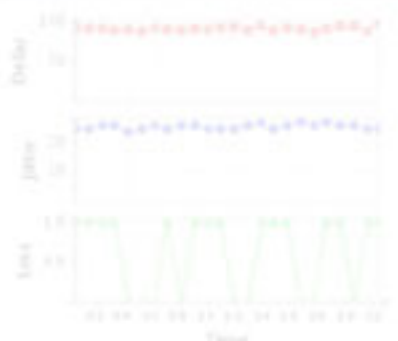


Summary Report

Call Volume



Call Quality



Flat data every: 1 hr

Total Calls	2818	Successful	2671	Waiting	1	Unanswered	146
Good Quality Calls	2567	Answer Success Rate (ASR)	94.8%	Peak Usage Period	11 hrs (13%)	Low Usage Period	21 hrs (24%)
Poor Quality Calls	251	Average Call Duration	1 min 49 secs	Call Rate	1/Minute		
Unanswered Calls	32						
Error Calls	31						
Unmonitored Calls	1						

	Min	Max	Avg
Delay (ms)	80	95	85
Jitter (ms)	25	35	28
Loss (%)	0	1	0
RJOS	3.3	3.4	3.4
R Factor	64	47	64
Good	Tolerable	Poor	Confused

- Quick Links
- Completed Calls
 - All Calls
 - All Alarms
 - Custom Reports

Total Alarms

Clear	12
Warning	25
Major	2
Critical	0
Total Alarms	49



ManageEngine® VQManager

- Quick Links
- Completed Calls
 - All Calls
 - All Alarms
 - Custom Reports
- Alarms by Status
- Error Calls
 - Unanswered Calls
 - Call quality Calls
 - Poor quality Calls
 - Unmonitored Calls
 - All Calls

Refresh Every: 20 Sec Flat data every: 1 hr

Active Calls Summary	Total	Min	Max	Avg	Total (Packets)	Min (Packets/sec)	Max (Packets/sec)	Avg (Packets/sec)
Delay	25.2 Kbps	2.8 Kbps	730Kbps	2.31Kbps	200700	0.3	Bandwidth Utilized	36.3
Jitter	1.4 ms	155.2 usps	309.3 usps	235.3 usps	200700	27.5	47.2	36.3
Loss - 43 ms	0.2 ms	1.5 ms	49.0ms	1.0ms	200700	100	100%	100%
Dropouts	1.7 ms	0.4 usps	176.2 usps	109.7 usps	200700	100	100%	100%



Active Calls

Indicator	Participant	Call Start Time	Duration	Call Status	Status Code	More
	John	Fri, 30 Aug 2007 21:30:29	10 sec	Active	999	
	Sharon	Fri, 30 Aug 2007 21:30:25	7 sec	Active	999	
	John	Fri, 30 Aug 2007 21:30:42	22 sec	Active	999	
	Sharon	Fri, 30 Aug 2007 21:30:52	21 sec	Active	999	10
	John	Fri, 30 Aug 2007 21:30:45	13 sec	Active	999	

Table Of Contents

VQMANAGER - INTRODUCTION.....	2
INSTALLATION & GETTING STARTED	4
VQMANAGER CONFIGURATION WIZARD.....	10
LICENSE OPTIONS	16
WORKING WITH VQMANAGER	21
Obtaining Call Information	22
The Calendar - Setting the Client View Port	25
VQManager Web Interface - The Seven Tabs	28
Monitoring Vital Parameters	29
Alarms Tab - Alerting the Administrator	39
Endpoints - Reports on VoIP Terminals	58
Resource Groups.....	65
Admin Operations	72
Reports	84
Data Export.....	90
Concurrent call licensing.....	91
KNOWN ISSUES.....	93
TROUBLESHOOTING TIPS	94
SIP CODES	100
CONTACTING TECHNICAL SUPPORT	103
RELEASE NOTES.....	106
SUPPORT - HELPS IN TROUBLESHOOTING.....	112
WORKING WITH VQMANAGER	114

VQManager - Introduction

Contents

- Overview
 - Features
 - Documentation Structure
-

Overview

In this age of the IT revolution, communication has proved to be very vital for the survival of organizations and businesses. While telephonic communication remains by and large the dominant medium of communication, the cost factor on long distance calls was a major hindrance for productivity gains. The deployment of IP Telephony built on Voice over Internet Protocol (VoIP) helped in achieving huge reduction in costs on communication. This apart, VoIP provides enhanced quality of service on many fronts with internet as the medium of transmission for telephone calls. VoIP has indeed revolutionized the entire telecommunication stream by enabling communication through various multimedia applications.

Deployment of VoIP infrastructure alone is not sufficient to sustain the business by reducing costs. A sound monitoring system should be in place to check the quality of the VoIP infrastructure continuously. Monitoring the call traffic, call quality, success to failure ratio, analyzing the reasons for failed calls and poor quality calls is important for ensuring customer satisfaction.

VQManager - an elegant solution

ManageEngine VQManager is a powerful, web-based, 24x7 real-time QoS monitoring tool for VoIP networks. It enables IT administrators to monitor their VoIP network for voice quality, call traffic, bandwidth utilization and keep track of active calls and failed calls. VQManager can monitor any device or user-agent that supports SIP, Skinny, H.323 and RTP/RTCP.

Data flow in VQManager is depicted in the diagram below:

Features

- Proactive, continuous monitoring of the QoS & Bandwidth of VoIP Network
- Monitor any device or user-agent that supports SIP, Skinny, H.323 and RTP/RTCP
- Alarm generation based on incomplete calls, answer delay, voice bandwidth usage and other metrics

Pictorial representation of call flow plotting all SIP, Skinny and H.323 requests from call start to end

- Real-time monitoring and trend analysis for troubleshooting
- Importing call information using CDR files such as FTP access or uploaded via HTTP

- Bandwidth usage graph with split up between voice and non-voice data
- Filtering criteria to capture or monitor call traffic from specific IP addresses
- Information on 'what is going on' in VoIP network and 'how it performs' are presented in the form of comprehensive, intuitive and informative reports

Documentation Structure

This document comprises the following sections structured based on the sequence of operations a user would perform using the VQManager:

- **Installation and Getting Started** provides information on how to install VQManager, how to connect Web Interface and start working with VQManager
- **Configuration Wizard** assists in setting up VQManager to receive VoIP call traffic so as to report on call statistics and quality information
- **License Options** provides information on the different editions of VQManager
- **Important Terminologies** provides brief explanation about the various commonly used terminologies in VQManager
- **Working with VQManager** begins with notes on setting up VQManager to obtain call information in the VoIP network, explains on the Calendar component and Web Interface, provides details on working with each tab in the VQManager UI and ends with an explanation on the various Data Export options available
- **Known Issues** provides a list of known issues in the latest VQManager release
- **Troubleshooting Tips** provides solutions to the common problems faced when working with VQmanager

Get Support lists out the various ways by which you can get solutions to any problems faced while working with VQManager

Installation & Getting Started

Contents

- Overview
- System Requirements
- Prerequisites
- Components of VQManager
- Installing VQManager
 - In Windows
 - In Linux
- Starting and Shutting Down
 - In Windows
 - In Linux
- VQManager as a Service
 - In Windows
 - In Linux
- Connecting Web Interface
- Ports Used by VQManager
- Uninstalling VQManager
 - In Windows
 - In Linux

Overview

Welcome to ManageEngine VQManager!

This section provides information on how to install VQManager in your system. System Requirements for VQManager, prerequisite software needed to work with the product, how to install VQManager, how to start and shutdown the server and how to connect Web-Interface after successfully starting the server have been dealt with in this section.

System Requirements

Hardware	Operating systems	Web-Interface
Processor* 1.8 GHz Pentium® processor RAM* 1GB Hard Disk 2 GB for product & database	Windows <ul style="list-style-type: none"> • Windows 2000 SP4 • Windows XP Professional • Windows Vista(How to enable VQManager in Windows Vista) Linux VQManager 6.1 installation requires the standard C++	Web-Interface requires one of the following browsers to be installed in the system: <ul style="list-style-type: none"> • IE 6.0 and above (on Windows) • Mozilla 1.7 and above (on Windows and Linux) • Firefox 1.0.5 and above (on Windows and Linux)

Hardware	Operating systems	Web-Interface
	libraries(libstdc++) and GCC(4.0 or above) core libraries(libgcc). The following list contains the minimal Linux distributions that contain these libraries: <ul style="list-style-type: none"> • Red Hat Enterprise Linux 4.4 • Mandriva 2006 • Debian 4.0 • Ubuntu 5.10 • CentOS 5 • SuSE Linux 10 • Fedora Core 4 For more details on GCC compatibility see: GCC libraries incompatibility	VQManager is optimized for 1024 x 768 resolution and above.

* Optimal hardware configurations required depends on the number of simultaneous calls that happen in the network. The following table recommends the RAM size requirements for different numbers of simultaneous calls.

No. of simultaneous calls	Processor speed*	RAM*
0-100	1.8 GHz	1 GB
101-300	2 GHz	2 GB
301-500	2 GHz, Dual Core	4 GB
501-800	2 GHz, Quad Processor	4 GB
800-1000	4 GHz, Quad Processor	8 GB

Note: A minimum of 100 MB of disk space is consumed by the database for every 10,000 calls' data stored.

Prerequisites

Prerequisite Software

VQManager requires the following platform-specific software:

- **For Windows:** WinPcap 4.0.2 needed by VQManager is bundled with the product. During product installation, it gets installed in the VQManager installation directory
- **For Linux:** Most linux systems come with the pcap libraries. If they are not present, download the latest libpcap source, compile them and install

<p>Note: If the aforesaid software is not present in the system, VQManager Server will not start. So, ensure pcap libraries (for Linux) are present.</p>

Prerequisite Setups

- VQManager monitors the VoIP calls by sniffing the VoIP packets in the network. In a switched network, by default, it is not possible to get all the packets flowing in a network from one machine. To overcome this, port mirroring has to be enabled in the switch to send all the VoIP packets to the machine where VQManager is running
- This link has information on configuring port-mirroring in a number of managed switches like 3Com, Cisco Systems, Linksys, NETGEAR, Avaya etc.
- As VQManager needs to sniff the packets from the interface card, it needs to be run in administrator mode

Components of VQManager

The VQManager download consists of the following components:

- **The VQManager Server** consisting of application server and database
- JRE 1.5.0_11 bundled with VQManager
- MySQL 5.0.44 bundled with VQManager

Installing VQManager

In Windows

- Download and install ManageEngine_VQManager.exe
- The installation wizard will guide you through the installation process
- Accept the License agreement
- Choose an installation directory - by default, it will be installed in C:\ManageEngine\VQManager; Henceforth, we shall refer to this installation directory path as "VQManager_Home".
- By default, VQManager uses **8647** as the webserver port and **5306** as the port for the database. If you want to change any of these ports, just enter the values
- Choose directories and file name for VQManager program icons
- Next comes a registration form for registering with VQManager support for quick response during evaluation. This is purely optional. Pass on to the next step if you do not wish to register for technical support.
- In the final step, you will see two check-boxes - one for viewing ReadMe file and the other one for starting the server immediately after installation; if you choose to start the server immediately, it will get started.
- If you do not choose this option (that is, not to start the VQManager server immediately after the installation process), you can start it later from the 'Start' menu Start >> Programs >> AdventNet ManageEngine VQManager >> Start Server.
- From the Start Menu, you can perform other actions such as shutting down the server ('Shutdown Server'), view ReadMe ('View ReadMe'), viewing help document ('View Help') and uninstalling the product ('Uninstall').

In Linux

- Download ManageEngine_VQManager.bin for linux
- Assign executable permission using command `chmod a+x <ManageEngine_VQManager.bin>`
- Execute the following command: `./ManageEngine_VQManager.bin`
- Follow the instructions as they appear on the screen
- VQManager is installed in your machine in the desired location. Henceforth, we shall refer to this installation directory path as "VQManager_Home"

Starting & Shutting Down VQManager

In Windows	In Linux
<p>To Start the server</p> <p>Navigate to <VQManager_Home>/bin directory Execute "run.bat"</p> <p style="text-align: center;">-OR-</p> <p>Navigate to <VQManager_Home>/bin directory Execute "startVQManager.bat"</p>	<p>To Start the server</p> <p>Open a console and navigate to <VQManager_Home>/bin directory (as root user) Execute the script "sh run.sh"</p>
<p>To Stop the server</p> <p>Open a console and navigate to the <VQManager_Home>/bindirector y Execute "shutdown.bat"</p>	<p>To Stop the server</p> <p>Open a console and navigate to <VQManager_Home>/bindirector y Execute the script "sh shutdown.sh"</p>
<p>To Reinitialize the DB</p> <p>Open a console and navigate to the<VQManager_Home>/bindirec tory Execute "reinitializeDB.bat"</p>	<p>To Reinitialize the DB</p> <p>Open a console and navigate to <VQManager_Home>/bindirector y Execute the script "sh reinitializeDB.sh"</p>

VQManager as a Service

The VQManager product can be installed as a Windows/Linux service during the installation time itself. Just in case this was missed out, you can still install the VQManager as a Windows/Linux service through the following means:

In Windows	In Linux
<p>To Install the Service</p> <p>Navigate to <VQManager_Home>/bin directory Execute "wrapper.exe -i ..\conf\wrapper.conf"</p>	<p>To Install the Service</p> <p>Open a console and navigate to <VQManager_Home>/bin directory (as root user) Execute the script "sh setup-service.sh install"</p>
<p>To Start the server</p> <p>Open a console and navigate to the <VQManager_Home>/bindirector y Execute "wrapper.exe -c ..\conf\wrapper.conf"</p>	<p>To Start the Server</p> <p>Open a console and navigate to <VQManager_Home>/bindirector y Execute the script "/etc/init.d/vqmanager- service start"</p>
<p>To Stop the Server</p> <p>Open a console and navigate to the<VQManager_Home>/bindirec tory Execute "wrapper -p ..\conf\wrapper.conf" or "net stop vqmanager"</p>	<p>To Stop the Server</p> <p>Open a console and navigate to <VQManager_Home>/bindirector y Execute the script "/etc/init.d/vqmanager-service stop"</p>

Connecting Web Interface

- On successful startup of the server, you will see the message "Connect to: [http://localhost:8647]" on the console
- VQManager provides a Web based client to monitor the calls. It can be accessed using a browser. Open a browser and connect to the URL as shown below:

http://<hostname>:portnumber/

where
 <hostname> - host where VQManager server is running

Default port is 8647. [8647 stands for **voip** in the telephone/mobile dial pad].

e.g. http://localhost:8647/.

- Type the Username and Password and press Enter. By default, the username and password will be admin and admin respectively
- For first-time logins, the "VQManager Configuration Wizard" will appear to help configure the data input options for VQManager

Ports Used by VQManager

VQManager uses the following four ports:

MySQL Port - 5306
Port for connecting Web Interface - 8647
SNMP Agent - 8001
SNMP Trap Listen - 8002

Uninstalling VQManager

In Windows

- Stop the VQManager server if it is already running.
- On your desktop, click on the Start button to open your Start menu
- When the Start Menu opens, click on the All Programs Menu option
- In the Menu that opens, click on the ManageEngine VQManager Menu option
- Click on the Uninstall option.
- You will be guided by the uninstallation wizard for the complete unistallation of VQManager from your machine

In Linux

Stop the VQManager server if it is already running
Open a console and navigate to *<VQManager Home>/_uninst* directory
Execute **`./uninstaller.bin`** *-console*

VQManager Configuration Wizard

Contents

- Introduction
 - Choosing the data input option
 - Using VQManager's in-built sniffer
 - Protocol Settings
 - Store registrations
 - Advanced Settings
 - RTCP based QoS calculation
 - RTP based QoS calculation
 - Using NAT
 - Store Raw Packets
 - Promiscuous Mode
 - Sniffing Enabled
 - Filter string
 - Log Level
 - RTP interruption
 - Signalling interruption
 - Choosing the Sniffer Interface
 - Using imported CDRs
 - Importing CDRs as syslog messages
-

Introduction

The VQManager configuration wizard appears when the user logs into the VQManager client for the first time. This wizard helps to set the initial configurations needed to have VQManager report on the call statistics and call quality information.

The first screen that opens up is the Configuration Wizard Welcome screen with a brief on the three ways of getting your network's VoIP call traffic details into VQManager.

Choosing the data input option

There are three ways of getting data input into VQManager so as to report on your VoIP call traffic. Each method differs in how quickly the VoIP calls in your environment are reported on by VQManager. The default and recommended option is using the in-built VQManager sniffer.

- **Using the in-built VQManager sniffer**

This is a real-time approach to monitoring VoIP call activity and QoS. VQManager reports & displays packet-level details of VoIP call traffic monitored in this method, thus enabling in-depth diagnosis and troubleshooting of call quality degradations or failures.

- **By importing Call Detail Records(CDRs) from call servers**

This method is not real-time and call statistics and quality information displayed by VQManager will depend on the information contained in the imported Call Detail Records. CDRs are best used for reporting on VoIP traffic from geographically distant locations whose traffic cannot be brought to the VQManager sniffer interface(NIC).

