settings*

This tab includes the following settings:

1. Web Port – You may choose to use any unused port to access Sparrow[IQ]. Note that any changes to this setting will take effect after Sparrow[IQ] is restarted.
2. Web Timeout – Users are automatically logged out of Sparrow[IQ] after idling for this duration.
3. Dashboard Refresh – This is the refresh rate of gadgets on the dashboard.
4. Ignore Short Flows – Network traffic sometimes consists of large number of short flows and may impact the performance of Sparrow[IQ]. Selecting this option will ignore such short flows with negligible impact on data accuracy and analysis, while yielding better performance.
5. Long Term Report Optimization – Enabling this feature will significantly speed up 1, 2, and 3 month reports by removing data associated with small flows. The resulting reports are still more than 95% accurate. Disabling this feature will restore the data for

these reports. Any changes to optimization level may take a few minutes to activate, depending on the size of your database.

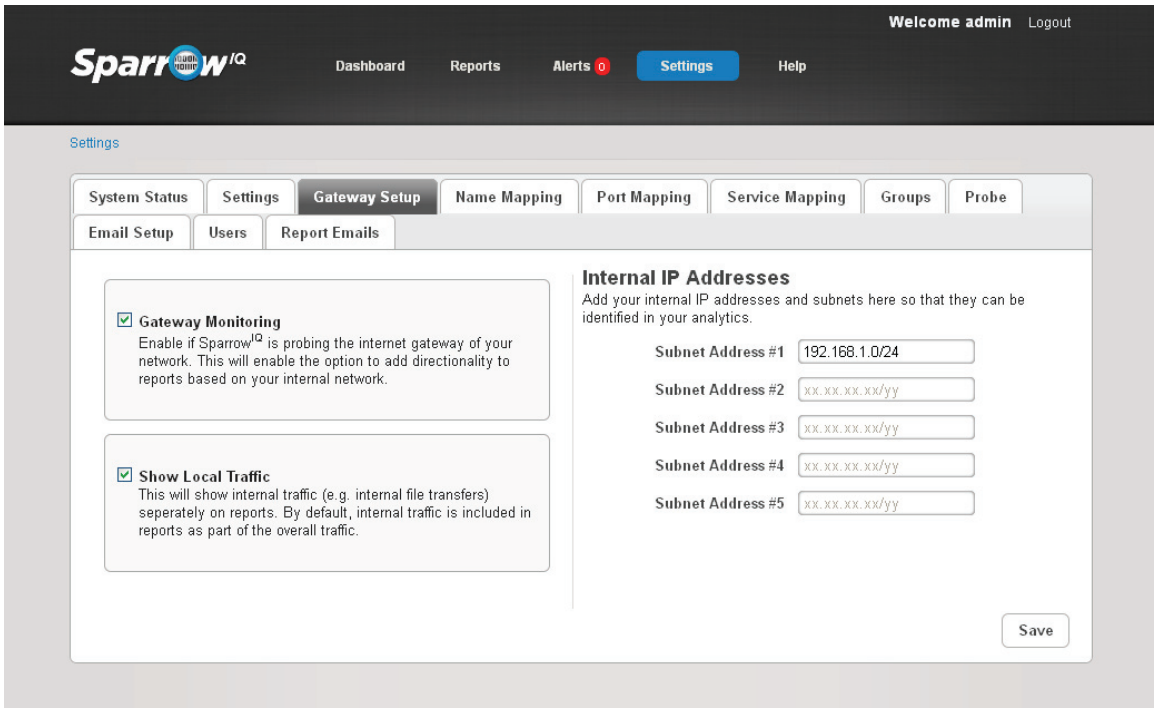
6. Delete Database – this clears out all network traffic data stored on the database.
7. Max Database size - This will set the maximum database size ranging from 80 GB to 160 GB.
8. Debug Logging - This causes additional debugging information to be logged.

8.3 *Gateway Setup*

Sparrow[IQ] can monitor and analyze traffic internal to the network (local traffic). Simply enable *Gateway Monitoring* and *Show Local Traffic*. Note that the subnet IP address and mask needs to be specified for this to work accurately.

If your local network IP addresses use 192.168.1.x with a subnet mask of /24 (255.255.255.0), you can specify subnet as 192.168.1.0/24 to monitor and analyze local traffic. This feature also enables identification of incoming and outgoing traffic.

