Sparrow^{IQ} User Guide

Release 1.3.2

www.sparrowiq.com

Table of Contents

Table of Figures

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*

- Flow Analysis dashboard: Customized dashboard provides network usage statistics and easy to follow trends
- Network traffic usage via various data points such as:
    - Top Conversations
    - Top Applications
    - Top Users/Endpoints
    - Top Classes of Service
    - Top Countries
    - Top Domains
    - Bandwidth Usage by Rate
    - Traffic Volume
    - Overall traffic summary/statistics
- Single-click drilldown capabilities
- Flow-based long term reports
- Flexible dashboard and report filtering
- Custom alert setup for bandwidth and traffic volume
- Track department-wide 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 on the same network to access Sparrow[IQ]

1.2.1 Hardware Requirements for the Sparrow[IQ] PC

Sparrow[IQ] was designed to be able to monitor small to medium sized enterprise networks on modest hardware. Processor speed and RAM required increases with the size of the observed network.

	Minimum System Requirements (for trial installations)	Recommended System Requirements (for production environments)
Processor	Dual Core 2GHz+	Quad Core 2Ghz+
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	

Table 1 : System Requirements

1.2.2 Software Requirements for Sparrow[IQ] PC

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

- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows Server 2008

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 Vista, 7,8, Server 2008
VMWare Player	Windows Vista,7, 8, Server 2008

Table 2: Supports Virtual Environments

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 minimum versions of these popular web browsers have been tested and are supported:

- Firefox 13
- Chrome 20
- Safari 5
- Internet Explorer 9, 10, 11

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 a future 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.
- Wireless interfaces: 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.
- In some instances, another application running mySQL may conflict with mySQL running on Sparrow[IQ]
- Please ensure that the email address a report is sent to be correct. Sparrow[IQ] does not currently advise if the report emailed has not been sent to the intended destination.

- Virtual box is not a currently supported virtual environment. Virtual box does not generate a SystemId that will generate a valid full license.
- The Internet Explorer browser requires the user to input "http://" before the ip address. If entering http://localhost:8000, some internet explorers may return an error message. If this happens, internet explorer requires the settings to be restored to default, or the user can enter the direct ip address, rather than local host. Example: Enter http://192.168.xxx.xxx:8000 instead of http://localhost:8000.

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 Installation*

It is recommended that Sparrow^{IQ} be installed on a dedicated PC with a configuration that meets the 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:

- A Trial license - you only need to specify name and email address.
- 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

Table 3: Division of Licensing

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 Sparrow^{IQ} Free License

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

2.3.3 Sparrow^{IQ} Full License

Sparrow^{IQ} is available for different levels of bandwidth support. All Sparrow^{IQ} purchases are perpetual licenses.

Note that Sparrow^{IQ} 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:

- Sparrow^{IQ} 7 – a perpetual license supporting up to 7 Mbps.
- Sparrow^{IQ} 15 - a perpetual license supporting up to 15 Mbps.
- Sparrow^{IQ} 30 - a perpetual license supporting up to 30 Mbps.

Threshold Allowance

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

Once the sustained bandwidth stays above the real max threshold value, data will be dropped by Sparrow^{IQ}.

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 Sparrow[IQ] 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 Sparrow[IQ] is already installed as a trial, launch the Configuration (right-click on Sparrow[IQ] icon in the system tray and select Sparrow[IQ] Configuration). The dialog box provided will display the installed PC's SystemID.
- Download and install Sparrow[IQ] 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 *Uninstallation*

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 switch capable of port mirroring or a network tap. If only one interface is present, Tap mode will be disabled. To rediscover interfaces, restart Sparrow[IQ].

3.1 *Deployment using SPAN switch*

In this deployment scenario, the Sparrow[IQ] workstation is connected directly to a switch or router that supports port mirroring. Many devices, even inexpensive switches, support this feature in some way, though it may be known as Port Mirroring, SPAN (used mostly by Cisco equipment), or RAP (used mostly by 3Com equipment). Many popular vendors support this, including Cisco, DLink, Dell, HP, Linksys, and Netgear.

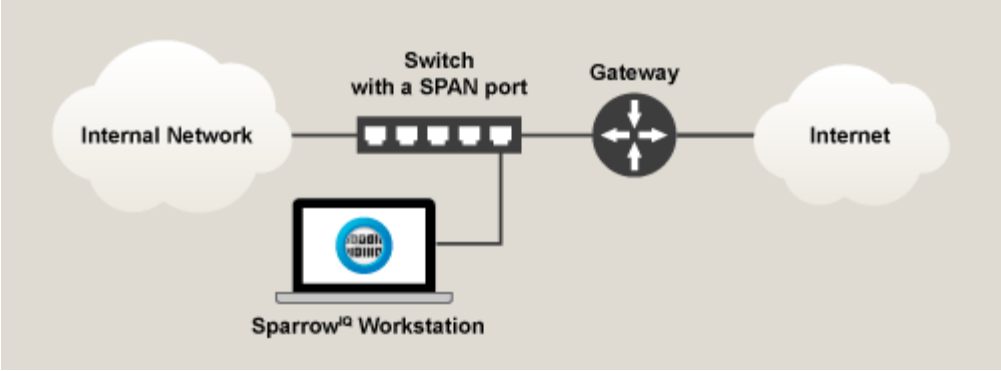


Figure 1: Deployment on SPAN Switch

3.2 *Deployment using Network Tap*

A network tap channels network traffic by providing drop lines which can be connected to the Sparrow[IQ] workstation. Regular taps provide the IN and OUT directions separately; both must be connected to the Sparrow[IQ] workstation. Aggregator taps copy both directions of traffic onto the same port. Several taps, of both types, from Barracuda, VSS Systems, and NetOptics have been tested successfully.

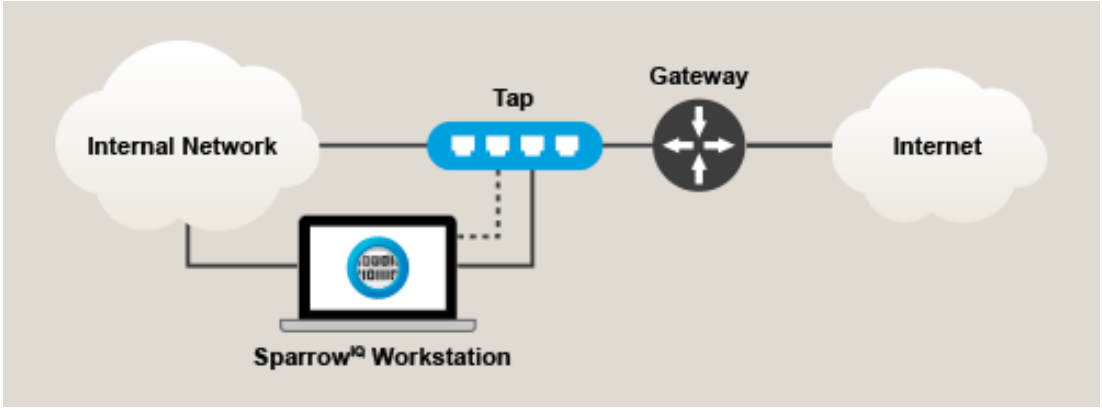


Figure 2: Deployment on Network Tap

3.3 *Launch & Access*

To launch Sparrow[IQ] select SparrowIQ > SparrowIQ Analyzer from the Windows start menu. On the first startup, Sparrow[IQ] will prompt you for a license key. Once the license is entered and validated the prompt 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.