- **By importing the Call Detail Records as syslog messages**

Similar to importing CDRs, this method allows automation of the import process and thus allows quicker 'almost real-time' reporting on VoIP call traffic.

Using VQManager's in-built sniffer

VQManager can 'sniff' traffic through the Network Interface Card(NIC) of the machine that has VQManager installed. You will need to ensure that all your VoIP traffic is directed to the NIC of the VQManager machine. One way of getting this done is by enabling port-mirroring in a managed switch. This link has information on configuring port-mirroring in a number of managed switches like 3Com, Cisco Systems, Linksys, NETGEAR, Avaya etc..

On selecting the sniffing method to report on VoIP call traffic, you will be led to a screen that helps to set various configurations found under two headings: "Protocol Settings" and "Advanced Settings"

Protocol Settings

VQManager supports monitoring of SIP, H.323, Cisco Skinny(SCCP), RTP and RTCP protocols. Of these, you can choose which protocols you need monitored by selecting the appropriate radio buttons next to the listed protocols. The signaling protocols are globally assigned specific ports and VQManager is set by default to monitor protocol traffic from these standard ports:

- SIP: 5060(SIP over UDP only supported)
- H.323(H.225 call signaling): 1720 and
- Cisco Skinny(SCCP): 2000

You can change these port numbers if your call servers have assigned different ports for the protocols. For each protocol, you can also configure VQManager to listen on "all ports" if the protocols in your environment are using multiple ports. Listening on multiple ports will affect the VQManager server performance and it is advised to set VQManager to listen on one port only for each protocol if such is the case in the environment.

Store registrations

In the "SIP information" section, there is also an option to enable storing of SIP registrations. By storing these, you can have VQManager report on details of registration and unregistration requests made by the phones to the SIP call servers. The registration request details can be found in the "Endpoints" tab of the product's User Interface. These come in handy when troubleshooting non-availability issues of endpoints.

Advanced Settings

VQManager can calculate QoS metrics from the RTCP streams, RTP streams and also by taking the QoS values from the "Connection Statistics Response" packets in the case of Cisco Skinny(SCCP) calls.

RTCP based QoS calculation

RTCP(Real Time Control Protocol) packets are generated and transmitted by the endpoints and these provide feedback on the Quality of Service being provided by the RTP(Real Time Transport Protocol)/voice streams. Thus, QoS calculation from RTCP packets provides efficient and accurate QoS reporting as these are from the endpoints themselves. Thus this option requires that the endpoints in the network are enabled with RTCP packet generation.

RTP based QoS calculation

VQManager can also calculate QoS statistics from the RTP(Real Time Transport Protocol) streams. For complete QoS reporting by this method, it is necessary that RTP packets from both participants of a call are available at the listening interface(NIC).

Note:

As endpoints themselves generate RTCP packets, enabling the "RTCP based QoS calculations" will allow VQManager to report closer to user quality experience as compared to calculation of QoS metrics from the RTP packets. It is advised to keep both "RTCP based QoS calculations" and "RTP based QoS calculations" enabled when you are unsure on whether all the endpoints in the network generate the RTCP packets. When both options are enabled, higher precedence is given to RTCP based calculations. In the presence of "Connection Statistics Response" packets in Cisco Skinny calls, these packets are given highest precedence for QoS calculations.

Using NAT

This option need not be enabled if your IP Phones are behind a NAT server and the phones have STUN(Simple Transversal of UDP through NATs) to resolve their external IP address. If the phones do not have STUN, then enable this option in VQManager so as to have proper, complete reporting of the QoS metrics.

Store Raw Packets

Enable this option if you want the raw, detailed SIP, Skinny and H.323 packets to be stored and displayed by VQManager. Raw packet information help in troubleshooting call problems.

Promiscuous Mode

Promiscuous mode refers to the state when the chosen interface(NIC) sniffs all information in the interface regardless of the destination of the individual packets. In

normal mode, the interface sniffs packets/information destined for itself alone. By default, "Promiscuous Mode" is enabled. If you want to disable this, deselect the checkbox

Sniffing Enabled

By default, sniffing is enabled to monitor VoIP call traffic in real-time using the in-built sniffer. In case, you wish to use other methods to obtain call information such as parsing the Call Detail Record (CDR) log files generated by call servers or Parsing the CDR logs sent as Syslog Message, you can disable this.

Filter String

You can provide the pcap filter string here to ensure required packets are only processed by the VQManager sniffer. This filter string expression can be provided in similar syntax as that in the case of WinPcap or Pcap filters. By default, the filter string is `tcp || udp || vlan`. This filter string allows only tcp, udp and vlan packets to be processed by the VQManager sniffer; all other packets are not processed.

Log Level

Choose "Log Level" for the messages generated by the sniffer from the drop-down. One of the three levels - DEBUG, SEVERE & INFO can be chosen. The default level is INFO. For VQManager sniffer problem troubleshooting, this can be changed to higher options.

RTP interruption

This setting is used to configure VQManager to handle calls whose RTP flow has been stopped for "x" duration of time. Provide the desired duration(in seconds) in the text field. By default, if RTP flow for any call has not been received for more than 30 seconds, this call is considered ended and the call flow diagram will depict "media transmission stopped" as the last packet. These type of calls can be distinguished by status code "8100". To prevent VQManager from terminating RTP interrupted calls, provide '0' seconds as the time duration in the text field.

Signaling Interruption

This setting is used to configure VQManager to handle calls whose signalling flow has been stopped for "x" duration of time. Provide the desired duration(in seconds) in the text field. By default, if signaling flow for any call has not been received for more than 60 seconds, this call is moved to the "Unmonitored" calls category. These calls can be distinguished by status code "8003". To prevent VQManager from categorizing such calls as "Unmonitored", provide '0' seconds as the time duration in the text field.

Choosing the sniffer interface

After saving the protocol settings and other advanced settings, the configuration wizard will auto-detect the interfaces (NICs) present in your machine. The wizard will also look for the available protocols in each interface. Once all available protocols are listed at each interface, you will need to select one interface that the VQManager sniffer will listen to.

Tips:

If there are no protocols detected on any interface:

- Check if there are VoIP calls being made in your network
- Check whether your VoIP traffic has been directed to one of the interfaces in the VQManager machine. One way of directing all traffic to the VQManager interface is by enabling port-mirroring in a managed switch. This link has information on configuring port-mirroring in a number of managed switches like 3Com, Cisco Systems, Linksys, NETGEAR, Avaya etc.
- Check if the protocols(SIP,H.323 & Skinny) are using the default ports, if not ensure that you have provided the correct ports in the previous "protocols settings" screen of the Configuration wizard.

If still no protocols are detected, it may be that your environment has protocols not supported by VQManager.

After selecting an interface to monitor on, save the settings. You will then see the summary of all settings configured for the VQManager sniffer. You can also go back and re-configure from this summary screen.

Using imported CDRs

Call Detail Records(CDRs) are files that are generated by call servers/ callmanagers/ gateways or other call routing devices. These files have a record of all the calls that have happened in the network. CDR files can be of many formats like .xls, .csv, .xml etc. By importing these CDR files, VQManager can report on the call information and quality statistics present in these files. Since these files are generated after the calls having taken place, this method of call traffic reporting by VQManager will not be in real-time and the information displayed will depend on that available in the CDRs. This method of reporting is best used for reporting on VoIP traffic from geographically distant locations whose traffic cannot be brought to the VQManager sniffer interface(NIC).

VQManager supports .csv formats of the following CDR types:

- Vocal CDR Format
- Cisco CallTracker CDR Format
- Asterisk CDR Format
- Avaya S8700
- Cisco Call Manager 4.x and 5.x CDR
- Cisco Unified Communications Manager 6.1, 7.0 CDRs
- Cisco Call Manager 5.0 CDR/CMR
- Shoretel 6.1
- Swyx 6.0
- Tekelec 5.6
- PortaOne

On clicking the CDR import option, you will be led to a screen inside the product that helps you to import the CDR files either from the local machine, or on a remote machine:

- In the UI that opens, click the link "**Import CDR File**" icon available in the top-right corner

- If the CDR log file is available in your local computer, just browse to the file location and click "**Import**". This is suitable for the processing of small size files
- If the CDR log file is available in a remote machine, you can configure the server to download the CDR log files periodically from a remote location using FTP
- Click "**Remote Location**" and fill-in the details such as the hostname and IP of the machine, username and password to access the system
- Browse to the location of the file or the directory in which the CDR files are present, specify the periodic time interval (in seconds) during which the files are to be parsed and uploaded automatically and then click "**Import**". This is suitable for large files that need to be processed periodically. VQManager can identify new CDR log files in a directory and will automatically import the new content
- A log of all the imported CDR logs will be displayed as a list below

Importing CDRs as syslog messages

VQManager can be configured as a syslog server to receive CDRs as syslog messages from a call server eg. the CallManager Express can be configured to send the CDRs as syslog messages to VQManager. This method automates the sending of CDRs to VQManager and also enables one to have 'almost real-time' reporting of call traffic by configuring the sending of syslog messages(CDRs) in very short intervals. A syslog port (in the VQManager machine) listens to the syslog messages. The call server is configured to send the CDRs as syslog messages to this port.

On choosing this method you will be led to a screen that helps set VQManager as a syslog server:

- Click on the "**Add Syslog Server**" icon seen on the right hand side.
- Provide a "**Name**" to the Syslog Server you wish to configure
- Provide the "**Port**" number through which you want the VQManager product to listen on for the syslog messages. By default the product listens for syslog messages on port 514.
- The "**IPAddress**" displayed is the default IP Address of the system in which the VQManager server is installed in. As VQManager listens on ANY address, no change would be required to be done on this field.
- Click on the "**Add**" button to configure the Syslog server.
- The Syslog servers list is displayed as a list with columns "**Name**", "**IPAddress**", "**Port**", "**Status**" and "**Action**".
- You can stop a Syslog server by clicking on the "**Stop**" icon under the "**Action**" column of the list. You can get the same Syslog server to start again by re-clicking the same icon, which would now be showing '**Play**'.
- Syslog Servers can be deleted by clicking on the dustbin "**Delete**" icon under the "**Action**" column of the list.

License Options

- Downloading VQManager
- Trial Edition
- Free Edition
- Professional Edition
- Licensing Options

Downloading VQManager

- The VQManager software is available as a single downloadable .exe or .bin file
- The VQManager website will have the latest updated .exe and .bin files at <http://www.manageengine.com/products/vqmanager/download.html?trial>

Trial Edition

- Any .exe or .bin file downloaded from the VQManager website is a Trial Edition of VQManager
- This .exe/.bin file is the fully functional VQManager product that can monitor unlimited number of endpoints and unlimited number of concurrent calls for the first 30 days from the installation date
- During your evaluation of the Trial Edition, you can avail support from the VQManager team through the mail alias vqmanager-support@manageengine.com.

Free Edition

- After 30 days of using the Trial Edition, the product will automatically downgrade to a Free Edition.
- This is again a fully functional VQManager product, but with the ability to monitor a maximum of only 10 Endpoints
- The Free Edition does not have any expiry time period but does not entitle to any support from the VQManager support team.

The Professional Edition

Commercially, the VQManager product is available as Professional Edition

The table below lists the availability of features in this edition.

Feature	Professional Edition
SIP protocol support	✓
H.323 protocol support	✓
Cisco® Skinny protocol support	✓
Live and History Reporting of QoS metrics and Bandwidth Utilization	✓
Alarms on threshold violations	✓
Endpoints based and Call based tracking of QoS details	✓

Feature	Professional Edition
Detailed Call Flow diagrams with packet details	✓
Integration with higher level Network management Systems	✓
CDR import and analysis	✓
CDR parsing through Syslog messages	✓
Resource Grouping of Endpoints	✓

Licensing Options

VQManager licenses can be purchased for the:

- Number of IP phones to be monitored or
- Number of concurrent VoIP calls (simultaneous calls at any instant) in the network

Refer to the "Monitored Endpoints" section for more on how VQManager identifies unique Endpoints and IP phones for the purpose of licensing. This licensing is available both as an annual subscription and as a one-time purchase.

In addition to the licensing model based on Number of Endpoints/IP Phones, VQManager also provides a licensing model based on 'Concurrent Calls'. 'Concurrent calls' is defined as the number of simultaneous active calls captured by VQManager at any point of time. The 'Concurrent calls' based license is meant only for Service Provider customers who offer VoIP monitoring service to their end-user customers. This licensing model will work with the 'Professional Edition' of VQManager. This model is based on the maximum number of concurrent calls in the network. For example, if a customer purchases a license for 100 concurrent calls, he/she can monitor at most 100 concurrent calls 'live' in their VoIP network at any point of time. Calls beyond that will not be monitored. For monitoring more calls, the customer will have to upgrade the license to a higher number of concurrent calls. This type of licensing is based on annual subscription, which means that usage of the product will be valid only for one year, beyond which the subscription has to be renewed. Refer to the Concurrent call licensing section for more details.

Important Terminologies

Contents

- Overview
- Terminologies

Overview

While working with VQManager, you will come across many terminologies, predominantly industry-standard terms. This section provides information on some of the important terminologies.

Terminologies

Terminology	Definition
Session Initiation Protocol [SIP]	SIP is a signaling protocol for initiating an interactive user session such as video, voice, instant messaging, online games, and virtual reality. SIP is used for modifying and terminating the user sessions too
CISCO® Skinny Protocol	The Skinny Client Control Protocol (SCCP) is a signaling protocol between Cisco® CallManagers and Cisco® IP phones
H.223 protocol	An umbrella standard defined by the ITU-T, under which a number of other protocols fit, supporting call setup and disconnect, audio encoding/decoding, video encoding/decoding. These protocols include the H.225, H.245 protocols, plus the IETF's Real-Time Transport Protocol (RTP), and others.
H.225 protocol	Call signalling protocols and media stream packetization for packet-based multimedia communication systems
H.245 protocol	Call control protocol for multimedia communication
RTP/RTCP	The Real-time Transport Protocol (RTP) represents the standardized packet format for delivering audio and video over the Internet. Real-time Transport Control Protocol (RTCP) provides the control information for RTP flow
CDR	Call Detail Record is a data record that contains information related to a telephone call, such as the origination and destination addresses of the call, the time the call started and ended, the duration of the call, the time of day the call was made, etc.

Terminology	Definition
SNMP	Simple Network Management Protocol; a standard for gathering statistical data about network traffic and the behavior of network components; SNMP uses management information bases (MIBs), which define what information is available from any manageable network device.
NAT	Network Address Translation is a process of re-writing the internal IP address or network address into a single globally unique IP address
STUN	Simple Transversal of UDP over Nat is a network protocol which helps many types of software and hardware receive UDP data properly through home broadband routers that use network address translation (NAT)
Latency or Delay	The amount of time taken by a Packet to travel from source to destination. Together, Latency and Bandwidth define the speed and capacity of a network
Jitter	The variation in the amount of latency among the packets being received
Packet Loss	Voice packets lost during the call
Mean Opinion Score [MOS]	MOS measures subjective call quality, ranges from 1 for unacceptable to 5 for excellent. [VoIP calls often are in the 3.5 to 4.2 range]
ACD(Average Call Duration)	The average duration of a call made by the endpoint
Average Length of Call (ALOC)	The ratio between the sum of the time duration of all successful calls and the number of all successful calls
Answer Seizure Ratio (ASR)	<p>The ratio between the number of successfully answered calls to the total number of calls attempted is known as Answer/Seizure Ratio.</p> <p>ASR = successful calls / attempted calls * 100</p> <p>The statistic pertaining to ASR is important as it may relate to a non-productive link. It helps in identifying the problem areas in your system</p>
Average Answer Delay	The difference in time duration between successful initiation of call handling by the device and the time taken by the person on the other end to actually attend the call (i.e. delay in answering the call)
e-model	The ETSI e-model as defined in ITU-T G.107 is a planning tool that assigns a certain equipment impairment factor I_e to each piece of equipment in the transmission chain.

Terminology	Definition
	These Ie values are then summed up and combined with several other parameters to give the final R factor or R rating.
CODECS	CODECS are used to convert an analog voice signal to digitally encoded version. CODECS vary in the sound quality, the bandwidth required, the computational requirements etc., Each service, program, phone, gateway etc., typically supports several different CODECS and when talking to each other, negotiate which CODEC they will use.

Working with VQManager

Contents

- Overview
 - Topics Covered in this section
-

Overview

After connecting the web interface with the VQManager server, the VQManager Home Page is displayed. The web interface is arranged in the form of seven tabs. Through these tabs, you can perform various monitoring operations of VQManager. This section provides brief information about each of the tabs.

Before proceeding to monitor the calls in your network, you need to decide the way in which you are going to provide the call information to the VQManager. This section explains this and also deals with the calendar component in VQManager, which plays a powerful role.