Note that this feature of gateway setup applies only to bandwidth, packets/sec and volume graphs.



8.4 *Name Mapping*

This feature allows you to give Friendly Name to IP Addresses. Some IP addresses may be resolved, but with long names and some IP addresses may not be resolved. Discovered IP addresses, and their resolved names, cannot be edited; however Friendly Names can be configured for these addresses. For the unresolved addresses simply click on Add Entry and enter the IP address and Friendly Name before clicking *Save*.

8.5 *Port Mapping*

This feature allows you to give Friendly Names to ports. Many standard, well known, and commonly used ports have been pre-configured. To add a new Port, simply click on *Add Entry,* enter the port number and Friendly Name, then click *Save*. To edit an existing entry, click on the Friendly Name and make the change. Only the Friendly Name of pre-configured ports can be modified.

8.6 *Service Mapping*

This feature allows you to give Friendly Name to the classes of services or DSCP field of IP packets. This table comes pre-populated with common names for all valid values of the field.

8.7 *Groups*

This allows you to allocate a group of IP addresses together. For example, one subnet can be grouped together which belongs to the Finance Department of the company. Entries added here will be available as global filters across Sparrow^{IQ} and you will be able to apply the filters on dashboard, drilldown or reports page.

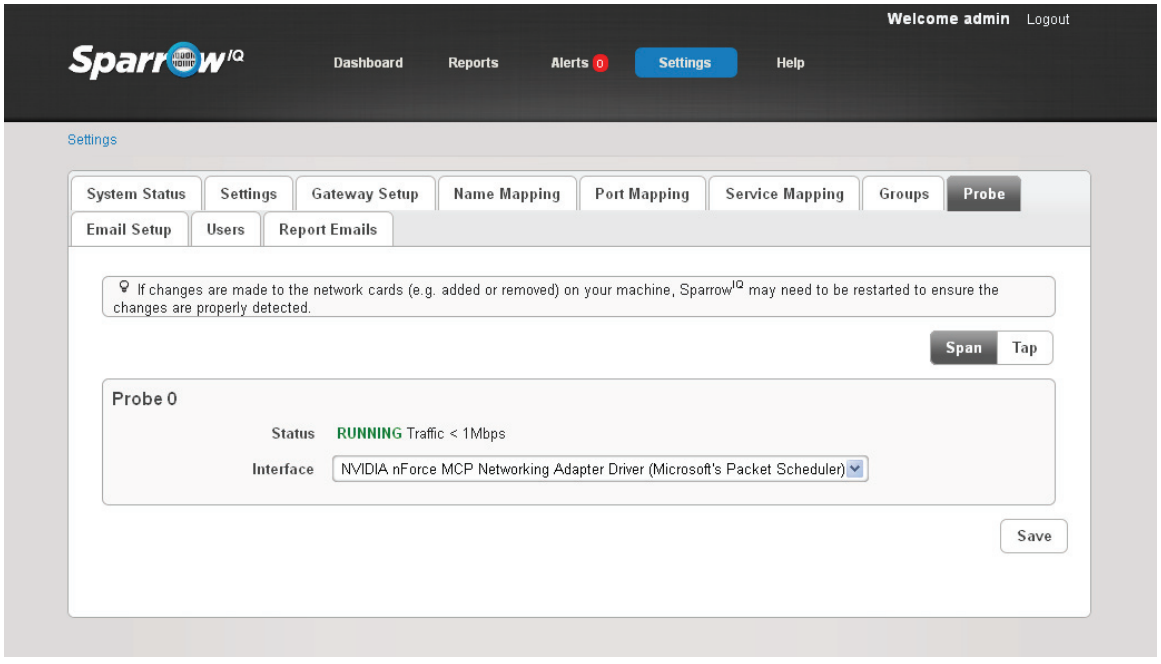
8.8 *Probe*

This feature allows the user to change the interface used for listening network traffic on the Sparrow^{IQ} machine.

This feature also allows the user to switch between the SPAN and TAP mode.

For each of the interfaces, it displays the current state of the probe module with each probe service's current traffic measurement.

Sparrow^{IQ} may need to be restarted if changes are made to the network cards.