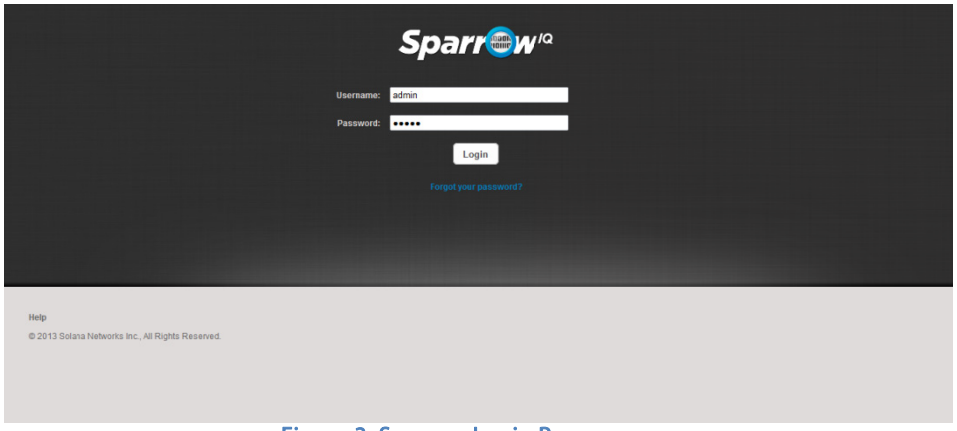


Figure 3: Sparrow Login Page

For example, if Sparrow[IQ] has an IP address of 192.168.1.100, enter "http://192.168.1.100:8000/" into the address bar of your browser. Alternatively, the address "http://localhost:8000/" will work if connecting to Sparrow[IQ] from the same computer on which it is installed.

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.

A forgotten password can be reset by clicking the "Forgot your password?" link and entering the email address previously registered 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*
7) Username: *admin*
8) Password: *admin*
9) Go to the *Settings* > *Probe* page and select the appropriate interface(s) for your setup. Select Span or Tap mode based on your port configuration.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. Dashboard

The dashboard presents analysis of recent network activity. Summary data is presented through a set of *gadgets* that provide details on different characteristics of network traffic. Also provided are tools to control the reported data, including dynamic filters, gadget selection, and duration selection.

Each of the gadgets shows a recent summary of network activity. Several gadgets show the "top" or most frequently seen attributes, such as endpoint or application. Note that only the top 5 of each attribute are presented and represented in the associated pie chart. Wedges of these pie charts compare the top 5 items against each other, not all observed traffic. Percentages of these items against up to 20 top items of observed traffic can be found by clicking the "Details" button of these gadgets.

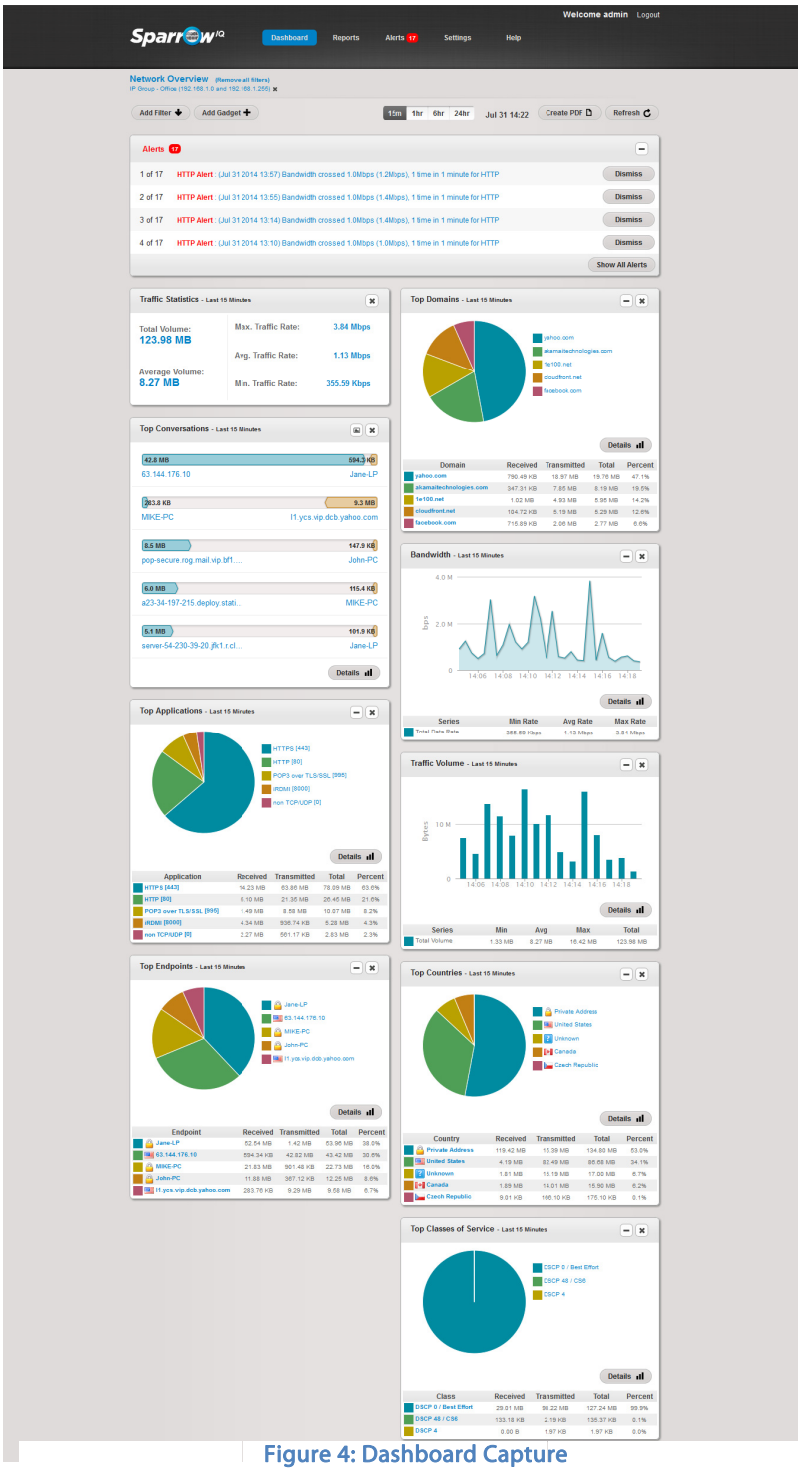


Figure 4: Dashboard Capture

4.1 *Duration*

The duration selector allows one to select the timeframe that is applied to all gadgets on the dashboard. The available options are:

- Previous 15 minutes
- Previous hour
- Previous 6 hours
- Previous 24 hours
- Custom time interval

Clicking any of these options will cause the dashboard to refresh itself using the selected duration.

4.2 *Filters*

This feature allows the user to focus the results of the dashboard gadgets by selecting certain criteria on which to run analysis. Seven different filters can be applied simultaneously. One value of each filter may be specified. The different types of filters include:

- *Endpoint* – Either an IPv4 address or a host address that has been added to the name mapping table can be specified. Auto-completion allows the user to select any entry in the name mapping table by entering part of the name or address.
- *IP Group* – An IP group is a range of IPv4 addresses that are specified by creating a group with the *Groups* interface on the *Settings* page. Once created, these groups can be selected as filters.