Topics Covered in this Section

- Obtaining Call Information
- Setting Client View Port
- VQManager Web Interface
- Monitoring Vital Parameters
- All about Calls
- Alarms - Alerting the Administrator
- Endpoints - Reports on VoIP Terminals
- Administrative Operations
- Reports
- Data Exporting

Obtaining Call Information

Contents

- Overview
 - Sniffing the Packets in the network
 - Parsing the CDR files
 - Parsing the CDR logs sent as Syslog Message
-

Overview

While using VQManager, one of the first things you need to do is deciding how to obtain the call information in the application (VQManager). It can be done in three ways:

- Sniffing the packets in the network
- Parsing the **Call Detail Record** (CDR) log files generated by call servers
- Parsing the CDR logs sent as Syslog Message

Sniffing the Packets in the Network

VQManager sniffs the network packets and filters the VoIP packets viz., SIP, Skinny, H.323, RTP and RTCP and thus monitors the call inventory and QoS information. It also monitors the overall packet flow and computes the ratio of bandwidth utilization of voice to non-voice usage. To get reliable metrics on this front, the VQManager should be able to sniff all the packets flowing in the network. In a typical Switch environment, to get ALL the network traffic into one interface, Port Mirroring has to be enabled and VQManager has to be run in this mirrored port. Refer to the Configuration Wizard section for more details on configuring the specific interface to sniff data from.

Parsing the CDR Files

Call Detail Records(CDRs) are files that are generated by call servers/ callmanagers/ gateways or other call routing devices. These files have a record of all the calls that have happened in the network. CDR files can be of many formats like .xls, .csv, .xml etc. By importing these CDR files, VQManager can report on the call information and quality statistics present in these files. Since these files are generated after the calls having taken place, this method of call traffic reporting by VQManager will not be in real-time and the information displayed will depend on that available in the CDRs.

This method of reporting is best used for reporting on VoIP traffic from geographically distant locations whose traffic cannot be brought to the VQManager sniffer interface(NIC).

VQManager supports .csv formats of the following CDR types:

- Vocal CDR Format
- Cisco CallTracker CDR Format
- Asterisk CDR Format
- Avaya S8700
- Cisco Call Manager 4.x and 5.x CDR
- Cisco Unified Communications Manager 6.1, 7.0 CDRs
- Cisco Call Manager 5.0 CDR/CMR
- Shoretel 6.1
- Swyx 6.0
- Tekelec 5.6
- PortaOne

On clicking the CDR import option, you will be led to a screen inside the product that helps you to import the CDR files either from the local machine, or on a remote machine:

- In the UI that opens, click the link "Import CDR File" icon available in the top-right corner
- If the CDR log file is available in your local computer, just browse to the file location and click "Import". This is suitable for the processing of small size files
- If the CDR log file is available in a remote machine, you can configure the server to download the CDR log files periodically from a remote location using FTP
- Click "Remote Location" and fill-in the details such as the hostname and IP of the machine, username and password to access the system
- Browse to the location of the file or the directory in which the CDR files are present, specify the periodic time interval (in seconds) during which the files are to be parsed and uploaded automatically and then click "Import". This is suitable for large files that need to be processed periodically. VQManager can identify new CDR log files in a directory and will automatically import the new content
- A log of all the imported CDR logs will be displayed as a list below

Parsing the CDR logs sent as Syslog Message

VQManager can be configured as a syslog server to receive CDRs as syslog messages from a call server eg. the CallManager Express can be configured to send the CDRs as syslog messages to VQManager. This method automates the sending of CDRs to VQManager and also enables one to have 'almost real-time' reporting of call traffic by configuring the sending of syslog messages(CDRs) in very short intervals. A syslog port (in the VQManager machine) listens to the syslog messages. The call server is configured to send the CDRs as syslog messages to this port.

On choosing this method you will be led to a screen that helps set VQManager as a syslog server:

- Click on the Add Syslog Server icon seen on the right hand side.
- Provide a Name to the Syslog Server you wish to configure
- Provide the Port number through which you want the VQManager product to

listen on for the syslog messages. By default the product listens for syslog messages on port 514.

- The IPAddress displayed is the default IP Address of the system in which the VQManager server is installed in. As VQManager listens on ANY address, no change would be required to be done on this field.
- Click on the " Add" button to configure the Syslog server.
- The Syslog servers list is displayed as a list with columns Name, IPAddress, Port, Status and Action.
- You can stop a Syslog server by clicking on the " Stop" icon under the Action column of the list. You can get the same Syslog server to start again by re-clicking the same icon, which would now be showing Play.
- Syslog Servers can be deleted by clicking on the dustbin "Delete" icon under the "Action" column of the list.

Syslog Servers

+ Add Syslog Server

Name
Port
IPAddress

1 - 1 of 1
⏪ ⏩
10
⏴ ⏵

Name ▲	IP Address	Port	Status	Action
Syslog Server-1	192.168.112.75	514	UP	

The Calendar - Setting the Client View Port

Contents

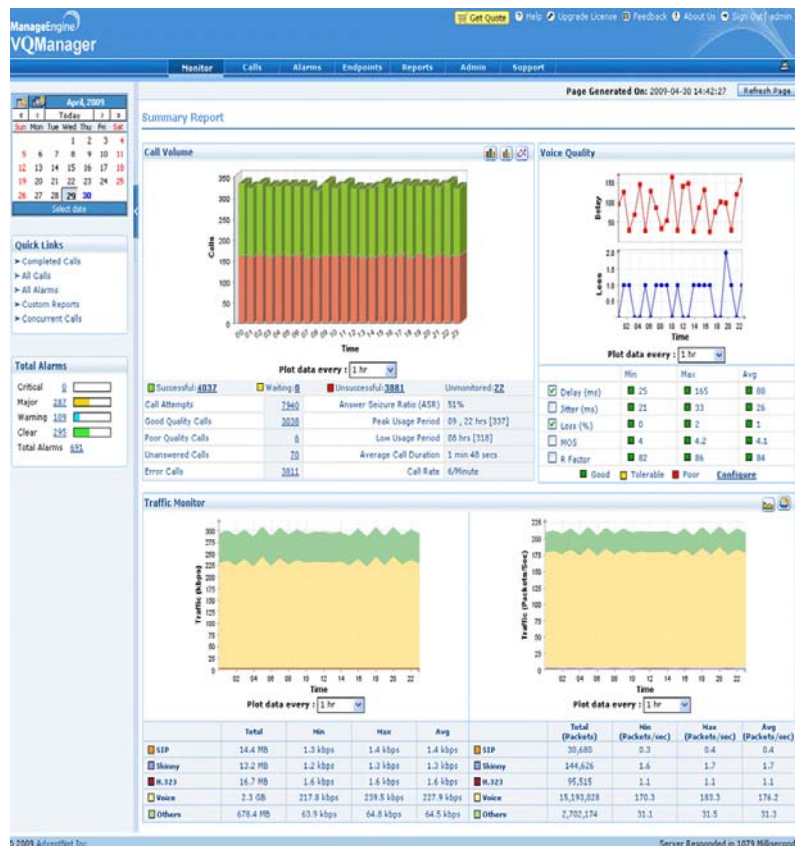
- Overview
- How to Set the Calendar

Overview

VQManager serves as a storehouse of data pertaining to the call details. The Administrator, however, would be inclined to view the data pertaining to a specific time period or the recent collection of data. The Calendar component is used to limit the amount of data that needs to be displayed in the client.

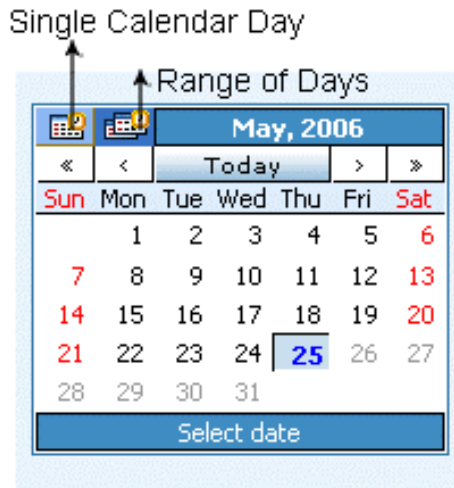
The Calendar component serves as the master control to set the view port in the client. That is, the value set in the calendar component will have its effect everywhere in the web interface except 'Reports' Tab, which has a different and independent Calendar Component.

The default view port is set as "Today" through the calendar. Only the data pertaining to the current day will be displayed in the client. If you wish to consider the data of, say, one week, you can set the calendar accordingly.



How to set the Calendar?

- On the left-hand side top-corner of the "Monitor" page, you will find the "Calendar" box.
- The calendar can be set to display data in two ways:
 - Data pertaining to a single, specific day
 - Data pertaining to a range of dates



To choose a single, specific day

- click the icon for "Single Calendar Day"
- click any desired date from the calendar
- by default, the dates for the current month are displayed in the calendar
- if you wish to view the data of previous months or years, click the buttons "<" "<<" on the left-hand side of the calendar respectively. Similarly, use the buttons ">" ">>" to navigate to months or years forward.

To choose a range of dates

- click the icon for "Range of Days"
- click any desired value from the drop-down menu for the field "Time" - Today, Yesterday, Last 7 days, Last 30 days or Custom. [Custom refers to selecting any desired range of dates]
- choose desired range of dates and also the time range in hours through the "From" and "To" fields
- click "Show"

The client view port is set through the calendar.

Note:

As stated above, the Calendar acts as the 'Master Control' to set the client view port for all the functionalities of VQManager. For instance, if you have set the calendar values to display the data of 'Last 7 days' and if you click to view certain data, say, 'Completed Calls', you will see the list of Completed Calls in the past seven days only.

The 'From' and 'To' time range selected in calendar component are applicable for the following four tabs only - Monitor, Calls, Alarms & Endpoints.

VQManager Web Interface - The Seven Tabs

Contents

- Overview
 - Topics Covered in this section
-

Overview

VQManager web interface contains the following seven tabs:

- **Monitor** - Provides a consolidated view of current state of the VoIP network as seen in the selected view port. It is more like a dashboard from where you can get to know about all the important parameters at a glance.
- **Calls** - Provides all necessary details about all the calls
- **Alarms** - When something goes wrong with the call quality, for instance, number of incomplete calls going beyond a particular value, the administrator can be alerted to take corrective action
- **Endpoints** - Provides reports based on the various VoIP endpoints
- **Reports** - Information on 'what is going on' in VoIP network and 'how it performs' are presented in the form of comprehensive, intuitive and informative reports
- **Admin** - Helps in performing various Administrative functions
- **Support** - Helps in troubleshooting issues with VQManager

Topics Covered in this section

The section provides detailed information about the seven tabs of VQManager web interface as stated above along with the details regarding how to work with VQManager.

Monitoring Vital Parameters

Contents

- Overview
 - Summary Report view
-

Overview

The "Monitor" tab is the first UI that appears after connecting the Web Client. It provides a consolidated view of current state of the VoIP network as seen in the selected view port. It is like a dashboard from where you can get to know about all the important parameters at a glance - that is, everything needed to monitor the health of your VoIP infrastructure from a single screen.

The Monitor tab has two main view: "Summary Report"

Summary Report View

This view is loaded by default and shows a summary of vital quality parameters over a user-defined time period. By default, the summary view shows the present day's call details. You can have a summarized view of calls that have happened over a defined time period by selecting the required date range from the calendar component on the top left hand corner.

The "Summary Report" has:

- The Call Volume graph showing the volume of calls that were successful or unsuccessful, of good or poor quality, the peak and low usage periods, the Average Call duration and overall ASR(Answer Seizure Ratio) etc..
- The Voice Quality graph that shows snapshot of the QoS metrics with their Min, Max and Avg values and whether good, tolerable or poor as defined by the user.
- The Traffic Monitor graph showing a split-up of bandwidth for each VoIP traffic component
- The Total Alarms section shows a summary of alarms generated over the chosen time-frame.

Call Volume Graph

- Displays the statistics of all the calls that were initiated in the chosen time frame as set in the calendar.
- The bar graph has the green areas representing the successful calls while the red areas denote unsuccessful calls.
- Provides the number of call attempts, successful, unsuccessful and waiting as a linked number. When these linked number are clicked you can view the information of the respective calls.
- The successful calls are divided into calls based on quality - Good and Poor quality calls. Calls with **MOS** (Mean Opinion Score) greater than 3.1 are classified as Good Quality Calls. Calls with MOS less than 3.1 are marked as Poor Quality Calls
- The unsuccessful calls are further divided into Unanswered calls and Error calls. Calls that were not answered by the user (user busy, user not available

etc.,) fall into the Unanswered Call category. Other calls that failed due to errors in server or client are marked as Error Calls

- The number of Unmonitored Calls during the chosen time-period is listed. Unmonitored calls are those that VQManager has abruptly stopped monitoring - this could be due to an abrupt stop and restart of the VQManager server, or because there were no voice packets that were received for a continuous duration(30 seconds) of time
- Answer Seizure Ratio(ASR) - ratio of successfully connected calls to attempted calls is displayed
- Lists the time period at which there were a maximum number of calls - its peak usage ; Similarly, time period at which the call volume was minimum - low usage
- Provides the average call duration time across all the calls during the selected time period
- The Call Rate is provided showing the rate at which the calls are being made in the VoIP network

Output Formats

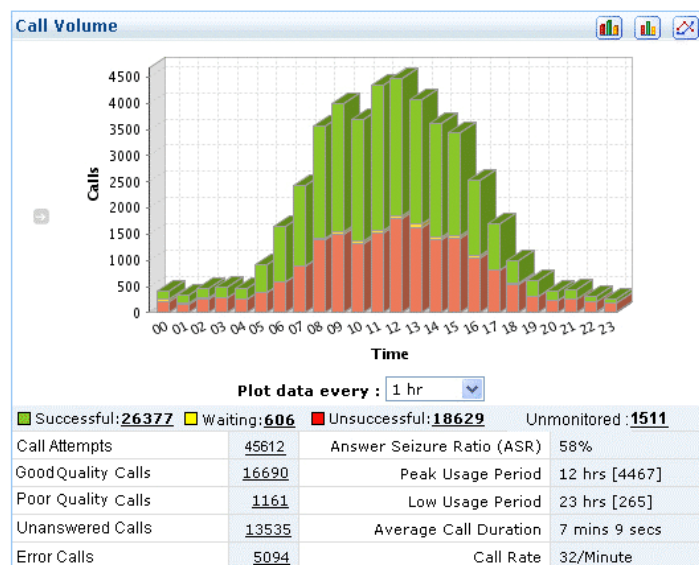
- The call volume graph can be generated in three formats - a simple bar diagram, a three-dimensional bar diagram and a simple line graph
- Click the respective icon on the top-right corner of 'Call Volume Graph' to get the respective view

Choosing the Time Interval

The Call Volume graph represents a summary of the calls that have happened over the time period as chosen in the calendar. You can split this time-period into intervals according to your requirement.

For example, if you have set the calendar to display past one month's call summary, you have the option of splitting the graph into intervals of 7 days (4 bars), or 15 days (2 bars) or for the whole month (1 bar) itself.

You can select the required time-interval using the drop-down "Plot data every" available under the graph.



Voice Quality Graph

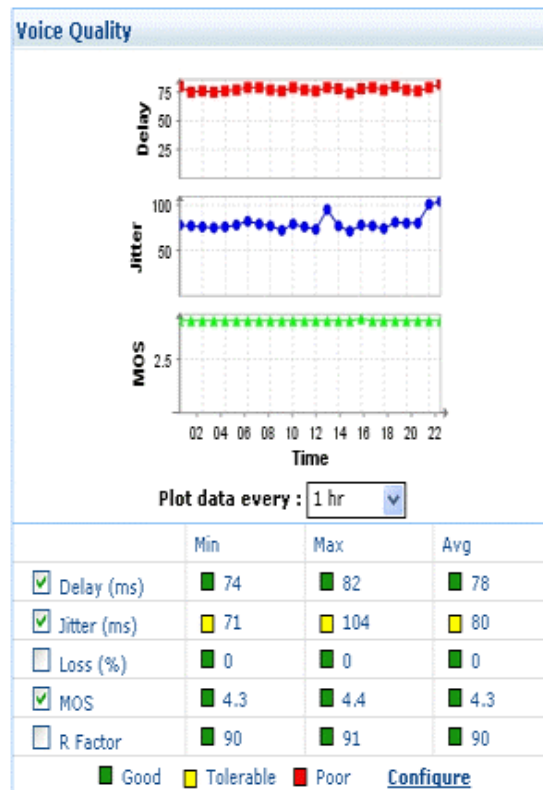
- Provides trends of vital quality parameters – Delay, Jitter, Packet Loss, MOS and R Factor over the defined time period as set in the calendar.
- A table of information shows the "Min", "Max" and "Avg" values for each quality parameter and also which of these values were "Good", "Tolerable" or "Poor" as defined by the user.
- Trend graphs are displayed for each parameter. Upto three graphs can be displayed at the same time by selecting the respective check-box next to each parameter. On reaching the maximum of three graphs displayed, you need to deselect parameters to have the required additional parameter's trend graph displayed.
- Each individual QoS value plot on the graph can be clicked to provide details of the calls that have contributed to the respective QoS value.