8.9 *Email Setup*

This page contains the settings needed for outgoing emails related to Alerts. The available fields are:

- SMTP Server: Outgoing mail's IP address or name
- SMTP Server Port: Outgoing mail's server port number
- Mail account: Mail account username
- Mail password: Mail account password
- Connection Security : "None" has default port number 25, "SSL/TLS" has default port number 465, "STARTTLS" has default port number 587
- Enable HTML Emails: HTML formatted emails for Alerts

Once the configuration details are entered, you can test the settings to check if they work by clicking the *Test Settings* button. Remember to *Save* before testing the settings.

8.10 *Users*

This lists all users on the Sparrow[IQ] system. This contains information such as the username, full name and email address.

Passwords can be changed/updated by clicking on the little lock icon next to each user.

User accounts can be deleted by clicking on the 'x' icon next to the user's details.

New users can be added with a maximum of up to five.

8.10.1 Adding User Account

This facility allows the admin to add users to Sparrow[IQ]. Adding a new user requires:

- Username
- Email address
- First name (optional)
- Last name (optional)
- Password

8.11 *Report Emails*

This section provides the user with a list of all the scheduled email reports and provides a way to cancel them. Several details of the scheduling are shown, including target email address, frequency, and the day on which the report is run. To remove any scheduled report, simply click the 'x' button on the associated row.

9. Help

The Help page displays this User Guide.

10. Troubleshooting Sparrow IQ

1. I cannot run the installer and it gives a message saying that Sparrow IQ is still running
    a. Shut down Sparrow IQ by right-clicking the Sparrow IQ system tray icon and click Exit.
    b. Open up Task manager with Ctrl + Alt + Del and go to the Processes tab. Verify that sparrow_node.exe, sparrow_analyzer.exe, sparrow_web.exe, mysqld.exe and probe.exe are not running. If they are, you can end the processes by selecting the process and clicking *End Process*.

You should now be able to install Sparrow IQ.

2. I am getting an error when running the Sparrow IQ SystemIDFinder

The Sparrow IQ SystemIDFinder requires the Microsoft .Net 2.0 framework installed. This software is available for free download from Microsoft's website.

3. I get an Invalid or Missing License message
    a. Please ensure that the license entered is copied or typed as given (case sensitive)
    b. If not a trial license, each Sparrow IQ license is tied to a machine. Verify that the license entered is for the destined machine by confirming the SystemID.
    c. Verify that the license version is for the correct version of Sparrow IQ. Each new version of Sparrow IQ will require a new license. Your license key can be updated for free (by going to Sparrow IQ support page) with new versions of Sparrow IQ if your maintenance period has not expired. For more details on this, check our FAQ page on www.sparrowiq.com

4. I get an *Invalid SystemID* message after entering the license
    a. Please ensure that the license entered is copied or typed as given (case sensitive)
    b. Check that the SystemID specified during your purchase matches the installed machine's SystemID

5. I get a *Timer file broken/missing* message after entering the license

The trial license file has been corrupted. You may need to reinstall the product.

6. I get a 404 error when pointing my browser to Sparrow IQ
    a. Please ensure that Sparrow IQ is up and running. Once started, it takes a few seconds to reach a stable state after which it allows connections and logins.
    b. If accessing Sparrow IQ remotely, please ensure you have network connectivity to the Sparrow IQ PC.

c. The IP address of the Sparrow[IQ] PC needs to be followed by the port number. The default is 8000. The address to access Sparrow[IQ] is http://<IPAddress>:<Port>

d. Check with your system/network administrator to make sure that the

i. Sparrow[IQ] PC is not blocking the port number by any firewalls

ii. The network is not blocking traffic on the port.

7. I cannot log into Sparrow[IQ]

a. Check your username and password. These are case sensitive. Sparrow[IQ] ships with one default account configured

Username: admin

Password: admin

b. If you have forgotten your password, click on the *Forgot your password?* link. Note that your outgoing mail server needs to be configured before you can use this feature.

8. I don't see any data on my dashboard gadgets and reports

a. On first startup, Sparrow[IQ] may take roughly 3 minutes before the first set of data gets processed and displayed on the gadgets

b. Verify the interface selection used by Sparrow[IQ] on the PC. To do this, go to Settings > Probe and select the right mode (SPAN or Tap) and select the appropriate interface used.

c. Verify that all the processes are up and running by going to Settings > System Status. If one or more processes are not running, please restart Sparrow[IQ].