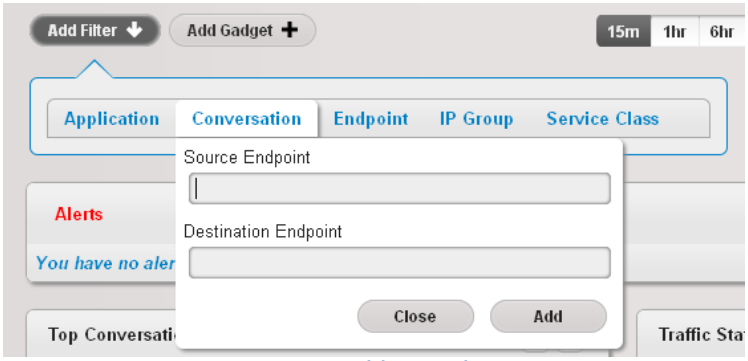


Figure 5: Adding a Filter

- *Application* – Any application found in the port mapping table, or any valid port number, can be selected as an application filter. Note that auto-completion allows the user to select applications from a list of matches.
- *Conversation* – A conversation filter selects all network traffic that is transferred between a pair of endpoints. Auto-completion functions for each endpoint in a conversation in the same way as a filter for a specific endpoint.
- *Service Class* – A service class filter selects data based on its class of service, as defined in the header of all IPv4 packets. Auto-completion allows the user to select from any service class defined in the service mapping table.
- Country-A country filter selects all network traffic transferred from or to the selected country. Auto-completion allows the user to select any country by entering part of the country name.
- Domain-A domain filter selects all network traffic based on its domain name. Auto-completion allows the user to select a domain by entering part of the domain name.

Use Case: "We have greatly increased it use of virtual desktop infrastructure (VDI) and I need to monitor its recent use."

To monitor the recent use of a particular application on the network, visit the dashboard, enable all desired gadgets, and follow these steps:

1) Click the "Add Filter" button.
2) Click the "Application" label from the list that appears.
3) In the form that appears, enter "3389", which is the port number used by common VDI protocols.
4) Click the "Add" button below the form. This creates the filter for the desired port and refreshes all of the gadgets on the dashboard.

Use Case: "I want to monitor and view all traffic from / to the Finance department."

Assuming that the finance department utilizes a block of IPv4 addresses, a group to represent this department can be created by following these steps:

1) Click on the "Groups" tab on the "Settings" page.
2) Click the "Add Group" button and enter the name and IP range of the target group. For example, if the Finance department is on subnet 192.168.109.0/24, enter "192.168.109.1" for the low address and "192.168.109.255" for the high address.
3) Click the "Save" button. The form will disappear and a new entry should appear in the groups table.

Once a group has been created, it can be applied to a dashboard as a filter. To do so, follow these steps:

1) Click on "Add Filter" button on the "Dashboard" page.
2) Click on the "IP Group" item from the list that appears.
3) Enter the group name, such as "Finance", or one of the ends of the range, and select the group from the list that appears. Auto-completion will automatically search the groups table for entries that contain the entered value.

4.3 *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.

4.4 *Refresh*

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

4.5 *Alerts Summary*

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].

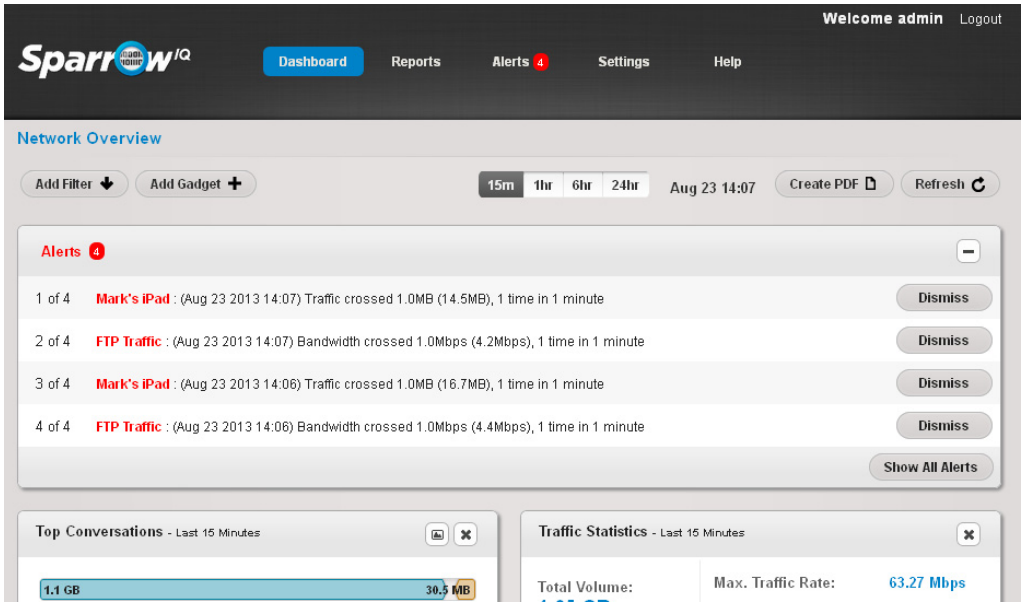


Figure 6: Generated Alerts

4.6 *Gadgets*

The dashboard represents network summary data using a collection of gadgets. Gadgets can be added to the dashboard via the "Add Gadget" user interface found by clicking the button of the same name. Initially, all gadgets are enabled and available, unless using the trial version of Sparrow[IQ]. Those that exist on the dashboard can be relocated by clicking the header and dragging into a new position. They can also be removed via the "Add Gadget" interface or by clicking the 'x' on the gadget's header. Sub-sections describe each available gadget.

4.6.1 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.

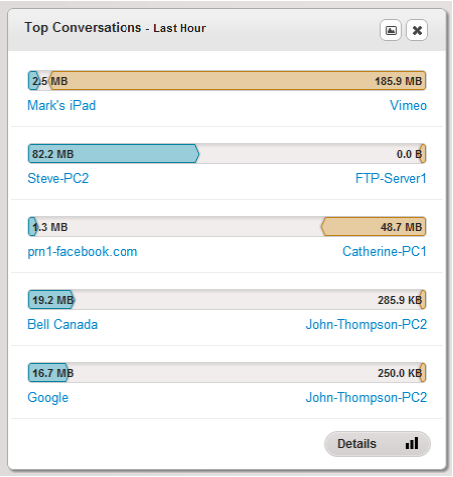


Figure 7: Top Conversations

4.6.2 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.

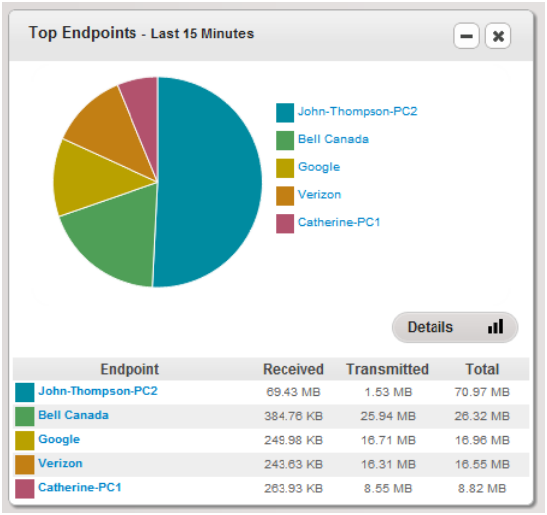


Figure 8: Top Endpoints

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.

4.6.3 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 9.5.

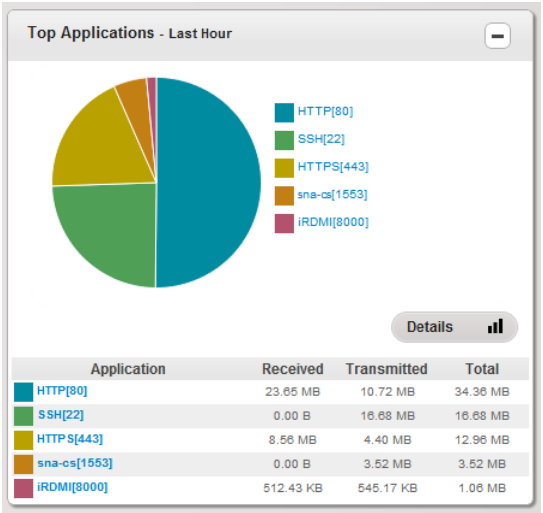


Figure 9: Top Applications

4.6.4 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 9.6.