Choosing the Time Interval

The Voice Quality graph represents a summary of the QoS statistics of the calls that have happened over the time period as chosen in the calendar. You can split this time-period into intervals according to your requirement.

For example, if you have set the calendar to display past one month's call summary, you have the option of splitting the graph into intervals of 7 days (4 plot-points), or 15 days (2 plot-points) or for the whole month (1 plot-points) itself.

You can select the required time-interval using the drop-down "Plot data every" available under the graph.



Configure QoS

The QoS metrics can be customized according to the your VoIP quality requirements. The system administrators can define the threshold value for the Delay, Jitter, Packet Loss, MOS and R Factor value. The minimum and maximum value of tolerable value helps in determining the good and poor quality score. QoS metrics below the minimum threshold level would be classified as "Good" while the metrics exceeding the maximum threshold value will be termed "Poor".

To configure QoS metrics tolerable range

Go to "Monitor" Tab and get to the Summary Report view
 Click on the "Configure" link, below the voice quality graph
 A screen to "Configure QoS Min/Max thresholds" pops up
 Fill in the tolerable range of various metrics like Delay, Jitter, Packet Loss, MOS
 Click on "Update" button to confirm the values

Note: QoS metrics below the minimum threshold level would be classified as "Good" while the metrics exceeding the maximum threshold value will be termed "Poor". However for MOS metrics vice versa of this rule will apply.

Traffic Monitor Graph

- Helps in finding out the traffic details (Bandwidth utilization) of the network managed by VQManager in a specific time interval as set in the calendar.
- The traffic information is plotted in two sets of graphs. One set depicts the total size(in kbps) of the packets transmitted and the other set provides the total number of packets transmitted per second(packets/sec).
- The bandwidth utilized by various components such as SIP, Skinny, H.323, Voice and Others are depicted each by individual graphs.
- A table of information shows the " Min", "Max" and "Avg" values for each traffic component.

Output Formats

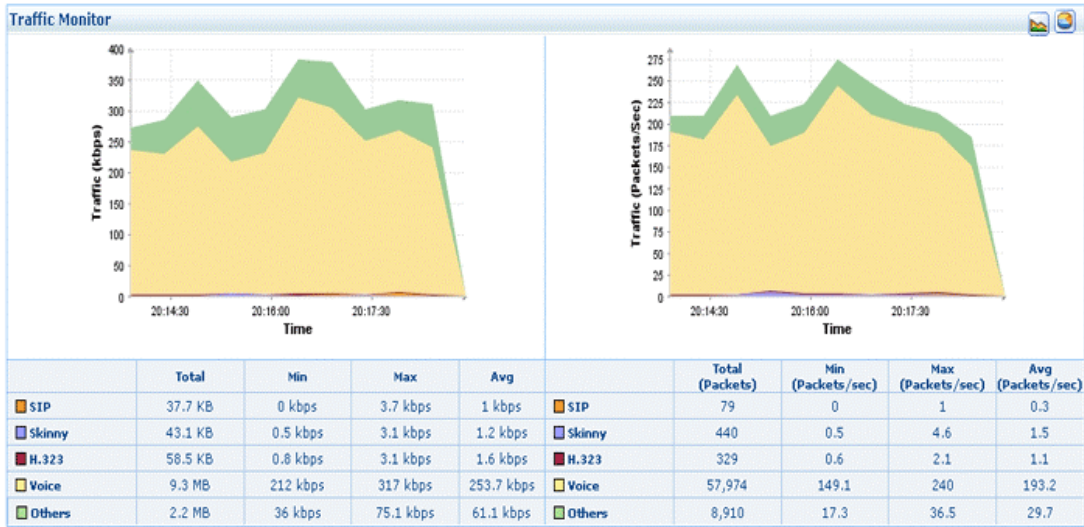
- The Traffic Monitor graph can be generated in two formats - an area graph and a three-dimensional pie diagram.
- Click the respective icon on the top-left corner of 'Traffic Monitor Graph' to get the respective view

Choosing the Time Interval

The Traffic Monitor graph represents the bandwidth summary of the calls made during the time-period as set in the calendar. You can split this time-period into intervals according to your requirement.

For example, if you have set the calendar to display past one month's call summary, you have the option of splitting the graph into intervals of 7 days (4 plot-points), or 15 days (2 plot-points) or for the whole month (1 plot-point) itself.

You can select the required time-interval using the drop-down "Plot data every" available under the graph.



Total alarms

- This summary of alarms is found in the left side of the UI, below the "Quick Links".
- Provides the summary of alarms generated for the time period as set in the calendar. All categories of alarms: "Clear", "Warning", "Major" and "Critical" are shown including the "Total Alarms" generated in the selected time period.
- You can view more details of respective alarms by clicking on the linked number next to the alarm name.

Calls Tab - All about Calls

Contents

- Overview
 - Active Calls Summary
 - Call Details
 - Calls by Status
 - History Data - Multiday Calls Summary
-


Overview

The Calls tab provides information on all the calls that have happened in the time duration as set in the calendar. Detailed quality metrics and trends for all calls are displayed through:

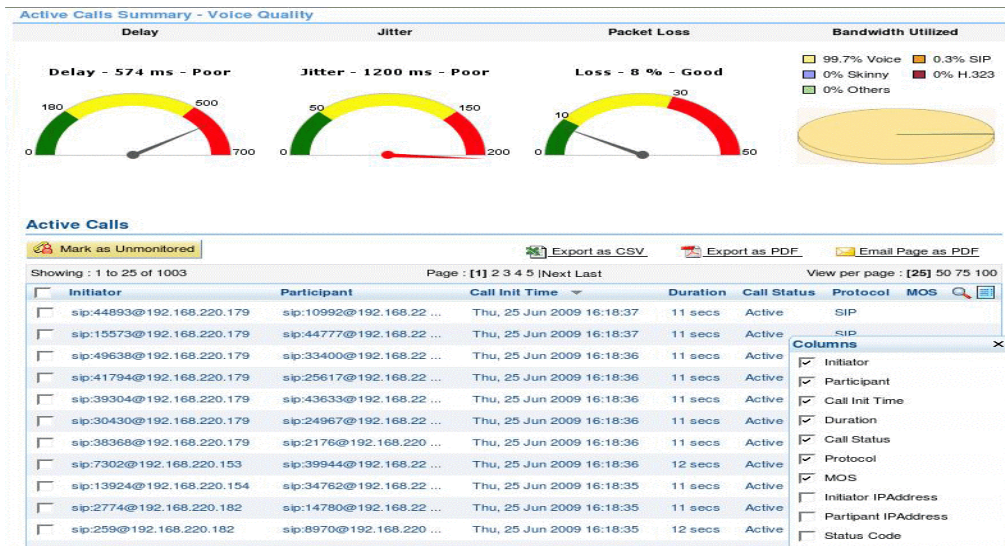
- The Active Calls Summary providing QoS details and bandwidth utilization for calls presently active
- The Call Details showing further details on individual calls
- The Calls by Status summary, which is a listing of calls based on their types eg. Error calls, Poor Quality Calls etc.

Active Calls Summary

- This is the first UI that opens in the calls tab showing the details of the active calls happening in the network.
- The QoS of the active calls are depicted in the form of intuitive charts. The average values of all the QoS parameters such as Delay, Jitter and Packet Loss are plotted in the chart.
- A Bandwidth utilized graph is also provided that shows the most recent bandwidth utilization in the network. The bandwidth usage is split into SIP, Skinny, H.323, Voice and Others. On rolling the mouse pointer over the different areas in the pie chart, respective volume of packets for the bandwidth components are shown in kbps.
- By default, this page gets reloaded every 20 seconds to show the latest Active calls that are happening in the network. The user can configure this refresh rate. This option is found in the top left hand side of the UI just below the line of tabs. Next to the "Refresh Every" field click on the edit icon next to the linked text entry. Select the required refreshing time interval (refresh rate) from the drop-down list that appears.
- Below the QoS charts is a list of all the current active calls in the network. Information such as the Initiator of the call, call initiation time, Duration, Status Code, and MOS of the call are displayed by default in the table.
- One can mark any stale/frozen calls in this list as unmonitored calls that wrongly appear as active in this list. This option is found above the list through the button "Mark as Unmonitored".
- You can view other details such as participant/initiator's ip, participant/initiator's url, call initialization time, duration, Call Status, Status

Code, MOS. To view the additional columns, click the column chooser icon  present at the top right of the 'Active Calls' table. Click "Save" after selecting the required columns.

- This list can be arranged by ascending or descending order of the Call Initialization Time and other column fields. Clicking on the column heading, that you want the list to be sorted according to, does this.
- The Active Calls list can be exported as a PDF or CSV file or emailed as a PDF attachment to a number of E-mail Ids. This can be done through the respective icons - CSV icon, PDF icon and mail icon, found on the right-hand side just above the Active Calls list.
- The list can be searched for a particular call by providing either Initiator / Participant / Call Status / Status Code. Click on the lens icon found on the extreme right hand side of the list's header. Text-boxes will appear in which you can provide the Initiator / Participant / Call Status / Status Code to search for the endpoint. After providing the search criteria, click on the Go button found below the lens icon to search for the call according to the provided search term/terms.



Note: Drill down to Call Details views from Active calls is not possible, as the Active Calls information is fetched from the Cache. Can view the call details once the call is completed.

Call Details

- On clicking any Initiator of a call in any of the Call lists, you are brought to details of that particular call. This UI shows a graphical display of the call QoS trends, participating endpoint details, CODEC details and a pictorial representation of the packets exchanged during the call.
- The Call Trend graph is similar to the Voice Quality graph in the Monitor tabs Summary Report View. All the QoS parameters such as Delay, Jitter, Packet Loss, and MOS are plotted in the graph. This shows the trends for the various QoS parameters for the duration of the call.

- To the right of the Call Trend graph, the details of the call and the participants of the call are displayed. Call details such as Start Time, Duration, Call Identifier and Call Status are shown. The Call Identifier is provided for SIP-based and H.323-based calls and is a unique identifier for each call. The linked character set shown for the Call Identifier is displayed as a truncated item. To view the full Call Identifier, click on the displayed Call Identifier to open up a dialogue box having the Call Identifier in full. Endpoint details such as Phone ID, Name, Skinny/SIP/H.323 URL, IP Address, Media Port, Octets and Packets are shown.
- On clicking the linked item View Trend found below the Name of the participants, you can see the individual QoS trend graphs for each participant during the call.
- Codec Details give information about the Codec used in the call along with its characteristics such as Bits per sample, Frame Size, RTP Clock Rate, Payload Type, Sampling Rate, Packet Size and No. of Channels.
- The Call Flow ladder diagram provides a pictorial representation of the packets exchanged during the call initiation, progress and end. It plots all the SIP, Skinny and H.323 requests that took place from call start to call end. This is useful for debugging error calls that failed due to some unknown reasons
- Call Trace provides summarized information for each of the SIP/ Skinny/ H.323 and RTCP packets that were exchanged during the call process. Details of Capture Time, Protocol, Status, Code, Source Port, Destination and Destination Port are provided for each packet.
- You can see the raw SIP, Skinny and H.323 packet details along with their Call Trace information by clicking on each packet in the Call Flow diagram. This information is displayed below the Call Flow diagram. "Tunnelled" H.323 packets are represented in the call-flow diagram as a three-dimensional box.

Call Details[1001 - 1002]

Call Trend

Plot data every: 1 min

	Min	Max	Avg
<input checked="" type="checkbox"/> Delay (ms)	2	22	11
<input checked="" type="checkbox"/> Jitter (ms)	0	20	9
<input type="checkbox"/> Loss (%)	0	0	0
<input checked="" type="checkbox"/> MOS	4.4	4.4	4.4
<input type="checkbox"/> R Factor	93	93	93

■ Good
 ■ Tolerable
 ■ Poor

Call Details

Start Time: Apr 28, 2009 7:57:21 PM
Duration: 4 mins 14 secs

Call Identifier: -

Call Status: **Active**

Phone ID	1001	1002
Name	suresh	sujith
Skiny URL	1001	1002
IP Address	10.10.10.16	10.10.10.14
Media Port	16480	16636
Octets	2.7 MB	3.3 MB
Packets	16,572	20,025

CODEC Details

Name	G711mu-law-64	Payload Type	4
Bits per sample	2	Sampling Rate	8000 Hz
Frame Size	0 ms	Packet Size	20 ms
RTP Clock Rate	8000 Hz	No. of Channels	1

Calls by Status

Error Calls

Initiator	Participant	Call Init Time	Duration	Call Status	Status Code	Protocol Name	MOS
10.10.10.11	10.10.10.1	Thu, 4 Sep 2008 16:00:00	NA	StartTone Reorder	0x82 0x25	SKINNY	
10.10.10.11	10.10.10.1	Thu, 4 Sep 2008 14:40:22	NA	StartTone Reorder	0x82 0x25	SKINNY	
subash	sip:8009@voip-lin2	Thu, 4 Sep 2008 11:05:46	NA	Temporarily Unavaila ...	480	SIP	
10.10.10.11	10.10.10.1	Thu, 4 Sep 2008 13:20:44	NA	StartTone Reorder	0x82 0x25	SKINNY	
subash	sip:8009@voip-lin2	Thu, 4 Sep 2008 11:05:04	NA	Temporarily Unavaila ...	480	SIP	
10.10.10.11	10.10.10.1	Thu, 4 Sep 2008 12:00:32	NA	StartTone Reorder	0x82 0x25	SKINNY	
subash	sip:5697@voip-lin2	Thu, 4 Sep 2008 10:50:43	NA	Temporarily Unavaila ...	480	SIP	
10.10.10.11	10.10.10.1	Thu, 4 Sep 2008 10:48:38	NA	StartTone Reorder	0x82 0x25	SKINNY	
subash	sip:madu@voip-lin2	Thu, 4 Sep 2008 10:49:30	NA	Temporarily Unavaila ...	480	SIP	
10.10.10.9	10.10.10.1	Thu, 4 Sep 2008 16:00:00	NA	StartTone Reorder	0x82 0x25	SKINNY	

- This listing is found as a separate menu bar on the left hand pane of the UI below the Quick Links section. Details of all the Error Calls, Unanswered Calls, Good Quality Calls, Poor Quality Calls, Unmonitored Calls and All Calls can be viewed by clicking the respective links in the menu bar
- Error Calls are those that did not connect ("Not Found", "Temporary Unavailable", "Cancelled") or those which failed abruptly after connecting(server shutdown, connection failed etc.)
- Unanswered Calls are those in when the called party does not answer. These could be because the called party is on another call ("User busy") or simply does not answer
- VQManager distinguishes from Good and Poor Quality calls based on the user's setting in the Monitor tab in the "Configure" section of the Voice Quality graph. By default, calls with **MOS** (Mean Opinion Score) greater than 3.1 are classified as Good Quality Calls. Those calls with MOS less than 3.1 are marked as Poor Quality Calls
- Unmonitored calls are those that VQManager has abruptly stopped monitoring - this could be due to:
 - an abrupt stop and restart of the VQManager server, such calls are identified by status code "8001"
 - an abrupt stop and restart of the VQManager sniffer, such calls are identified by status code "8002"
 - Signaling flow interruption as configured in the "Advanced settings" of the sniffer configuration. Such calls are identified by status code "8003"
 - User manually marking a call as "Unmonitored" in the "Active calls" section of the "calls" tab. These calls are identified by status code "8000".
 - Concurrent call license limiting the number of calls that are monitored by the VQManager server. These calls are identified by the status "8004"
- The last link in the Calls by Status menu bar shows the details of all the calls that have taken place in the time duration as set in the calendar.

History Data - Multiday Calls Summary

- The 'Multiday Calls Summary' view provides a summary of the calls data across multiple days. This can be viewed for a range of days like 'Last 7 days', 'Last 30 days' or a 'Custom' timeperiod.
- Choose a required time period from the 'Calendar' component on the top left of the 'Calls' tab and click on 'Show'. This will bring up a table with the call count details of all the categories of calls, namely Total Calls, Successful, Unsuccessful, Good Quality, Poor Quality, Waiting for each day in the chosen time period. To view the list of the calls under any category for any particular day, click on the corresponding number link in the respective call category.
- The waiting calls are the number of calls that remain or remained in waiting mode at the chosen time frame. Calls in waiting mode are those that have been initiated but are yet to get connected with the called party.
- This list also provides the averaged values of the Answer Seizure Ratio (ASR) in % and MOS for each day in the list.
- Additional columns, namely, Unanswered, Error, Unmonitored, ALOC(min), Call Rate(/Hour), Delay, Jitter, Packet Loss can also be chosen from the 'Column Chooser' component available in the top right side of the list.
- The list can also be extracted as a 'CSV', 'PDF' file or can be e-mailed as a 'PDF' attachment to desired recipients.