9. The gadgets on dashboard say "Could not retrieve data…" or "Loading"

a. Click Refresh and if that work, please reload the page on your browser. Note that on first start, Sparrow[IQ] takes approximately 3 minutes for the first set of data to get processed and loaded into gadgets.

b. Verify that the right mode and interface(s) is/are selected on the Settings > Probe page.

c. If you are still having trouble, log out and log back in.

10. What is causing the dashboard to refresh so slow?

a. The more gadgets you have, the longer it takes to calculate the data required.

b. Certain browsers use up a lot more memory than others. Check the Windows Task Manager to track your browser memory footprint. It may help to restart your browser.

11. Why do I automatically get logged out from the session?

a. After 30 minutes of inactivity, your session will be closed by Sparrow[IQ]. This timer can be configured on the Settings > Settings page.

b. If you login from a second machine in the network, you will be logged out from the first machine.

12. I am not getting any email Alerts, but I see the alerts getting generated in Sparrow[IQ].

a. Check the Settings > Email Setup page to make sure your email settings are correct. Once setup, use the *Test Settings* feature to confirm that the settings are working. If the settings are setup correctly, this page will confirm so, else you will see an error message and some details on why it failed. Remember to *Save* the configuration before testing.

b. Some mail servers require TLS. Please check with your administrator or mail provider to confirm.

c. Check if the email address specified in the Alert is correct. Also, check the frequency selected as emails can be configured to go either immediately, hourly, daily or never.

13. I am not seeing any difference when I apply a filter

The filters are applied on all IP addresses displayed in the gadgets and will be applied to any traffic that falls within the range that has been configured. For the Top Conversation gadget, this can mean either end of the conversation.

14. Why am I seeing License Alarms on the top of the page?

Your Sparrow[IQ] license has a bandwidth regulation. When the thresholds are crossed, the License Warning and License Exceeded messages are generated.

15. Why are there drops in the bandwidth gadget?

a. The Sparrow[IQ] PC may have some power saving settings which turn off the hard drive. Please check your Windows settings to disable this as this may result in missed data packets in your network monitoring solution.

b. A license limit alarm could have occurred where your network bandwidth has exceeded the limits of your Sparrow[IQ] license.

16. I got an error indicating that one of the Sparrow[IQ] processes died. How do I proceed?

a. Restart Sparrow[IQ]

b. If problem persists, contact us with as many details as possible at support@sparrowiq.com

17. I was instructed to export log files for debugging. How do I do that?

a. Go to Settings > System Status page and click on the *Export Log Files* button. This will download an archived file to your default download directory.

b. If the product is not functioning, you can retrieve the log files by copying the SparrowIQ\logs directory.

18. I want to erase all collected data from the Sparrow[IQ] database. How do I do that?

Go to Settings > Settings page and click on *Delete Database*.

Appendix A – Port Mirroring Switches and Taps

This section describes some of the details about hardware that can be used for Sparrow[IQ] deployment. Sparrow[IQ] can be deployed using either a switch which support port mirroring feature or using a Network Tap. Both these devices achieve the goal of sending data traffic, by either channeling through or copying, to a port of interest. For details on how to connect your Sparrow[IQ] PC to your switch or tap, see Section 3

Majority of even inexpensive switches now come with port mirroring functionality support. This feature may be termed differently by different manufacturers, but the most commonly terms used are: Port Mirroring, SPAN – Switched Port Analyzer (term most commonly used by Cisco Systems) or RAP – Roving Analysis Port (term most commonly used by 3Com). Port mirroring feature in switches can be found in most of the Cisco Catalyst switches, DLink, Dell PowerConnect, HP, Linksys, Netgear switches etc.

A network tap channels the network traffic data by providing drop line(s), which can be fed into the Sparrow[IQ] PC. Network taps can vary in prices depending on the quality and reliability of the device. Network taps can vary depending on the type of functionality provided. Some taps provide three ports where data from both IN and OUT are copied to the same port – called Aggregator Network Taps. These taps generally tend to be pricier of the taps. Sparrow[IQ] has been tested successfully on both regular and aggregator network taps from Barracuda, VSS Systems, NetOptics etc.