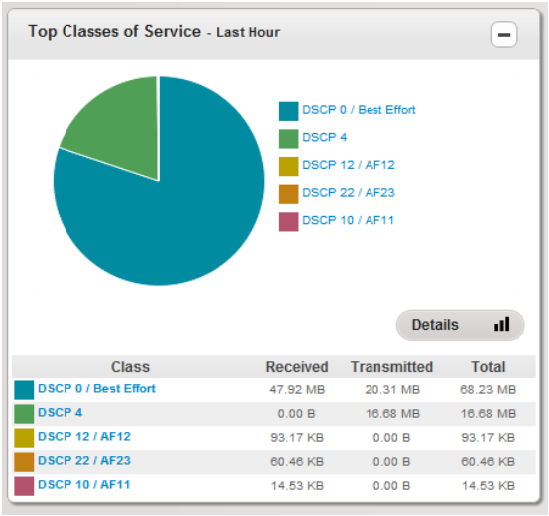


Figure 10: Top Classes of Service

4.6.5 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.

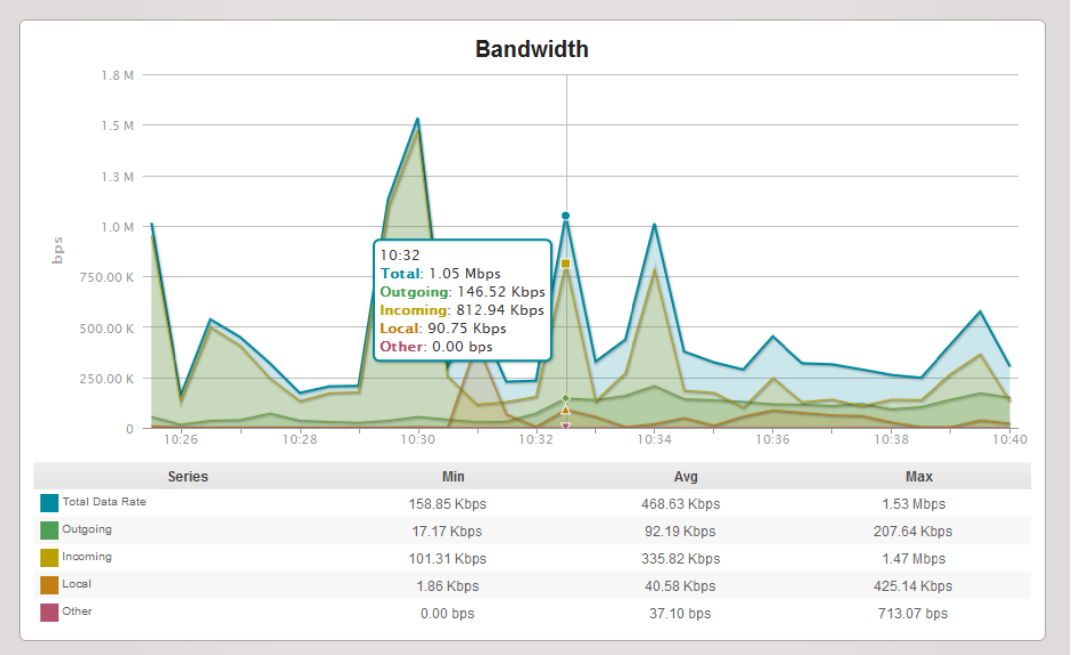


Figure 11: Bandwidth Graph

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 that will provide you with a breakdown of all traffic entering and leaving your network.

1) Select the "Gateway Setup" tab on the "Settings" page.
2) Enable "Gateway Monitoring" by clicking on the associated checkbox.
3) Enable "Show Local Traffic."
4) Add local subnet address in xx.xx.xx.xx/yy format, where xx.xx.xx.xx is the network address and yy is the length of the subnet mask. For example, if local subnet is 192.168.1.0 and subnet mask is 255.255.255.0, set "Subnet Mask # 1" to "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.

4.6.6 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. In figure 12, the local traffic is also displayed due to the gateway monitoring feature being enabled. Now the user can differentiate between local traffic volume and external traffic volume.

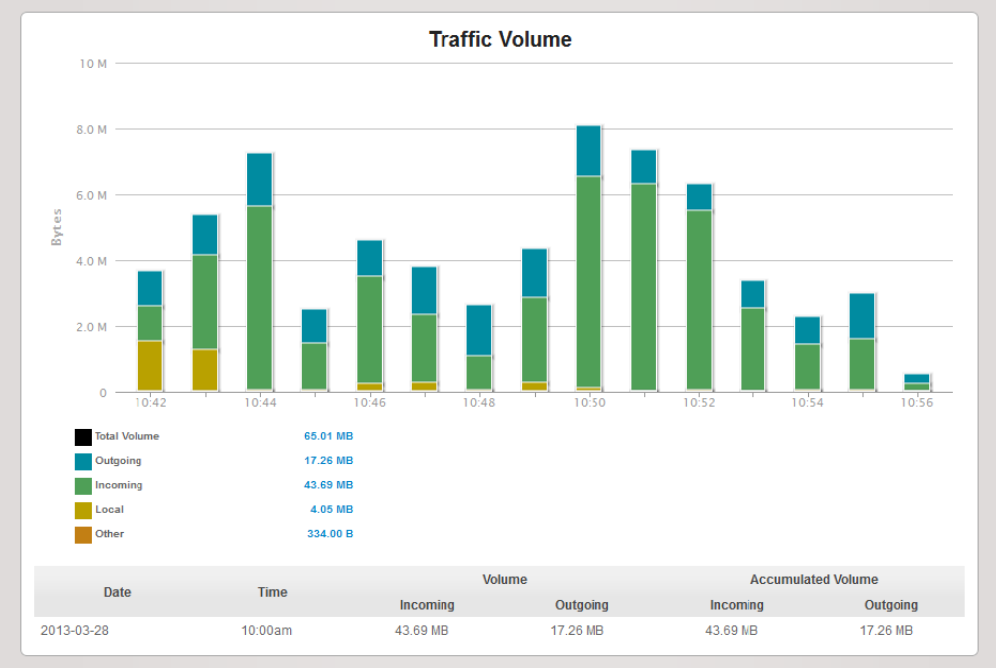


Figure 12 : Traffic Volume Chart

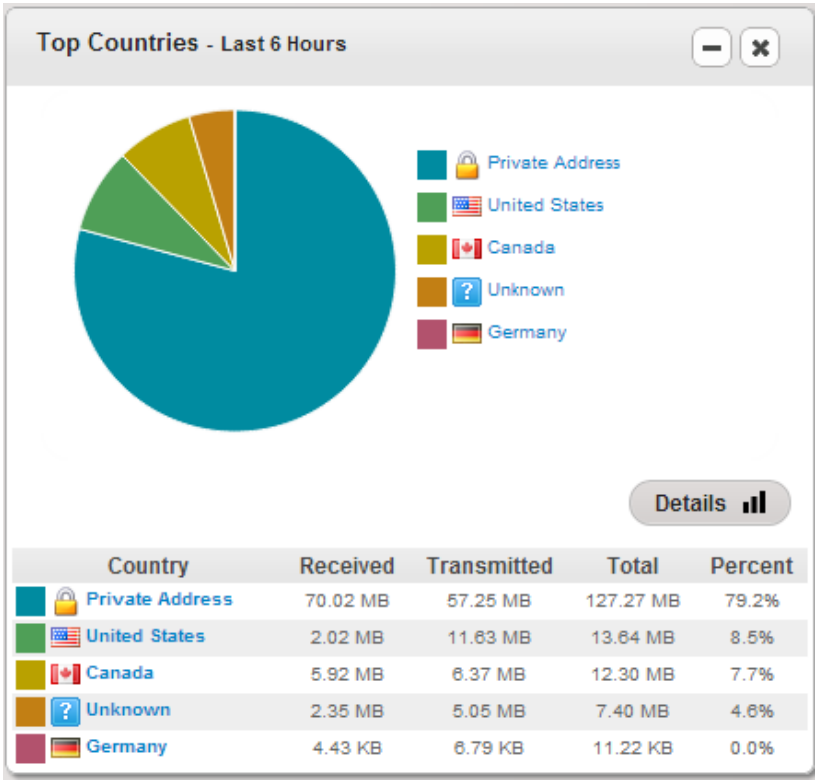
4.6.7 Traffic Statistics

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.