Alarms Tab - Alerting the Administrator

Contents

- Overview
 - Creating Alarm Profiles
 - Editing Alarm Profiles
 - Deleting Alarm Profiles
 - Pre-Created Alarm Profiles
 - Total Alarms
-

Overview

When something goes wrong with the call quality, it is important that the administrator is alerted on the same in order to initiate some corrective action. VQManager can generate alarms when a particular vital parameter goes beyond a particular value - for instance, number of incomplete calls going beyond a particular value. You can specify the criteria based on which the alarms are to be generated. This can be done by creating Alarm Profiles.

- The Alarms Tab displays the list of all the available alarm profiles, alarms generated in the network with information about the reason for the alarm (for instance, ASR less than a particular value), the timestamp of the alarm and its severity.
- Alarms tab displays two views - Summary View and Detailed View. Summary View displays the list of all Alarm Profiles. Detailed View provides the list of all the individual alarms.

Creating Alarm Profiles

As stated above, Alarm Profiles are created to define the condition based on which alarms are to be generated. Alarms can be generated when the VoIP network suffers problems in any or all of the following aspects:

- **Incomplete Calls** - when calls go incomplete consecutively and when the number of such consecutive incomplete calls go beyond a certain value
- **Average Length of Call (ALOC)** - when the ratio between the sum of the time duration of all successful calls and the number of all successful calls goes below or beyond the desired value
- **Answer Seizure Ratio (ASR)** - when the ratio between successfully connected calls to attempted calls goes beyond the desired value
- **Average Answer Delay**- when the difference in time duration between

successful initiation of call and the time taken by the person on the other end to actually attend the call (i.e. delay in answering the call), goes beyond a particular value

- **Concurrent calls**- An alarm can be generated if the number of concurrent calls goes beyond a certain value for a certain number of times
- **Voice Bandwidth Utilization** - when the call traffic in the network goes beyond a particular limit making heavy voice bandwidth utilization
- **Call Set up Time** - The time from the initiation of a call request to the beginning of the call ringing tone received. An alarm is raised when the call set up time is more than the desired delay (in seconds)
- **SIP Error Codes** - An alarm is triggered when the number of calls with same or similar SIP error codes is greater than the specified number of calls
- **Jitter** - An alarm can be generated when jitter values increases beyond a specified milliseconds
- **Packet Loss** - An alarm is raised when the packet loss is greater than the specified percentage
- **Call Volume** - An alarm can be triggered when the call count is below or more than the desired limits in the given time interval
- **Disconnect Time** - An alarm can be generated when the number of calls with same disconnect time is greater than the specified number of calls
- **Talk Time** - An alarm can be generated when the Total Talk time is less than or greater than the talk time value defined by the administrator
- **R Factor** - When the R Factor less than or between the specified values by the administrator, an alarm can be triggered off to inform the administrator
- **MOS** - An alarm can be triggered when the MOS value is less than or within the range specified by the administrator
- **MOS Trend** - The trend of MOS over a period of time can be taken as the basis for generating an alarm. For example, if the MOS trend during a period of say, three days falls below a certain range specified by the administrator, an alarm can be generated

While specifying the conditions for generating Alarms, you can also set the severity for the alarm, For every alarm generation condition, you can have any of the three levels of severity - Critical, Major and Warning. Even within one category (say incomplete calls), you can configure three different alarms, one for each severity and you can define different threshold limit for each severity.

Add Alarm Profile

Alarm Profile Name * based on ▾

For * consecutive incomplete calls,
 generate a ▾ alarm with message *

Repeat alarm for same intervals

Send E-mail to :

Send SNMP Trap

For * consecutive incomplete calls,
 generate a ▾ alarm with message *

Send E-mail to :

Send SNMP Trap

For * consecutive incomplete calls,
 generate a ▾ alarm with message *

Send E-mail to :

Send SNMP Trap

To create an Alarm Profile,

- Go to "Alarms" tab
- Click the link "Add Alarm Profile"
- In the 'Add Alarm Profile' UI that opens, provide a "Name" for the new profile in the text field
- Choose the base condition for generating the Alarm from the drop-down menu. There are several options such as Incomplete Calls, ALOC, ASR, Average Answer Delay, Voice Bandwidth Utilization etc. Choose the desired option
- Define "**Time Filter**" criteria - that is the data getting accrued during a particular time period that has to be considered for generating the alarm. For example, one would like to generate the alarms for the abnormal conditions happening only during business hours. Or some would not like to generate alarms for the happenings during the weekends. For all such cases, you can define 'Time Filter' criteria. To define this, click the link "Time Filter" present on the right hand side corner of the 'Add Alarm Profile' UI. In the UI that opens,
 - set the 'Sampling Interval' - that is the time interval at which the

VOManager database has to be queried for details. You can specify the time interval in minutes, hours or days.

- set the 'Time Filter' - that is the data that got accrued during which time span has to be considered - whole day or business hours or non-business hours or your own custom time period
- if you do not wish to consider the data accrued during weekend (Saturday & Sunday), select the check box "Exclude Weekends"
- click "Set"
- Define the "Threshold" value for the chosen condition. When data touches or goes beyond the threshold value specified, alarm will be generated

Defining Threshold Values

For Incomplete Calls

- In the textfield, specify the number of consecutive incomplete calls beyond which you would like to receive an alarm. Choose the severity which you would like to assign (Critical/Major/Warning). In addition, specify a meaningful message for the alarm. For example: "Incomplete Calls exceeded 10". This message would be highly helpful in understanding the type of problem when you receive the alarm
- You also have the option to generate repeat alarms when the number of consecutive calls reach the multiples of the threshold value. For example, if you have set 10 as the threshold value for incomplete calls, the alarm will be generated when 10 consecutive calls go incomplete. If the problem continues and number of incomplete calls grow further and it crosses 20 (the multiple of 10 which was set as the threshold value), another alarm would be generated. This would continue for 30, 40 and so on. If you want to have this option, just check the checkbox "Repeat Alarm for same intervals". This option is available only for 'Critical' category alarms. By default, this option is enabled.
- When a successful call comes after a number of consecutive incomplete calls, a Clear Alarm will be generated with the message "A successful call received after XX consecutive incomplete calls". However, it is to be noted that a Clear Alarm for incomplete calls will be generated for a profile, only if the profile had generated at least one alarm.
- You can make use of any or both the remaining two severities (Major/Warning) and define different threshold values for them. In such a case, click the link "Add Threshold" and repeat the above steps
- **Email Notification:** You have the option of automatically sending an email to notify the desired recipients when an alarm is generated. To use this option, you need to enable the option "Send Email to" and specify the email id in the textfield. Once you enable this option, email notification would be sent to the specified recipients upon the generation of the particular alarm. The email message will contain details such as Subject, Alarm ProfileName, severity, alarm message, time of creation of the alarm and other details

- **SNMP Trap Forwarding:** The administrator can enable the VQManager to generate SNMP traps on specific alarms. This will help in integrating the VQManager alarms with any higher-level NMS like ManageEngine OPManager. The VQManager allows the administrator to set up the list of SNMP trap listeners to forward the SNMP traps. By specifying the required SNMP parameters (viz., hostname, port, community, version etc.), the embedded VQManager SNMP agent can generate appropriate SNMP traps and forward to the defined entries. Currently the VQManager SNMP agent can generate a SNMP V1 and SNMP V2C traps.

Note: The incomplete error calls does not include "**Request Terminated**" calls (SIP error code: **487**).

For ALOC

- In the text field, specify the ALOC value in seconds (sum of the duration of all successful calls divided by the number of all successful calls) below or beyond which you want to generate the alarm. In the drop-down menu, choose '<' for ALOC below the specified value and '>' for ALOC going beyond the specified value. In the adjacent text field define the number of calls beyond which the alarms is to be generated. Choose the severity which you would like to assign (Critical/Major/Warning). In addition, specify a meaningful message for the alarm. For example: "ALOC falling below 30 seconds for more than 5 calls". This message would be highly helpful in understanding the type of problem when you receive the alarm.
- You can make use of any or both the remaining two severities (Major/Warning) and define different threshold values for them. In such a case, click the link "Add Threshold" and repeat the above steps.
- **Email Notification:** You have the option of automatically sending an email to notify the desired recipients when an alarm is generated. To use this option, you need to enable the option "Send Email to" and specify the email id in the text field. Once you enable this option, email notification would be sent to the specified recipients upon the generation of the particular alarm. The email message will contain details such as Subject, Alarm Profile Name, severity, alarm message, time of creation of the alarm and other details.
- **SNMP Trap Forwarding:** The administrator can enable the VQManager to generate SNMP traps on specific alarms. This will help in integrating the VQManager alarms with any higher-level NMS like ManageEngine OPManager. The VQManager allows the administrator to set up the list of SNMP trap listeners to forward the SNMP traps. By specifying the required SNMP parameters (viz., hostname, port, community, version etc.), the embedded VQManager SNMP agent can generate appropriate SNMP traps and forward to the defined entries. Currently the VQManager SNMP agent can generate a SNMP V1 and SNMP V2C traps.

For ASR

- In the text field, specify the ASR value in percentage (the ratio between successfully connected calls to attempted calls) below which you want to generate the alarm. In the adjacent text field define the number of calls

beyond which the alarms is to be generated. Choose the severity which you would like to assign (Critical/Major/Warning). In addition, specify a meaningful message for the alarm. For example: "ASR falling below 30%". This message would be highly helpful in understanding the type of problem when you receive the alarm.

- You can make use of any or both the remaining two severities (Major/Warning) and define different threshold values for them. In such a case, click the link "Add Threshold" and repeat the above steps.
- **Email Notification:** You have the option of automatically sending an email to notify the desired recipients when an alarm is generated. To use this option, you need to enable the option "Send Email to" and specify the email id in the text field. Once you enable this option, email notification would be sent to the specified recipients upon the generation of the particular alarm. The email message will contain details such as Subject, Alarm Profile Name, severity, alarm message, time of creation of the alarm and other detail.
- **SNMP Trap Forwarding:** The administrator can enable the VQManager to generated SNMP traps on specific alarms. This will help in integrating the VQManager alarms with any higher-level NMS like ManageEngine OPManager. The VQManager allows the administrator to set up the list of SNMP trap listeners to forward the SNMP traps. By specifying the required SNMP parameters (viz., hostname, port, community, version etc.), the embedded VQManager SNMP agent can generate appropriate SNMP traps and forward to the defined entries. Currently the VQManager SNMP agent can generate a SNMP V1 and SNMP V2C traps.

For Average Answer Delay

- In the text field, specify the maximum permissible Average Answer Delay value in seconds (the difference in time duration between successful initiation of call handling by the device and the time taken by the person on the other end to actually attend the call (i.e. delay in answering the call)) beyond which you want to generate the alarm. Also enter the number of calls beyond which the alarms is to be generated. Choose the severity which you would like to assign (Critical/Major/Warning). In addition, specify a meaningful message for the alarm. For example: "Average Answer Delay going beyond 40 seconds". This message would be highly helpful in understanding the type of problem when you receive the alarm.
- You can make use of any or both the remaining two severities (Major/Warning) and define different threshold values for them. In such a case, click the link "Add Threshold" and repeat the above steps.
- **Email Notification:** You have the option of automatically sending an email to notify the desired recipients when an alarm is generated. To use this option, you need to enable the option "Send Email to" and specify the email id in the text field. Once you enable this option, email notification would be sent to the specified recipients upon the generation of the particular alarm. The email message will contain details such as Subject,

Alarm Profile Name, severity, alarm message, time of creation of the alarm and other details.

- **SNMP Trap Forwarding:** The administrator can enable the VQManager to generate SNMP traps on specific alarms. This will help in integrating the VQManager alarms with any higher-level NMS like ManageEngine OPManger. The VQManager allows the administrator to set up the list of SNMP trap listeners to forward the SNMP traps. By specifying the required SNMP parameters (viz., hostname, port, community, version etc.), the embedded VQManager SNMP agent can generate appropriate SNMP traps and forward to the defined entries. Currently the VQManager SNMP agent can generate a SNMP V1 and SNMP V2C traps.

For Concurrent Calls

- In the first text field, enter the value of 'number of concurrent calls' beyond which the alarm is to be generated. Also enter the value for the number of occurrences in the next input field. For example : "Number of concurrent calls greater than 50 and occurrences more than 5". This condition will generate an alarm if the number of concurrent calls goes beyond 50, 5 times. Choose the severity you would like to assign and also enter an appropriate message. This message would be highly helpful in understanding the type of problem when you receive the alarm. The default sampling interval duration for concurrent calls based alarms will be 5 minutes.
- You can make use of any or both the of remaining two severities (Major/Warning) and define different threshold values for them. In such a case, click the link "Add Threshold" and repeat the above steps.
- **Email Notification:** You have the option of automatically sending an email to notify the desired recipients when an alarm is generated. To use this option, you need to enable the option "Send Email to" and specify the email id in the text field. Once you enable this option, email notification would be sent to the specified recipients upon the generation of the particular alarm. The email message will contain details such as Subject, Alarm Profile Name, severity, alarm message, time of creation of the alarm and other details.
- **SNMP Trap Forwarding:** The administrator can enable the VQManager to generate SNMP traps on specific alarms. This will help in integrating the VQManager alarms with any higher-level NMS like ManageEngine OPManger. The VQManager allows the administrator to set up the list of SNMP trap listeners to forward the SNMP traps. By specifying the required SNMP parameters (viz., hostname, port, community, version etc.), the embedded VQManager SNMP agent can generate appropriate SNMP traps and forward to the defined entries. Currently the VQManager SNMP agent can generate a SNMP V1 and SNMP V2C traps.

For Call Set-up Time

- In the text field, specify the call setup time in seconds and also set the number of calls beyond which you would like to receive an alarm. Choose

the severity which you would like to assign (Critical/Major/Warning). In addition, specify a meaningful message for the alarm. For example: "Call Set up Time is more than 10 seconds for more than 5 calls". This message would be highly helpful in understanding the type of problem when you receive the alarm

- You can make use of any or both the remaining two severities (Major/Warning) and define different threshold values for them. In such a case, click the link "Add Threshold" and repeat the above steps
- **Email Notification:** You have the option of automatically sending an email to notify the desired recipients when an alarm is generated. To use this option, you need to check the option "Send Email to" and specify the email id in the text field. Once you enable this option, email notification would be sent to the specified recipients upon the generation of the particular alarm. The email message will contain details such as Subject, Alarm Profile Name, severity, alarm message, time of creation of the alarm and other details
- **SNMP Trap Forwarding:** The administrator can enable the VQManager to generate SNMP traps on specific alarms. This will help in integrating the VQManager alarms with any higher-level NMS like ManageEngine OPManager. The VQManager allows the administrator to set up the list of SNMP trap listeners to forward the SNMP traps. By specifying the required SNMP parameters (viz., hostname, port, community, version etc.), the embedded VQManager SNMP agent can generate appropriate SNMP traps and forward to the defined entries. Currently the VQManager SNMP agent can generate a SNMP V1 and SNMP V2C traps

For Voice Bandwidth Utilization

- In the text field, specify the Voice Bandwidth Utilization value and select the units from drop down menu (Kbps/Mbps/Gbps) beyond which you want to generate the alarm. Choose the severity which you would like to assign (Critical/Major/Warning). In addition, specify a meaningful message for the alarm For example: "Voice Bandwidth Utilization going beyond 100 mbps". This message would be highly helpful in understanding the type of problem when you receive the alarm.
- You can make use of any or both the remaining two severities (Major/Warning) and define different threshold values for them. In such a case, click the link "Add Threshold" and repeat the above steps.
- **Email Notification:** You have the option of automatically sending an email to notify the desired recipients when an alarm is generated. To use this option, you need to enable the option "Send Email to" and specify the email id in the text field. Once you enable this option, email notification would be sent to the specified recipients upon the generation of the particular alarm. The email message will contain details such as Subject, Alarm Profile Name, severity, alarm message, time of creation of the alarm and other details.

- **SNMP Trap Forwarding:** The administrator can enable the VQManager to generate SNMP traps on specific alarms. This will help in integrating the VQManager alarms with any higher-level NMS like ManageEngine OPManger. The VQManager allows the administrator to set up the list of SNMP trap listeners to forward the SNMP traps. By specifying the required SNMP parameters (viz., hostname, port, community, version etc.), the embedded VQManager SNMP agent can generate appropriate SNMP traps and forward to the defined entries. Currently the VQManager SNMP agent can generate a SNMP V1 and SNMP V2C traps.