4.6.8 Top Countries

The Top Countries gadget displays the top five countries consuming the network bandwidth for the appropriate time period. The default view is a pie chart of the top 5 countries with a table view of the data. The table view can be hidden by selecting minimize on this gadget. The pie chart displays the top 5 countries percentage of traffic consumption in relation to the top 5 countries displayed. The table displays the received, transmitted and total traffic for each country. Hovering over the country also displays the percentage of traffic consumption for that country.

Clicking details at the bottom right of the gadget will display the top 20 countries in a report for the selected time frame on the dashboard. Now, the top 20 countries are displayed with their respective percentages. The table below the pie chart lists the countries from highest generated traffic to lowest generated traffic and outlines the received, transmitted, and total traffic for that country.



Country	Received	Transmitted	Total	Percent
Private Address	70.02 MB	57.25 MB	127.27 MB	79.2%
United States	2.02 MB	11.63 MB	13.64 MB	8.5%
Canada	5.92 MB	6.37 MB	12.30 MB	7.7%
Unknown	2.35 MB	5.05 MB	7.40 MB	4.6%
Germany	4.43 KB	6.79 KB	11.22 KB	0.0%

Figure 13: Top Countries

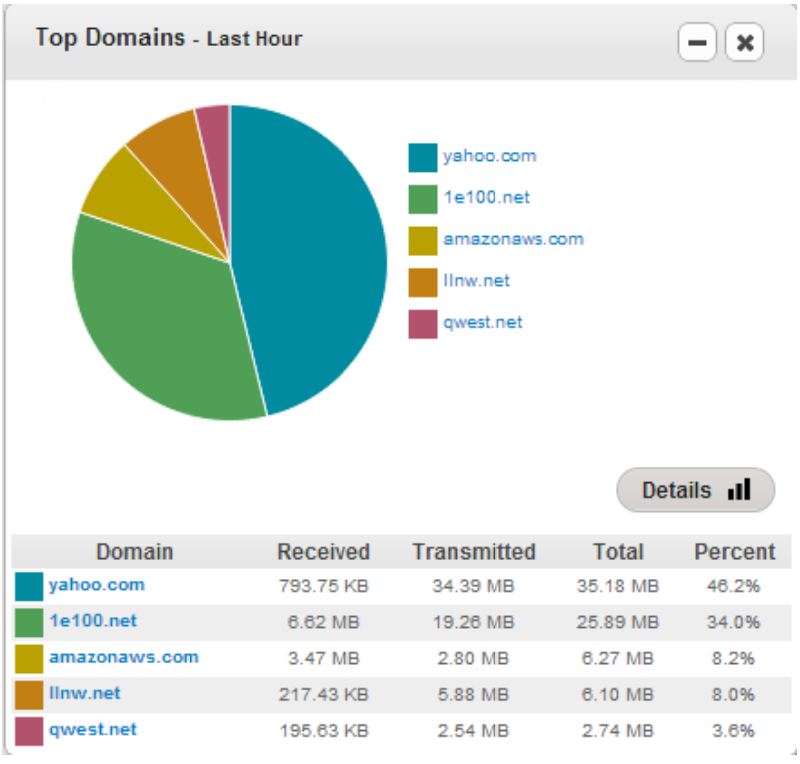
4.6.9 Top Domains

The top domains gadget will display the most domains. The gadget displays the top five domains consuming the network bandwidth for the time period specified on the dashboard. The top domains gadget displays a pie chart of the top 5 domains with a table view of the data. The table view can be hidden by selecting minimize on this gadget. The pie chart illustrates the top 5 domains percentages of traffic consumption in relation to the top 5 domains displayed. The table displays the received, transmitted and total traffic for each domain. Hovering over the domain also displays the percentage of traffic consumption for that domain.

Clicking details at the bottom right of the gadget will display the top 20 domains in a report for the selected time frame on the dashboard. Now, the top 20 domains are displayed with their respective percentages. The table below the pie chart lists the domains from highest generated traffic to lowest generated traffic and outlines the received, transmitted, and total traffic for that domain.

To view data associated with a domain, drilldown by clicking on the domain of interest. For more information on drilldown see section 5.

Note: when adding a domain filter on to the dashboard that has not yet been populated, a warning message will pop up. This is to ensure the correctness of the domain name. If the domain is later populated, then this will reflect in the filtered dashboard.



Domain	Received	Transmitted	Total	Percent
yahoo.com	793.75 KB	34.39 MB	35.18 MB	46.2%
1e100.net	6.62 MB	19.26 MB	25.89 MB	34.0%
amazonaws.com	3.47 MB	2.80 MB	6.27 MB	8.2%
llnw.net	217.43 KB	5.88 MB	6.10 MB	8.0%
qwest.net	195.63 KB	2.54 MB	2.74 MB	3.6%

Figure 14: Top Domains

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
- Top domains
- Top countries

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.

6. Custom Time Intervals

The custom time interval allows the user to view any period of time in the past 3 months. This gives the user accessibility to view stored live traffic on any dashboard gadget or generated report. For example, if the user wanted to view a past day they would simply set the start and end time in the custom time interval, as seen in the below figure.