For SIP Error Code

- In the text field, specify the SIP error code for which you would like to raise the alarm. For raising the alarm for the exact SIP error code choose 'equals' in the drop down menu or use 'like' to get alarms for SIP error code from similar series. There is also provision to 'exclude' SIP code in 'like' condition. Specify the number of calls beyond which you would like to receive an alarm. This will raise the alarm when the number of calls with similar / same SIP error code are beyond the tolerable number of calls specified by the administrator. Choose the severity which you would like to assign (Critical/Major/Warning). In addition, specify a meaningful message for the alarm. For example: "More than 50 calls have Sip Error Code: 400". This message would be highly helpful in understanding the type of problem when you receive the alarm.
- You can make use of any or both the remaining two severities (Major/Warning) and define different threshold values for them. In such a case, click the link "Add Threshold" and repeat the above steps.
- **Email Notification:** You have the option of automatically sending an email to notify the desired recipients when an alarm is generated. To use this option, you need to enable the option "Send Email to" and specify the email id in the text field. Once you enable this option, email notification would be sent to the specified recipients upon the generation of the particular alarm. The email message will contain details such as Subject, Alarm Profile Name, severity, alarm message, time of creation of the alarm and other details.
- **SNMP Trap Forwarding:** The administrator can enable the VQManager to generate SNMP traps on specific alarms. This will help in integrating the VQManager alarms with any higher-level NMS like ManageEngine OPManger. The VQManager allows the administrator to set up the list of SNMP trap listeners to forward the SNMP traps. By specifying the required SNMP parameters (viz., hostname, port, community, version etc.), the embedded VQManager SNMP agent can generate appropriate SNMP traps and forward to the defined entries. Currently the VQManager SNMP agent can generate a SNMP V1 and SNMP V2C traps.

For Jitter

- In the text field, specify the jitter threshold (in milli seconds) beyond which you would like to receive an alarm. Choose the severity which you would like to assign (Critical/Major/Warning). In addition, specify a

meaningful message for the alarm. For example: "The Jitter is greater than 10ms". This message would be highly helpful in understanding the type of problem when you receive the alarm.

- You can make use of any or both the remaining two severities (Major/Warning) and define different threshold values for them. In such a case, click the link "Add Threshold" and repeat the above steps.
- **Email Notification:** You have the option of automatically sending an email to notify the desired recipients when an alarm is generated. To use this option, you need to enable the option "Send Email to" and specify the email id in the text field. Once you enable this option, email notification would be sent to the specified recipients upon the generation of the particular alarm. The email message will contain details such as Subject, Alarm Profile Name, severity, alarm message, time of creation of the alarm and other details.
- **SNMP Trap Forwarding:** The administrator can enable the VQManager to generate SNMP traps on specific alarms. This will help in integrating the VQManager alarms with any higher-level NMS like ManageEngine OPManager. The VQManager allows the administrator to set up the list of SNMP trap listeners to forward the SNMP traps. By specifying the required SNMP parameters (viz., hostname, port, community, version etc.), the embedded VQManager SNMP agent can generate appropriate SNMP traps and forward to the defined entries. Currently the VQManager SNMP agent can generate a SNMP V1 and SNMP V2C traps.

For Packet Loss

- In the text field, specify the packet loss criterion (in percentage) beyond which you would like to receive an alarm. Choose the severity which you would like to assign (Critical/Major/Warning). In addition, specify a meaningful message for the alarm. For example: "Packet loss greater than 5%". This message would be highly helpful in understanding the type of problem when you receive the alarm.
- You can make use of any or both the remaining two severities (Major/Warning) and define different threshold values for them. In such a case, click the link "Add Threshold" and repeat the above steps.
- **Email Notification:** You have the option of automatically sending an email to notify the desired recipients when an alarm is generated. To use this option, you need to enable the option "Send Email to" and specify the email id in the text field. Once you enable this option, email notification would be sent to the specified recipients upon the generation of the particular alarm. The email message will contain details such as Subject, Alarm Profile Name, severity, alarm message, time of creation of the alarm and other details.
- **SNMP Trap Forwarding:** The administrator can enable the VQManager to generate SNMP traps on specific alarms. This will help in integrating the VQManager alarms with any higher-level NMS like ManageEngine OPManager. The VQManager allows the administrator to

set up the list of SNMP trap listeners to forward the SNMP traps. By specifying the required SNMP parameters (viz., hostname, port, community, version etc.), the embedded VQManager SNMP agent can generate appropriate SNMP traps and forward to the defined entries. Currently the VQManager SNMP agent can generate a SNMP V1 and SNMP V2C traps.

- For MOS
- The MOS alarm can be generated when the MOS value is less than or between the ranges defined by the administrator. To set the alarm, define the criteria by entering the MOS value below which you want the alarm to be activated. Alternatively, you can also define the MOS range between which the alarms are to be raised. Choose the severity, which you would like to assign (Critical/Major/Warning). In addition, specify a meaningful message for the alarm. For example: "The MOS less than 2.9". This message would be highly helpful in understanding the type of problem when you receive the alarm.
- You can make use of any or both the remaining two severities (Major/Warning) and define different threshold values for them. In such a case, click the link "Add Threshold" and repeat the above steps.
- **Email Notification:** You have the option of automatically sending an email to notify the desired recipients when an alarm is generated. To use this option, you need to enable the option "Send Email to" and specify the email id in the text field. Once you enable this option, email notification would be sent to the specified recipients upon the generation of the particular alarm. The email message will contain details such as Subject, Alarm Profile Name, severity, alarm message, time of creation of the alarm and other details.
- **SNMP Trap Forwarding:** The administrator can enable the VQManager to generate SNMP traps on specific alarms. This will help in integrating the VQManager alarms with any higher-level NMS like ManageEngine OPMManager. The VQManager allows the administrator to set up the list of SNMP trap listeners to forward the SNMP traps. By specifying the required SNMP parameters (viz., hostname, port, community, version etc.), the embedded VQManager SNMP agent can generate appropriate SNMP traps and forward to the defined entries. Currently the VQManager SNMP agent can generate a SNMP V1 and SNMP V2C traps.

For MOS Trend

- The MOS alarm can also be generated based on the MOS trend. For example, if the MOS value goes below or stays in between the range defined by the administrator beyond a specified number of times, an alarm can be generated. To set the alarm, define the criteria by entering the MOS value below which you want the alarm to be activated. Alternatively, you can also define the MOS range between which the alarms are to be raised. Also, specify the number of times the MOS trend could continue, beyond which you would wish to generate an alarm.

Choose the severity, which you would like to assign (Critical/Major/Warning). In addition, specify a meaningful message for the alarm. For example: "The MOS less than 2.9 for more than 3 times". This message would be highly helpful in understanding the type of problem when you receive the alarm.

- You can make use of any or both the remaining two severities (Major/Warning) and define different threshold values for them. In such a case, click the link "Add Threshold" and repeat the above steps.
- **Email Notification:** You have the option of automatically sending an email to notify the desired recipients when an alarm is generated. To use this option, you need to enable the option "Send Email to" and specify the email id in the text field. Once you enable this option, email notification would be sent to the specified recipients upon the generation of the particular alarm. The email message will contain details such as Subject, Alarm Profile Name, severity, alarm message, time of creation of the alarm and other details.
- **SNMP Trap Forwarding:** The administrator can enable the VQManager to generate SNMP traps on specific alarms. This will help in integrating the VQManager alarms with any higher-level NMS like ManageEngine OPManger. The VQManager allows the administrator to set up the list of SNMP trap listeners to forward the SNMP traps. By specifying the required SNMP parameters (viz., hostname, port, community, version etc.), the embedded VQManager SNMP agent can generate appropriate SNMP traps and forward to the defined entries. Currently the VQManager SNMP agent can generate a SNMP V1 and SNMP V2C traps.

For R Factor

- The R Factor alarm can be generated when the R Factor value is less than or between the ranges defined by the administrator. To set the alarm, define the criteria by entering the R Factor value below which you want the alarm to be activated. Alternatively, you can also define the R Factor range between which the alarms are to be raised. Choose the severity, which you would like to assign (Critical/Major/Warning). In addition, specify a meaningful message for the alarm. For example: "The R Factor less than 90". This message would be highly helpful in understanding the type of problem when you receive the alarm.
- You can make use of any or both the remaining two severities (Major/Warning) and define different threshold values for them. In such a case, click the link "Add Threshold" and repeat the above steps.
- **Email Notification:** You have the option of automatically sending an email to notify the desired recipients when an alarm is generated. To use this option, you need to enable the option "Send Email to" and specify the email id in the text field. Once you enable this option, email notification would be sent to the specified recipients upon the generation of the particular alarm. The email message will contain details such as Subject, Alarm Profile Name, severity, alarm message, time of creation of the alarm and other details.

- **SNMP Trap Forwarding:** The administrator can enable the VQManager to generate SNMP traps on specific alarms. This will help in integrating the VQManager alarms with any higher-level NMS like ManageEngine OPManager. The VQManager allows the administrator to set up the list of SNMP trap listeners to forward the SNMP traps. By specifying the required SNMP parameters (viz., hostname, port, community, version etc.), the embedded VQManager SNMP agent can generate appropriate SNMP traps and forward to the defined entries. Currently the VQManager SNMP agent can generate a SNMP V1 and SNMP V2C traps.

For Call Volume

- The call volume alarm can be generated for both increase in call volume as well as decrease in the call volume. To set the alarm, define the criteria by entering the number of calls beyond/ below which you want the alarm to be activated. Choose the severity which you would like to assign (Critical/Major/Warning). In addition, specify a meaningful message for the alarm. For example: "The Call volume less than 50 calls". This message would be highly helpful in understanding the type of problem when you receive the alarm.
- You can make use of any or both the remaining two severities (Major/Warning) and define different threshold values for them. In such a case, click the link "Add Threshold" and repeat the above steps.
- **Email Notification:** You have the option of automatically sending an email to notify the desired recipients when an alarm is generated. To use this option, you need to enable the option "Send Email to" and specify the email id in the text field. Once you enable this option, email notification would be sent to the specified recipients upon the generation of the particular alarm. The email message will contain details such as Subject, Alarm Profile Name, severity, alarm message, time of creation of the alarm and other details.
- **SNMP Trap Forwarding:** The administrator can enable the VQManager to generate SNMP traps on specific alarms. This will help in integrating the VQManager alarms with any higher-level NMS like ManageEngine OPManager. The VQManager allows the administrator to set up the list of SNMP trap listeners to forward the SNMP traps. By specifying the required SNMP parameters (viz., hostname, port, community, version etc.), the embedded VQManager SNMP agent can generate appropriate SNMP traps and forward to the defined entries. Currently the VQManager SNMP agent can generate a SNMP V1 and SNMP V2C traps.

For Disconnect Time

- In the text field, specify the number of calls disconnected, at a specific moment of time, beyond which you would like to receive an alarm. Choose the severity which you would like to assign (Critical/Major/Warning). In addition, specify a meaningful message for the alarm. For example:

"Disconnect Time greater than 15". This message would be highly helpful in understanding the type of problem when you receive the alarm.

- You can make use of any or both the remaining two severities (Major/Warning) and define different threshold values for them. In such a case, click the link "Add Threshold" and repeat the above steps.
- **Email Notification:** You have the option of automatically sending an email to notify the desired recipients when an alarm is generated. To use this option, you need to enable the option "Send Email to" and specify the email id in the text field. Once you enable this option, email notification would be sent to the specified recipients upon the generation of the particular alarm. The email message will contain details such as Subject, Alarm Profile Name, severity, alarm message, time of creation of the alarm and other details.
- **SNMP Trap Forwarding:** The administrator can enable the VQManager to generate SNMP traps on specific alarms. This will help in integrating the VQManager alarms with any higher-level NMS like ManageEngine OPManger. The VQManager allows the administrator to set up the list of SNMP trap listeners to forward the SNMP traps. By specifying the required SNMP parameters (viz., hostname, port, community, version etc.), the embedded VQManager SNMP agent can generate appropriate SNMP traps and forward to the defined entries. Currently the VQManager SNMP agent can generate a SNMP V1 and SNMP V2C traps.

For Talk Time

- The Talk Time alarm can be generated for both increase in Total Talk Time as well as decrease in the Talk Time. To set the alarm, define the criteria by entering the number of call minutes beyond/ below which you want the alarm to be activated. Choose the severity which you would like to assign (Critical/Major/Warning). In addition, specify a meaningful message for the alarm. For example: "The Total Talk Time is less than 50 minutes". This message would be highly helpful in understanding the type of problem when you receive the alarm.
- You can make use of any or both the remaining two severities (Major/Warning) and define different threshold values for them. In such a case, click the link "Add Threshold" and repeat the above steps.
- **Email Notification:** You have the option of automatically sending an email to notify the desired recipients when an alarm is generated. To use this option, you need to enable the option "Send Email to" and specify the email id in the text field. Once you enable this option, email notification would be sent to the specified recipients upon the generation of the particular alarm. The email message will contain details such as Subject, Alarm Profile Name, severity, alarm message, time of creation of the alarm and other details.
- **SNMP Trap Forwarding:** The administrator can enable the VQManager to generate SNMP traps on specific alarms. This will help in integrating the VQManager alarms with any higher-level NMS like ManageEngine

OPManager. The VQManager allows the administrator to set up the list of SNMP trap listeners to forward the SNMP traps. By specifying the required SNMP parameters (viz., hostname, port, community, version etc.), the embedded VQManager SNMP agent can generate appropriate SNMP traps and forward to the defined entries. Currently the VQManager SNMP agent can generate a SNMP V1 and SNMP V2C traps.

Click 'Add'

The required Alarm profile has been created

Note:

Each Alarm Profile Name should be unique.

The alarm message field is mandatory.

At least one threshold definition should be added and a maximum of three can be added with different severities.

More than one threshold cannot be added with same severity for a particular profile.

For ALOC, ASR, Average Answer Delay, SIP Error Codes, Disconnect Time, Call Volume, Packet Loss, Jitter and Voice Bandwidth Utilization Time the default time interval for raising the alarm is 60 minute while for Talk Time the default time interval is 1 day.

For generating alarms for ALOC, ASR, Average Answer Delay, SIP Error Codes, Disconnect Time, Call Volume, Packet Loss, Jitter and Voice Bandwidth Utilization Time a scheduler fetches data. The data is fetched at half of the time interval, set for sample duration, by the administrator i.e. If the administrator wants the alarm alert every 60 minutes, then the scheduler will fetch data every 30 minutes.

The order of triggering of alarms is done in the following way: For a single profile, you can define three different thresholds with different severities - CRITICAL, MAJOR & WARNING. Whichever severity has been defined first in the UI, it will get executed first. If WARNING is defined first in the UI, it will get executed first and other severities are executed in the same order as created in the UI. So, it is advisable to define 'CRITICAL' as the first severity. (For example, assume that you have created an ASR profile to raise a WARNING alarm when ASR goes below 60 per cent (first severity in the UI). Assume further that you have defined the second severity to generate a CRITICAL alarm when ASR falls below 50 per cent. Also assume that ASR suddenly touches 40 percent. Only a WARNING alarm would be generated first even though the condition falls under CRITICAL category).

Editing Alarm Profiles

You can edit an existing alarm profile, at any point of time.

To edit an alarm profile,

- Go to "Alarms" tab
- In the Summary View, all the alarm Profiles available at the moment get listed
- Click the edit icon against the name of the profile that is to be edited
- Alarm Profile Name and based on information are non-editable

- Carry out the required changes
- Click "Update"

Deleting Alarm Profiles

You can delete the alarm profiles that are no longer needed, at any point of time.

To delete an alarm profile

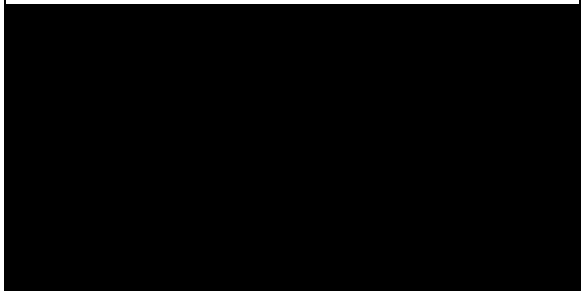
- Go to "Alarms" tab
- In the Summary View, all the alarm Profiles available at the moment get listed
- Click the icon against the name of the profile that is to be deleted
- The Alarm profile would be deleted once and for all

Note: When you delete an alarm profile, all the alarms that were associated with the particular profile would get deleted.

Pre-created Alarm Profiles

By default, VQManager provides four pre-created alarm profiles namely IncompleteCallsProfile, ALOCPProfile, ASRProfile, AverageAnswerDelayProfile.

Profile Name	Description
ALOCProfile	<div style="border: 1px solid black; height: 20px; width: 100%;"></div> <p>ALOC profile has been created for raising a critical alarm when ALOC exceeds 1200 seconds. Similarly, when ALOC falls below 25 seconds, a Major alarm and when it exceeds 900 seconds, a Warning alarm would be generated. You can edit this</p>

	<p>default profile and set your own condition</p> 
ASR Profile	<p>ASR profile has been created for raising a critical alarm when ASR goes below 40 per cent. Similarly, when ASR falls below 50 per cent, a Major alarm and when it is less than 60 per cent, a Warning alarm would be generated. You can edit this default profile and set your own condition</p>

<p>AverageAnswerDelayProfile</p>	<p>This profile has been created for raising a critical alarm when it goes beyond 60 seconds. Similarly, when Average Answer Delay exceeds 45 seconds a Major alarm and when it goes above 20 seconds, a Warning alarm would be generated. You can edit this default profile and set your own condition</p>
<p>Call Set up Time</p>	<p>The call Set up Time profile has been added to provide the exact time between the call initiation and call ringing on the other end, while Average Call Delay includes the delay caused by the person to pick the call. Whenever the call set-up time exceeds 30 seconds and the number</p>

of calls exceeds one, a critical alarm is raised. Similarly a major alarm is raised when the call set time is over 20 seconds for more than two calls and a warning alarm is raised when the call set up time is more than 10 seconds for more than three calls.

Total Alarms

- This is a summary of the different alarms that have been generated during the time period as set in the calendar and is found on the left hand side below the "Quick Links".
- All categories of alarms: 'Clear', 'Warning', 'Major' and 'Critical' are shown including the 'Total Alarms' generated in the selected time period.
- You can view more details of respective alarms by clicking on the linked number next to the alarm name.

Endpoints - Reports on VoIP Terminals

Contents

- Overview
 - Endpoints Summary
 - Endpoints Details
 - Resource Grouping
 - SIP Registration Requests
-
-

Overview

This 'Endpoint' tab provides endpoints specific details that would help in analyzing and troubleshooting endpoint specific quality deficiencies. The information presented here is in the form of:

- The Endpoints Summary showing a listing of all the monitored endpoints and their call information summary
 - Managing Endpoints list to be monitored
- The Endpoint Details giving a more in-depth view to calls participated in by each endpoint
- The Resource Groups provides group specific summary of call and QoS details
- The SIP registrations request details

Endpoints Summary

- This is the first UI that opens in the Endpoints tab providing the list of the monitored Endpoints and their Phone ID, Name, URL and IP Address will be displayed.
- To find a specific Endpoint, click on the lens icon found on the extreme right hand side of the list's header. Provide the Phone ID, Name/URL/IP Address of a endpoint to search.
- To view further details on each Endpoint, click on the specific endpoint link
- The Endpoints summary list can be arranged according to ascending or descending order of Phone ID by the Endpoints by clicking on the arrow next to the Phone ID field
- The Endpoints summary list can be exported as a PDF or CSV file or emailed as a PDF attachment to a number of E-mail Ids. This can be done through the respective icons - CSV icon, PDF icon and mail icon, found on the right-hand side just above the Endpoints Summary list.

The screenshot shows the ManageEngine VQManager interface. At the top, there are navigation links: Help, Upgrade License, Feedback, About Us, and Sign Out [admin]. Below the navigation is a menu with options: Monitor, Calls, Alarms, Endpoints (selected), Reports, Admin, and Support. A date range is displayed: From : 2009-06-25 00:00 To : 2009-06-25 23:59.

On the left side, there is a calendar for June 2009 and a 'Quick Links' section with options like Completed Calls, All Calls, All Alarms, Custom Reports, and Concurrent Calls. Below that is a 'Registration Requests' section with options like Registrations by Endpoints, Successful Requests, Unregistration Requests, Failed Requests, and All Requests.

The main content area is titled 'Endpoints' and has two tabs: 'Endpoints List' (selected) and 'Resource Group Summary'. Below the tabs are three buttons: 'Import Endpoints', 'Delete Endpoint', and 'Export as CSV'. A status bar indicates 'Showing : 1 to 25 of 5062' and 'Page : [1] 2 3 4 5 |Next Last'. The 'View per page' dropdown is set to [25] with options 50, 100, 250, 500.

<input type="checkbox"/>	Phone ID	Name	URL	IP Address
<input type="checkbox"/>	9315	sip:9315@192.168.220 ...	sip:9315@192.168.220 ...	192.168.220.184
<input type="checkbox"/>	15879	sip:15879@192.168.22 ...	sip:15879@192.168.22 ...	192.168.220.134
<input type="checkbox"/>	15056	sip:15056@192.168.22 ...	sip:15056@192.168.22 ...	192.168.220.154
<input type="checkbox"/>	4073	sip:4073@192.168.220 ...	sip:4073@192.168.220 ...	192.168.220.104
<input type="checkbox"/>	24323	sip:24323@192.168.22 ...	sip:24323@192.168.22 ...	192.168.220.102
<input type="checkbox"/>	49253	sip:49253@192.168.22 ...	sip:49253@192.168.22 ...	192.168.220.104
<input type="checkbox"/>	14149	sip:14149@192.168.22 ...	sip:14149@192.168.22 ...	192.168.220.154
<input type="checkbox"/>	30200	sip:30200@192.168.22 ...	sip:30200@192.168.22 ...	192.168.220.104
<input type="checkbox"/>	23202	sip:23202@192.168.22 ...	sip:23202@192.168.22 ...	192.168.220.132
<input type="checkbox"/>	42234	sip:42234@192.168.22 ...	sip:42234@192.168.22 ...	192.168.220.104
<input type="checkbox"/>	32299	sip:32299@192.168.22 ...	sip:32299@192.168.22 ...	192.168.220.113
<input type="checkbox"/>	33544	sip:33544@192.168.22 ...	sip:33544@192.168.22 ...	192.168.220.152
<input type="checkbox"/>	45499	sip:45499@192.168.22 ...	sip:45499@192.168.22 ...	192.168.220.132

Managing Endpoints

- Import Endpoints
- Delete Endpoints
- Export as CSV

Note: This section is visible only for:
 1) Trail version and Concurrent call based licensed version. Will not be available for IP Phone based Licensed version.

VQManager Endpoint listing is based on unique PhoneIDs discovered by VQManager:

- For SIP endpoints having the URL format "SIP:phoneID@hostname:portnumber" or "SIP:phoneID@IPAddress:portnumber", the endpoints are identified by the 'phoneID' part present in the SIP URL. If the 'phoneID' part is not available, then the SIP URL excluding the port number is considered as the endpoint ID. For example, a SIP endpoint of the format 'SIP: 1234@10.11.12.13:7777' will be identified as '1234' and an endpoint of the format 'SIP: 10.11.12.13:5555' will be identified as 'sip: 10.11.12.13'.
- Skinny phones are identified only by the PhoneID.
- In the case of H.323, endpoints are available either in URL format or as plain numbers from the Q.931 packets or simply as H.323 ID. If it is a URL of the format 'userid@hostname', the userid will be considered. If it is the number

from Q.931 packet, the number itself will be considered. If not the above two cases, the H.323 id is considered as the phoneID.

The phone IDs discovered will be those of unique endpoints(hard phones, soft phones, call servers, media proxy servers, gateways and other VoIP devices) participating in calls in the network. The IP Phone based(Enterprise) licensed version of VQManager does not have the "Import Endpoints" section as these versions of VQManager monitor all calls and endpoints in the network specified in the Monitored IP Phones sections.

Importing Endpoints

VQManager by default will add the endpoints participating in calls. Hence for defining the specific set of Endpoint(Subscribers/ IP Phones) list to be monitored. One can import the specific set of Endpoints available in their environment.

- VQManager will hence forth will store and maintain the endpoint details information for the calls participated by those Phone IDs. In concurrent calls based licensing and trail version of VQManager, this import endpoints will help to collect reports for speicfied endpoints rather than maintaining huge number of endpoints that may belonged to other network (For Example public numbers).
- In Concurrent calls license, Concurrent call license limit will be considered for call processing while Imported endpoints list will be considered to whether a particular endpoint reports should be added to Endpoint summary or not.
- In trail version, all the calls will be processed and Imported endpoints list will be considered only to check whether a particular endpoint reports should be added to Endpoint summary or not.

Endpoints

Endpoints List
Resource Group Summary

Import Endpoints
Delete Endpoint
Export as CSV

Import IP Phones from text file Browse...

Manually add IP Phone IDs

[as comma separated entries]

- By default, VQManager lists all the Endpoints/IP phones that are participating in calls. To avoid this, please import the PhoneIDs of Endpoints that need to be listed by VQManager
- We strongly recommend you to import the endpoints need to be listed for better performance.

Save
Cancel

Delete Endpoints

- Select endpoints needs to be deleted and click on the 'Delete Endpoint' button available above the Endpoint summary table

Export as CSV

- Endpoint summary can be exported as CSV
In exported CSV one can add/edit/delete phone id and can be used for importing the Endpoint list

Note: To enable the auto-discovery mode after importing some endpoint. Select all the endpoint and delete them. If the endpoint list is empty the auto-discovery mode will be enabled and endpoints will get added from on going calls

Endpoints Details

By clicking on an Endpoint in the Endpoint Summary list you are brought to the Endpoints Details UI showing the details of that particular endpoint. The endpoint's name/URL/IP Address is displayed on top of the Call Volume Graph. Here, the call volume, Incoming and Outgoing Call QoS metrics and Call history pertaining to the single Endpoint is shown. The information displayed here is also for the time-period as set in the calendar. The sections presented here are:

- Call Volume graph
- Incoming & Outgoing Call and QoS Metrics
- Traffic Metrics
- The Calls list



Call Volume Graph

The "Call Volume" graph is similar to that in the Monitor tab's Summary Report view but shows call information for a single Endpoint.

- Displays the statistics of all the calls that the Endpoint participated in over the chosen time frame as set in the calendar
- The bar graph has the green areas representing the successful calls while the red areas denote unsuccessful calls
- Provides the number of Total, Successful, Unsuccessful and Waiting calls as a linked number. When these linked numbers are clicked you can view the information of the respective calls
- The Successful Calls are divided into calls based on quality - Good and Poor quality calls. VQManager distinguishes from Good and Poor Quality calls based on the user's setting in the Monitor tab in the "Configure" section of the Voice Quality graph. By default, calls with **MOS** (Mean Opinion Score) greater than 3.1 are classified as Good Quality Calls. Calls with MOS less than 3.1 are marked as Poor Quality Calls
- The Unsuccessful Calls are further divided into Unanswered Calls and Error Calls. Calls that were not answered by the user (user busy, user not available etc.,) fall into the Unanswered Call category. Other calls that failed due to errors in server or client are marked as Error Calls
- The Waiting Calls are the number of calls that remain or remained in waiting mode at the chosen time frame
- The number of Unmonitored Calls that the endpoint participated in is listed. Unmonitored calls are those that VQManager has abruptly stopped monitoring - this could be due to an abrupt stop and restart of the VQManager server, or because there were no voice packets that were received for a continuous duration(30 seconds) of time
- Answer Seizure Ratio(ASR) - ratio of successfully connected calls to attempted calls for the endpoint is displayed
- Lists the time at which the endpoint participated in the maximum number of calls - peak usage, and the time at which there were least number of calls - low usage time
- Provides the Average Call Duration(ACD) time across all the calls during the selected time period
- The Call Rate is provided showing the rate at which the endpoint has participated in calls
- The date and time of the Last Call in which the endpoint has participated in is also shown

Note:

The "Total Calls" count in the Endpoints Summary view and the "Total Calls" count in the Endpoint Details view for the respective endpoints may differ. This is because the Endpoints Details view information takes into consideration all calls made by an endpoint - even those under Active and Waiting state.

Incoming & Outgoing Call and QoS Metrics

The next section below the “Call Volume” graph provides separate summaries for the “Outgoing Call and QoS Metrics” and the “Incoming Call and QoS Metrics”.

- Displays the Total number of outgoing and incoming calls from/to the endpoint. On clicking the linked number, you can view the list of the calls
- The Last call that the Endpoint made and received is displayed. On clicking the Last Call Phone ID displayed, you can view the Call Details of that particular call.
- The Last call made and received date and time is displayed by “Last Call At” entry
- The number of Successful outgoing and incoming calls is displayed. On clicking this linked number, you can view the list of these calls
- The total Duration of Outgoing and Incoming calls is provided
- Provides the Average Call Duration(ACD) time across all the calls during the time period as set in the calendar
- The colored horizontal bars in the Outgoing call and Incoming call sections show the average MOS value for the calls
- The QoS parameter values for Jitter, Delay and Loss are shown. On clicking the “More” link, you can see all QoS statistics with their Min, Max and Avg values and whether Good, Tolerable or Poor as defined by the user in the Monitor tab

Traffic Metrics

The “Traffic metrics” section is found below the “Incoming Call and QoS Metrics” and “Outgoing call and QoS Metrics” section. Here the traffic details are displayed specific to the endpoint.

- In Octets - The number of octets sent to the endpoint
- Out Octets - The number of octets sent out by the endpoint
- In Packets – the number of packets that has flowed into the endpoint
- Out Packets – the number of packets that has flowed out of the Endpoint

















The Calls List

The final section in the Endpoint Details UI is the Call list that has the call information on all the calls that the endpoint has participated in over the time period as set in the calendar

- The call details displayed by default are the call’s Initiator, the Call Initiation time, Duration of the call, the Call Status and the Status Code
- More information on the calls can be displayed by clicking on the column chooser icon found on the extreme right side of the list next to the lens icon. Check the items from the list that appears to have the required information displayed
- You can search this list for a particular Initiator, Call Status or Status Code by clicking on the lens icon found on the top-right side of the list and providing the required search criteria
- Clicking on any Initiator brings you more Call Details for the particular call

- This calls list can be exported as a PDF or CSV file or emailed as a PDF attachment to a number of E-mail Ids. This can be done through the respective icons - CSV icon, PDF icon and mail icon, found on the right-hand side just above the list. The PDF document can have a maximum of 10 columns information displayed at a time

Calls for 5559

Initiator	Participant	Call Init Time	Duration	Call Status
 subash	 sip:5760@voip-lin2	Thu, 4 Sep 2008 11:09:16	29 secs	Completed
 subash	 sip:8006@voip-lin2	Thu, 4 Sep 2008 11:09:08	NA	Busy Here
 subash	 sip:8006@voip-lin2	Thu, 4 Sep 2008 11:08:07	NA	Busy Here
 Srikanth.B	 subash	Thu, 4 Sep 2008 11:06:07	15 secs	Completed
 J.Sujith Regan..	 subash	Thu, 4 Sep 2008 11:06:06	18 secs	Completed
 subash	 sip:wqdweweqd@voip-l ...	Thu, 4 Sep 2008 11:05:49	NA	Not Found
 subash	 sip:8009@voip-lin2	Thu, 4 Sep 2008 11:05:46	NA	Temporarily Unavaila ...
 subash	 sip:8009@voip-lin2	Thu, 4 Sep 2008 11:05:45	NA	Temporarily Unavaila ...
 subash	 sip:8006@voip-lin2	Thu, 4 Sep 2008 11:05:39	NA	Busy Here
 subash	 sip:8006@voip-lin2	Thu, 4 Sep 2008 11:05:37	NA	Busy Here

Resource Groups

The Resource Group section is displayed as a separate menu in the left-hand panel below the Quick Links. You can group certain specific endpoints as a 'resource group'. Resource grouping can be used when you want to monitor the calls from specific group based on specific URL or IP address or based on participant identifier.

Resource group summary view

On clicking the menu item "Resource Groups", the resource groups are listed showing the Group Name and their Created Time. To view the endpoints for specific resource group, click the respective resource Group Name. Upon clicking the link, you can see the Endpoints with their URL/Phone ID, total calls, duration, MOS, Failed Calls and Octets. To drill down on endpoint details, click the respective Endpoint URL/Phone ID.

Resource Group Summary

+ Add Resource Group 1 - 2 of 2 25			
Group Name	Created Time	Edit	Delete
UserMeachine	Fri, 5 Sep 2008 11:11:52		
ipaddressgroup	Fri, 5 Sep 2008 11:12:33		

1 - 2 of 2 25

To Add a Resource Group,

- Click the "Add Resource Group" link
- In the UI that opens, provide the Group Name for the new Resource Group (mandatory)
- You can provide upto three conditions to include required endpoints for the new Resource Group. These conditions are in the form of three rows of drop-down lists and text-boxes
- You can create the Resource group matching any or all of the three conditions you provide. Check the respective condition radio button "Match all of the following" or "Match any of the following" based on your need
- Endpoints can be included in the group by either identifying them by their URL or their IP address, the two options are found in the first drop-down list. Select the required identification condition.
- On choosing URL identification of endpoints, you can either specify what the Endpoint's URL string contains or by specifying what the URL starts with or ends with. Select the required condition from the second drop-down list and provide the URL detail in the final text-box
- In case of IP address identification of endpoints, specify the range between which the endpoints are to be considered to form the Resource Group. Two text-boxes are provided to enter the two IP addresses within which the endpoints are to be selected
- Click "Create" button to save and activate the group. Click on "Cancel" to cancel the resource group.

Add Resource Group

Group Name: *

Match all of the following
 Match any of the following

<input type="text" value="URL"/>	<input type="text" value="contains"/>	<input type="text"/>
<input type="text" value="URL"/>	<input type="text" value="contains"/>	<input type="text"/>
<input type="text" value="URL"/>	<input type="text" value="contains"/>	<input type="text"/>

To Edit / Update the Resource Group

- Click the "Resource Groups" link
- Click the "Edit" icon present against the respective resource Group Name
- Add or edit the conditions for including endpoints
- Once the required changes are done, click "Update" button present on the end of the page

To Delete a Resource Group,

- Click the "Resource Groups" link
- Click the "Delete" button present against the respective resource group
- A dialog box pops-up to confirm your request. Click "OK" to delete the resource group permanently

Note:

Each group name is unique. You can create unlimited resource group profiles. You cannot rename an already created 'group name'. The parameters and criteria of the resource group can be changed but cannot be renamed.