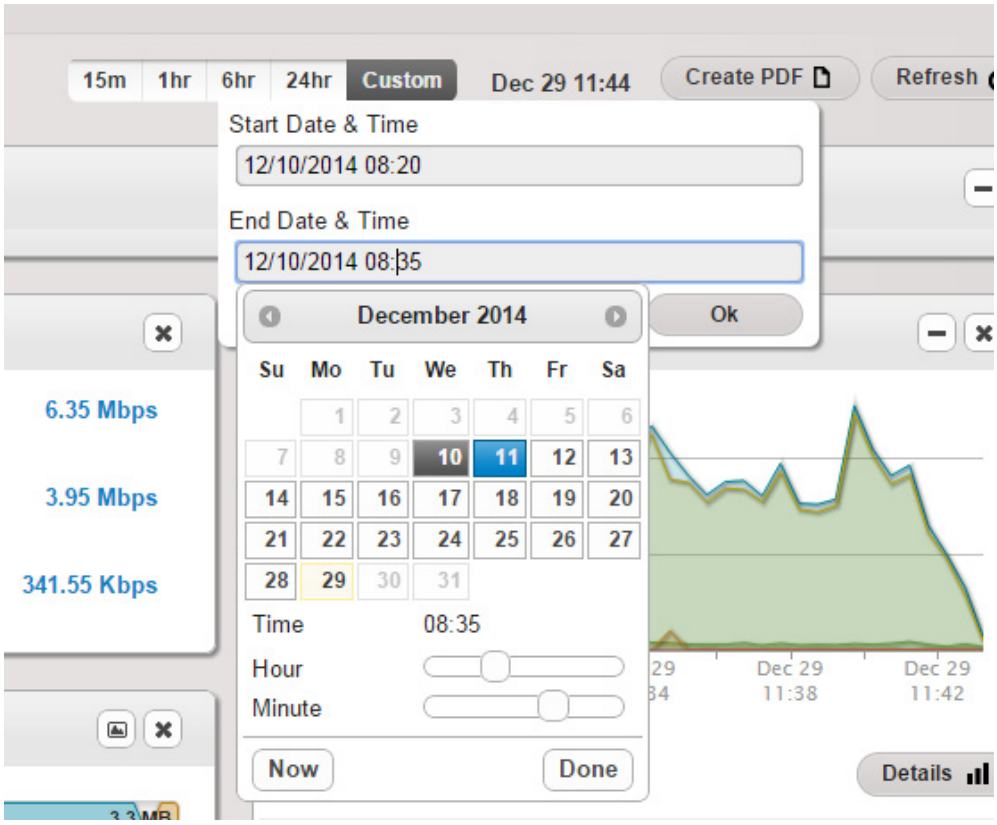


Figure 15: Custom Time Interval

The custom time interval also has a calendar to visually select a past date. After selecting a custom interval, simply select "Ok" to generate the dashboard with a chosen interval's traffic. All of the features available with the other time tabs, such as 15min, are also available with the custom time interval. The custom time interval traffic can be filtered or drilled down on to provide further insight. The reports (as described in the next section) can also be generated to correspond to the traffic in a customized interval.

7. 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:

- Executive Summary
- Traffic Usage Summary
- Bandwidth
- Traffic Volume
- Top 20 Applications
- Top 20 Conversations
- Top 20 Classes of Service
- Top 20 Endpoints
- Top 20 Countries
- Top 20 Domains
- Top Application Detailed
- Top Conversation Detailed
- Top Endpoint Detailed

Each of the above reports can also be generated for pre-defined IP-Groups and/or any of the filters described in 4.2.

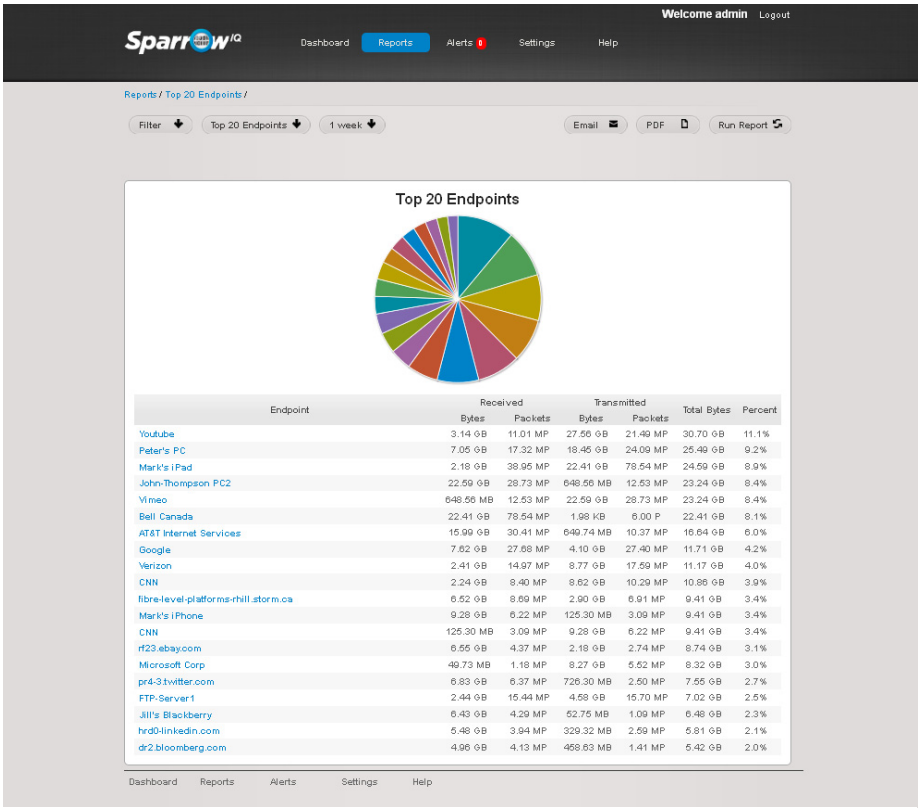


Figure 16: Top Endpoints Report

Reports are available in the following timeframes.

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

Data older than 3 months is purged automatically.

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

7.1 *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 9.9 for details. To email the report, click the "Email" button, fill out the form, and click Send. A message at the top of the page will notify you that the email will be sent shortly. It is imperative that the correct email address of the recipient be used.

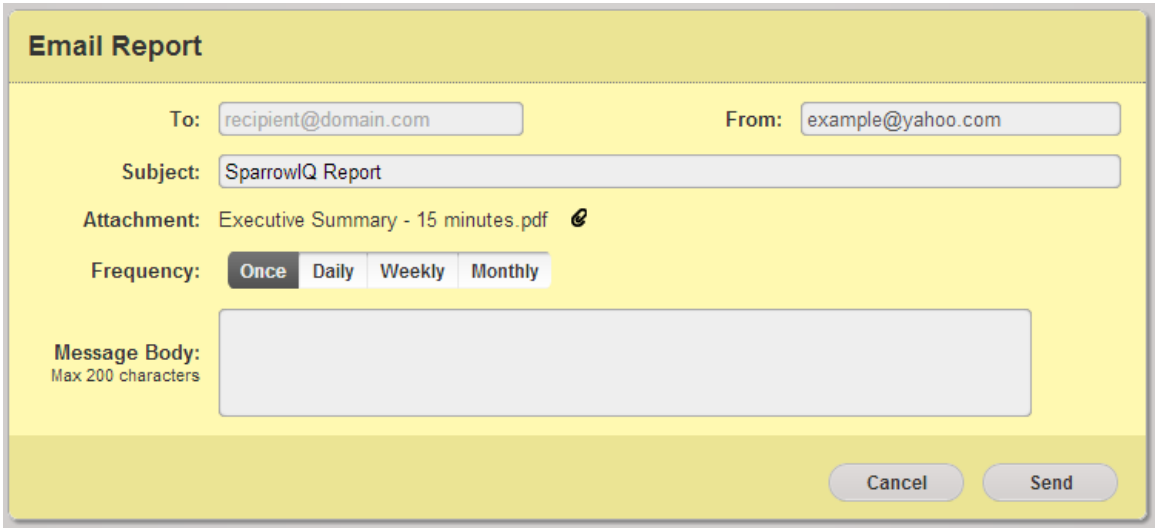


Figure 17: Email Report

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 the time created on the selected day. In order to see the list of scheduled emails, and to cancel any previously scheduled reports, see section 9.11.

8. 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.

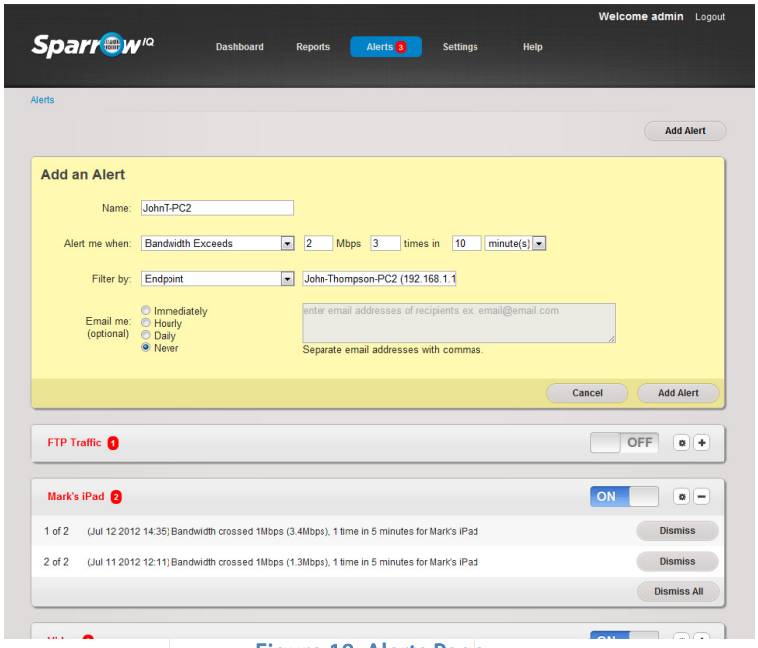


Figure 18: Alerts Page

- 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, Classes of Service (CoS), Countries or Domains. For the selected filter, Sparrow[IQ] provides the list of available options
- Note: When entering an alert with a domain filter that has not yet been populated, a warning message will appear. This message is to ensure correctness of the domain entered. The custom alert will be generated if the domain crosses the specified alert threshold.

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 defined above, follow the following steps:

1. Go to the *Alerts* page.
2. Click Add Alert.
3. Enter the following details:
   - Name: SSH*Alert*
   - Alert me when: *Bandwidth Exceeds, 2* Mbps, *3* times, in *1* hour
   - Filter by: Application SSH (22)
   - Notify me: *Daily*
   - 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 Sparrow[IQ] 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.

9. Settings

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

9.1 *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:

- Number of flows processed in last cycle
- Sparrow[IQ] version information
- License information - Maintenance and update expiry date
- 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.

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

9.2 *Settings*

This tab includes the following settings:

- 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.
- Web Timeout – Users are automatically logged out of Sparrow[IQ] after idling for this duration.
- Dashboard Refresh – This is the refresh rate of gadgets on the dashboard.
- 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.
- 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.
- Delete Database – this deletes all network traffic data stored on the database.
- Max Database size - This will set the maximum database size ranging from 80 GB to 160 GB.
- Debug Logging - This causes additional debugging information to be logged.

9.3 *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.xxx 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, traffic statistics and traffic volume graphs.

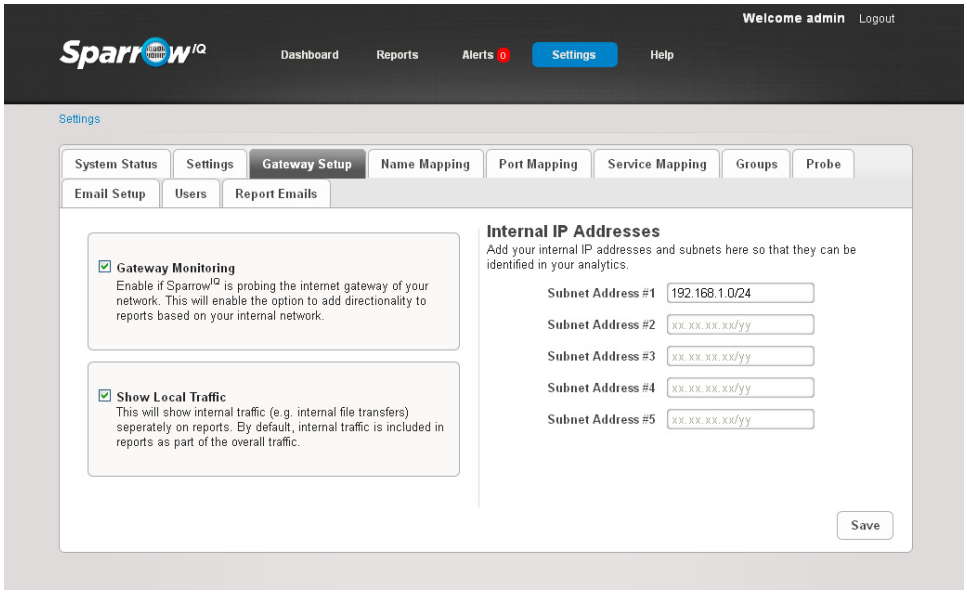


Figure 19: Gateway Setup

9.4 *Name Mapping*

This feature allows you to give aliases to IP Addresses. IP addresses may be resolved to a longer name then desired, or an IP address may not be resolved. This tool allows you to give friendly names to IP addresses that you will recognize. Simply click on *Add Entry* and enter the IP address and Alias before clicking the checkmark to *save*.

Discovered IP addresses, and their resolved names, cannot be edited; however aliases can be configured for these addresses.

9.5 *Port Mapping*

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

9.6 *Service Mapping*

This feature allows you to give aliases 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. Only the alias of pre-configured classes of service can be modified. To add a new alias, simply click on *Add*

Entry, enter the value and alias, and then click on the checkmark to *save*. To edit an existing entry, click on the alias and make the change.

9.7 *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.

9.8 *Probe*

This feature allows the user to change the interface used for listening to 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, the probe page 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.

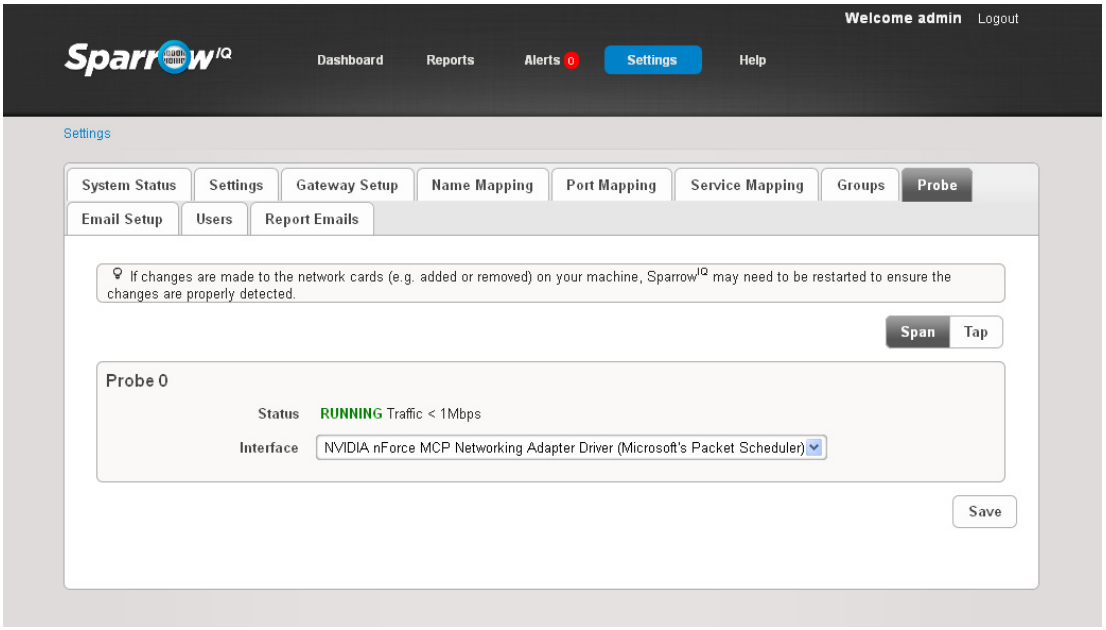


Figure 20: Probe Setup

9.9 *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 select *Save* before testing the settings.

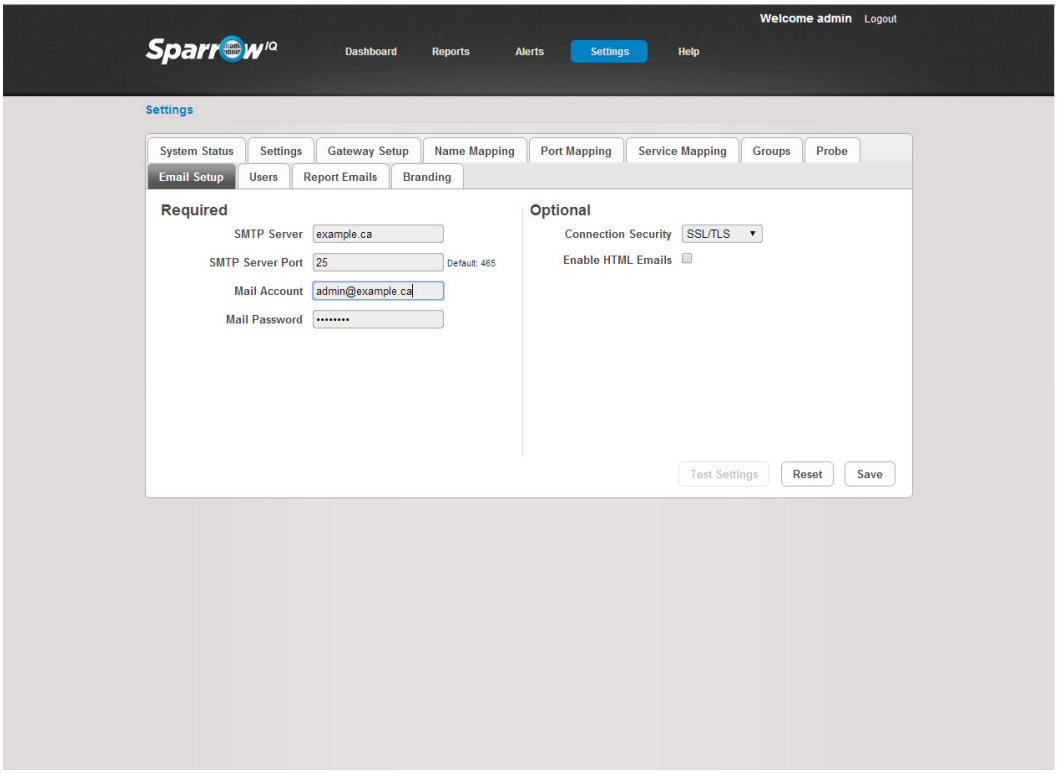


Figure 21: Email Setup

9.10 *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 or updated by clicking on the 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, depending on your license..

9.10.1 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

9.11 *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 and time on which the report is run. To remove any scheduled report, simply click the 'x' button on the associated row.

10. Help

The Help page displays this User Guide.

11. Troubleshooting Sparrow[IQ]

1. *When I try to run the installer, I receive a message saying that Sparrow[IQ] is already running.*

    a. Shut down Sparrow[IQ] by right-clicking on the Sparrow[IQ] icon in the system tray and clicking the "Exit" item.
    b. To be sure all processes have stopped, start the Task Manager using CTRL + ALT + DEL and select the Processes tab. If any of the following processes are in the list, select them and click "End Process":
        - sparrow_node.exe
        - sparrow_analyze.exe
        - sparrow_web.exe
        - sparrow_logger.exe
        - probe.exe
        - mysqld.exe

    You should now be able to install Sparrow[IQ].

2. *I get an error when attempting to run the Sparrow[IQ] SystemIDFinder.*

    The Sparrow[IQ] SystemIDFinder requires that the Microsoft .Net 2.0 Framework be installed. This software is freely available from the Microsoft website.

3. *I get an "Invalid or Missing License" message after starting Sparrow[IQ] or after entering my license code.*

    a. Please ensure that the license entered is copied or typed exactly as given. Licenses are case-sensitive.
    b. Purchased licenses are tied to a specific computer. Verify that the license to be used is appropriate for the computer by confirming the SystemID.
    c. Verify that the license corresponds to the correct version of Sparrow[IQ]. Each new version will require a new license. Your license key can be updated free of charge within your maintenance period by going to the Sparrow[IQ] support page. For more details, check out the FAQ page on www.sparrowiq.com.

4. *After entering my license, I get a "Timer file broken / missing" message.*

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

5. *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 moments to initialize before connections and logins are allowed.
b. If accessing Sparrow IQ remotely, please ensure that you have network connectivity to the Sparrow IQ computer.
c. Sparrow IQ runs on port 8000 by default and this address must be specified within your browser using the format "http://<IP Address>:<port>/", where <IP Address> is the computer running Sparrow IQ and <port> is 8000 (unless you've changed it).
d. Check with your system or network administrator to ensure that:
    - The Sparrow IQ computer isn't blocking or filtering the web port, and
    - The same isn't blocked by any routers on the network.

6. I cannot log into Sparrow IQ.

a. Check your username and password; both 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 on the login page. Note that this feature requires that an outgoing SMTP server be previously configured.

7. I don't see any data on my dashboard or reports.

a. On first startup, or on restart after being shut down for an extended period, Sparrow IQ may take up to three (3) minutes before the first set of data is processed and available for gadgets and reports.
b. Verify the interface selection used by Sparrow IQ. To do this, select the "Probe" tab on the "Settings" page, select the Span or Tap mode as necessary, and select the appropriate network interface, the click Save to save any changes.
c. Verify that all processes are running by going to the "System Status" tab on the "Settings" page. If one or more processes are not running, please restart Sparrow IQ.

8. The gadgets on the dashboard contain the message "Could not retrieve data…" or "Loading…"

a. Click the "Refresh" button. Note that it may take up to three minutes for initially recorded data to become available for gadgets and reports.
b. Verify the probe configuration on the "Settings" > "Probe" page.

9. Why does the dashboard refresh so slowly?

a. Several things affect the time needed to generate data for the dashboard, including:
    - Number of gadgets on the dashboard
    - Selected duration
    - Volume of network traffic recorded for the selected timeframe.

b. Some web browsers are more resource intensive than others. You can examine your browser's resource usage with the Windows Task Manager. Restarting the browser may help.

10. Why do I automatically get logged out from my session?

a. Your session with Sparrow IQ is automatically terminated after 30 minutes of inactivity. This setting can be configured on the "Settings" tab of the "Settings" page.
b. You can only be logged in from one computer at a time. If you log into Sparrow IQ from a second computer, your session on the first computer will be automatically closed.

11. I see alerts generated in Sparrow IQ, but I am not receiving any alert notifications via email.

a. Check the "Email Setup" tab on the "Settings" page to ensure that your email configuration is correct. Once configured, use the "Test Settings" button to confirm that the configuration is working. If the test fails, an error will be reported that may explain the failure. Remember to "Save" changes before testing.
b. Some email providers require SSL or TLS. Check with your email administrator to confirm the required security type and port.
c. Check to see that the email address specified in the alert configuration is correct. Also verify that the value selected for "Email me" is anything but "Never".

12. Why do I see license alarms on the top of every page?

Your Sparrow IQ license has a bandwidth restriction. When certain thresholds are crossed, the "License Warning" and "License Exceeded" messages appear.

13. Why does my bandwidth graph sometimes drop to zero?

a. The Sparrow IQ computer may have power saving features enabled that disable the hard drive or put the computer into hibernation mode. Please check to ensure that these settings are disabled as they interrupt traffic monitoring.
b. A license limit alarm may have occurred if the bandwidth of the monitored network exceeded the limits of your Sparrow IQ license.

14. I received an error indicating that one of the Sparrow IQ processes have died. How do I proceed?

a. Follow the procedure for question 1 to ensure that all Sparrow IQ processes have been stopped and restart Sparrow IQ.
b. If problems persist, please contact us and provide as many details as possible at support@sparrowiq.com.

15. I was asked to export log files for debugging purposes. How do I do that?

a. Go to the "System Status" tab on the "Settings" page and click the "Export Log Files" button. This will download an archive of log files to your default download directory.
b. If the product is not functioning, log files may be retrieved by copying the contents of the "<Sparrow^{IQ} Home> \ logs" directory.

16. How do I erase all network data previously collected by Sparrow^{IQ}?

Go to the "Settings" tab on the "Settings" page and click "Delete Database".