Registration Requests

The SIP "Registration Request" section is available on the left hand side panel below the Resource Groups section. Administrators can view the various SIP registrations requests like successful requests, unregistration requests and failed requests. To get the required information on the different Registration request types, click on the respective links under the "Registration Request" heading. The various registration requests that can be viewed are:

- Registrations by Endpoints
- Successful Requests
- Unregistration Requests
- Failed Requests
- All Requests
- History Data - Multiday Registrations Summary

In the the above Registration Request lists, you can get the Registration Details of all the Registration Requests from any particular phone by clicking on the Phone URL.

Registration by Endpoints

- The "Registrations by Endpoints" view provides a summary of the registration, unregistration and failed registrations along with the current status grouped by the endpoints URLs.
- The tabular view has details on the Phone URL, the total number of Registered requests, the total number of Unregistered requests, the number of failed requests, the Total number of Registration requests, Last registration Time and the current Status of the URL (registered / unregistered).
- The data can be further drilled down by clicking the linked numbers showing the number of requests - registered / unregistered / failed / total.
- This list can be arranged in ascending or descending order of Phone URL by clicking on the arrow next to the Phone URL header.
- You can search for Registration requests from a particular Phone URL or search by the Status of the requests (Registered/Unregistered) by clicking on the lens icon found on the top-right side of the list.
- This calls list can be exported as a PDF or CSV file or emailed as a PDF attachment to a number of E-mail Ids. This can be done through the respective icons - CSV icon, PDF icon and mail icon, found on the right-hand side just above the list. The PDF document can have a maximum of 10 columns information displayed at a time.

Registrations by Endpoints

Phone URL ▲	Registered	Unregistered	Failed	Total	Last Register
sip:1001@10.10.10.20 ...	12	0	0	12	Thu, 4 Sep 2
sip:5559@voip-lin2	2	1	0	3	Thu, 4 Sep 2

Successful Requests

- The "Successful Requests" view displays all the successful SIP registration requests.
- The details shown are the Phone URL, the Registrar URL, the Phone IP, the Registration Time, the Status (Registered or Unregistered) and the registration's Expiry time (in seconds).
- This Registration Request list can be exported as a PDF or CSV file or emailed as a PDF attachment to a number of E-mail Ids. This can be done through the respective icons - CSV icon, PDF icon and mail icon, found on the right-hand side just above the list. The PDF document can have a maximum of 10 columns information displayed at a time.

Successful Requests

Phone URL	Registrar URL	Phone IP	Registration Time	Status	Expiry (Secs)
sip:1001@10.10.10.20 ...	sip:10.10.10.200	10.10.10.201	Thu, 4 Sep 2008 18:20:22	Registered	3600
sip:1001@10.10.10.20 ...	sip:10.10.10.200	10.10.10.201	Thu, 4 Sep 2008 17:38:01	Registered	3600
sip:1001@10.10.10.20 ...	sip:10.10.10.200	10.10.10.201	Thu, 4 Sep 2008 16:58:07	Registered	3600
sip:1001@10.10.10.20 ...	sip:10.10.10.200	10.10.10.201	Thu, 4 Sep 2008 16:18:15	Registered	3600
sip:1001@10.10.10.20 ...	sip:10.10.10.200	10.10.10.201	Thu, 4 Sep 2008 15:38:25	Registered	3600
sip:1001@10.10.10.20 ...	sip:10.10.10.200	10.10.10.201	Thu, 4 Sep 2008 14:58:34	Registered	3600
sip:1001@10.10.10.20 ...	sip:10.10.10.200	10.10.10.201	Thu, 4 Sep 2008 14:18:46	Registered	3600
sip:1001@10.10.10.20 ...	sip:10.10.10.200	10.10.10.201	Thu, 4 Sep 2008 13:39:00	Registered	3600
sip:1001@10.10.10.20 ...	sip:10.10.10.200	10.10.10.201	Thu, 4 Sep 2008 12:58:46	Registered	3600
sip:1001@10.10.10.20 ...	sip:10.10.10.200	10.10.10.201	Thu, 4 Sep 2008 12:18:57	Registered	3600
sip:1001@10.10.10.20 ...	sip:10.10.10.200	10.10.10.201	Thu, 4 Sep 2008 11:38:49	Registered	3600
sip:1001@10.10.10.20 ...	sip:10.10.10.200	10.10.10.201	Thu, 4 Sep 2008 11:01:02	Registered	3600
sip:5559@voip-lin2	sip:voip-lin2	192.168.110.231	Thu, 4 Sep 2008 10:50:26	Registered	3600
sip:5559@voip-lin2	sip:voip-lin2	192.168.110.231	Thu, 4 Sep 2008 10:49:09	Registered	3600

- You can search for Registration requests from a particular phone URL / Registrar URL / Phone IP / Status of the requests (Registered/Unregistered) by clicking on the lens icon found on the top-right side of the list.
- The data can be further drilled down to give the Registration Details for the particular Registration Request by clicking the linked Phone URL.

Unregistration Requests

- The "Unregistration Requests" view displays all the successful unregistration requests.
- The details shown are the Phone URL, the Registrar URL, the Phone IP, the Registration Time, the Status (Registered or Unregistered) and the registration's Expiry time (in seconds). (An unregistration request is always sent with an Expiry time of zero seconds)
- This Registration Request list can be exported as a PDF or CSV file or emailed as a PDF attachment to a number of E-mail Ids. This can be done through the respective icons - CSV icon, PDF icon and mail icon, found on the right-hand side just above the list. The PDF document can have a maximum of 10 columns information displayed at a time.
- You can search for Registration requests from a particular phone URL / Registrar URL / Phone IP / Status of the requests (Registered/Unregistered) by clicking on the lens icon found on the top-right side of the list.
- The data can be further drilled down to give the Unregistration Details for the particular Registration Request by clicking the linked Phone URL.

Failed Requests

- The "Failed Requests" view displays all the failed registration and unregistration requests.
- The details shown are the Phone URL, the Registrar URL, the Phone IP, the Registration Time, the Status (Registered or Unregistered) and the registration's Expiry time (in seconds). (An unregistration request is always sent with an Expiry time of zero seconds)
- This Registration Request list can be exported as a PDF or CSV file or emailed as a PDF attachment to a number of E-mail Ids. This can be done through the

respective icons - CSV icon, PDF icon and mail icon, found on the right-hand side just above the list. The PDF document can have a maximum of 10 columns information displayed at a time.

- You can search for Registration requests from a particular phone URL / Registrar URL / Phone IP / Status of the requests (Registered/Unregistered) by clicking on the lens icon found on the top-right side of the list.
- The data can be further drilled down to give the Failed Request Details for the particular Registration Request by clicking the linked Phone URL.

All Requests

- The "All Requests" view displays all the registration, unregistration and failed requests that took place within the chosen time frame. It includes the entire request whether they are successful, failed or unregistered
- The details shown are the Phone URL, the Registrar URL, the Phone IP, the Registration Time, the Status (Registered or Unregistered) and the registration's Expiry time (in seconds). (An unregistration request is always sent with an Expiry time of zero seconds)
- This Registration Request list can be exported as a PDF or CSV file or emailed as a PDF attachment to a number of E-mail Ids. This can be done through the respective icons - CSV icon, PDF icon and mail icon, found on the right-hand side just above the list. The PDF document can have a maximum of 10 columns information displayed at a time.
- You can search for Registration requests from a particular Phone URL / Registrar URL / Phone IP / Status of the requests (Registered/Unregistered) by clicking on the lens icon found on the top-right side of the list.
- The data can be further drilled down to give the Registration Details for the particular Registration Request by clicking the linked Phone URL.

History Data - Multiday Registrations Summary

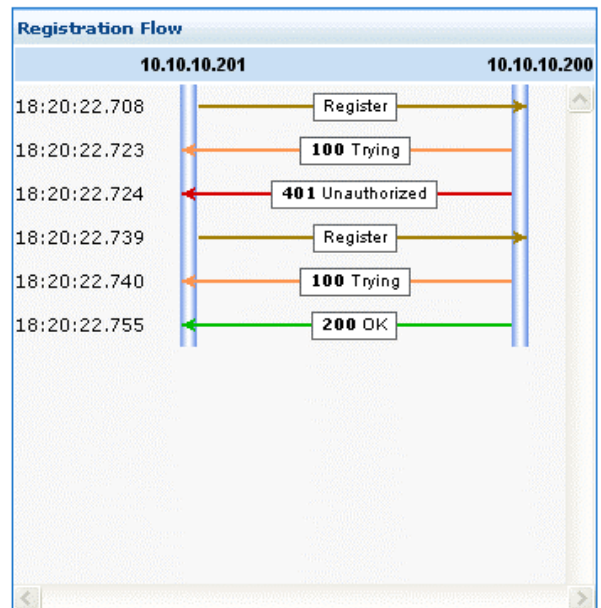
Day	Total	Registered	Unregistered	Failed
29 Apr 2009	335	229	106	0
28 Apr 2009	648	444	204	0
27 Apr 2009	164035	144326	16820	2700
26 Apr 2009	301421	263396	32846	5104
25 Apr 2009	304911	266500	33224	5147
24 Apr 2009	51676	45136	5622	885

- The 'Multiday Registrations Summary' view provides a summary of the 'SIP Registrations' data across multiple days. This can be viewed for a range of days like 'Last 7 days, Last 30 days' or a 'Custom' timeperiod.
- In the 'Endpoints' tab, click on 'All Requests'. Choose a required time period from the 'Calendar' component on the top left and click on 'Show'. This will bring up a table with the registrations count details for categories, namely 'Total', 'Registered', 'Unregistered' and 'Failed' registration requests for each day in the chosen time period. To view the list of the registrations under any category for any particular day, click on the corresponding number link in the respective call category.
- The list can also be extracted as a 'CSV', 'PDF' file or can be e-mailed as a 'PDF' attachment to desired recipients.

Registration Details

Registration Details for sip:1001@10.10.10.200

Registration Details	
Status	 Registered
Time	Sep 4, 2008 6:20:22 PM
Expires (seconds)	3600
IP Phone more...	
URL	sip:1001@10.10.10.200
IP Address	10.10.10.201
Port	5060
Registrar	
URL	sip:10.10.10.200
IP Address	10.10.10.200
Domain	10.10.10.200
Port	5060



Registration Trace							
Capture Time	Protocol	Status	Code	Source	Src Port	Destination	Des Port
18:20:22.708	SIP	Register	2001	10.10.10.201	5060	10.10.10.200	5060
18:20:22.723	SIP	Trying	100	10.10.10.200	5060	10.10.10.201	5060
18:20:22.724	SIP	Unauthorized	401	10.10.10.200	5060	10.10.10.201	5060
18:20:22.739	SIP	Register	2001	10.10.10.201	5060	10.10.10.200	5060
18:20:22.740	SIP	Trying	100	10.10.10.200	5060	10.10.10.201	5060
18:20:22.755	SIP	OK	200	10.10.10.200	5060	10.10.10.201	5060

- This view is got on clicking a Phone URL from the list of Successful / Unregistration / Failed Registration Requests in the "Registration requests" section.
- The Registration request details such as Status, Time of Registration and Time of Expiry are shown.
- The URL, IP Address and Port of the IP phone requesting registration is shown. More details such as User Agent, Alternate Contact, Methods, Allowed Events and Expiry time are got on clicking the "More" link found next to the IP Phone header.
- The Registrar details such as URL, IP Address, Domain and Port are displayed.
- On the right half of the UI, the Registration flow shows a complete representation of the Request flow. This is useful in troubling Registration failures.
- The last section of the Registration details UI is the Registration Trace which shows a tabular representation of the request flow showing Capture Time, Protocol, Status, Code, Source, Source Port, Destination and Destination Port.

Admin Operations

Contents

- **Overview**
 - **System Settings**
 - Sniffer
 - Syslog Servers
 - Import CDR Logs
 - Business Hours
 - Monitored Endpoints
 - **Admin Settings**
 - User Management
 - Runtime Administration
 - Mail Settings
 - SNMP Trap forwarding
 - Proxy Settings
 - Database Administration
 - Bandwidth Monitor
 - **General Settings**
 - Edit Account Settings
 - Skin Selector
-

Overview

To configure VQManager to monitor the VoIP calls in your network and for the efficient working of VQManager, certain administrative operations are involved. These operations include sniffer configuration, configuring syslog server, importing Call Detail Record (CDR) logs generated by call servers, user management, Proxy settings, Runtime and Database administration, SNMP trap settings, Account settings etc. The administrative operations have been classified into three categories:

- System Settings
- Admin Settings
- General Settings

This section provides details about each of these sections.

System Settings

This section enables you to perform certain operations that involve setting up of VQManager to monitor the VoIP calls traffic. These are namely: setting the VQManager sniffer to listen for VoIP traffic, setting the VQManager server as a Syslog server for receiving CDRs and setting VQManager to import the CDRs logs. Other operations in this section are configuring of Business Hours and tracking of the IP phones monitored by VQManager. Each operation can be accessed by clicking on the respective icons in the "Admin" tab.

Sniffer

This section consists of sniffer settings as seen in the Configuration Wizard. If you have skipped the wizard, the screen that will be displayed will be the "Protocols Settings" page. Refer to the notes on the Configuration wizard for more from this stage of the sniffer configuration. If you have already configured the sniffer using the configuration wizard, then the summary of the sniffer settings will be displayed on clicking the "Sniffer" icon. You can then re-configure the required settings and save the same. Refer to the Configuration wizard for complete information on sniffer settings.

Syslog Servers

- Detailed explanation provided in the Configuration Wizard section. Please refer to this.

Import CDR Log

- Detailed explanation provided in the Configuration Wizard section. Please refer to this.

Business Hours

In production environments, VoIP traffic would peak during business hours and it would wane in off-peak hours or non-working hours. Administrators would wish to receive alarms/reports separately for working hours and non-working hours. For example, a failed call during working hour would have to be viewed very seriously than the one during off-peak hours. To achieve this, VQManager aids you in specifying your 'Working Time'.

To specify working time,

- Go to "Admin" >> "System Settings" in the Web Client
- Click "Business Hours"
- In the UI that opens, set your business hours by specifying the starting and end timings
- Click "Save"

Once you set the business hours here, it can be used wherever applicable. For example, in setting alarm profiles, it is enough if you specify 'Business Hours' or 'non-business hours' as per your requirements. The timing will take effect according to this setting.

Monitored Endpoints

Admin Settings



The Monitored Endpoints section contains a list of the endpoints being monitored by VQManager and is present under the "System Settings" section of the Admin tab.

Note:

This section is visible only for:

- 1) a licensed version of VQManager which can monitor only 'x' number of endpoints depending on the license purchased
- 2) a free version of VQManager that allows monitoring of only 10 endpoints

VQManager licensing is based on the number of unique phone IDs discovered by VQManager:

- For SIP endpoints having the URL format "SIP:phoneID@hostname:portnumber" or "SIP:phoneID@IPAddress:portnumber", for the purpose of licensing, the endpoints are identified by the 'phoneID' part present in the SIP URL. If the 'phoneID' part is not available, then the SIP URL excluding the port number is considered as the endpoint ID. For example, a SIP endpoint of the format 'SIP:1234@10.11.12.13:7777' will be identified as '1234' and an endpoint of the format 'SIP:10.11.12.13:5555' will be identified as 'sip:10.11.12.13'.
- Skinny phones are identified only by the phoneID.
- In the case of H.323, endpoints are available either in URL format or as plain numbers from the Q.931 packets or simply as H.323 id. If it is a URL of the format 'userid@hostname', the userid is considered. If it is the number from Q.931 packet, the number itself is considered. If not the above two cases, the H.323 id is considered as the phoneID.

The phone IDs discovered will be those of unique endpoints(hard phones, soft phones, call servers, media proxy servers, gateways and other VoIP devices) participating in calls in the network. The trial version or the unrestricted/unlimited licensed version of VQManager does not have the "Monitored Endpoints" section as these versions of VQManager monitor all calls and endpoints in the network without being limited to a specified number of endpoints.

The "Monitored Endpoints" section also allows you to input new endpoints you want to monitor, edit and make changes to endpoints already being monitored and make other monitoring configurations:

Monitored Endpoints

Monitor Configuration Delete IP Phone Export as CSV 1 - 25 of 48 25

Import IP Phones from text file Browse...

Manually add IP Phone IDs

 [as comma separated entries]

Auto-Discovery

Outbound Call (Matching call originator PhoneID)

Inbound Call (Matching call receiver PhoneID)

Both

Save Cancel

<input type="checkbox"/> PhoneID	Discovery Time	Discovery Mode
<input type="checkbox"/> 123456789	Thu, 30 Apr 2009 15:16:28	Auto-discovered
<input type="checkbox"/> 111222333	Thu, 30 Apr 2009 15:16:28	Auto-discovered
<input type="checkbox"/> 246891214	Thu, 30 Apr 2009 15:16:28	Auto-discovered

Delete IP phone

Select the endpoints you want to delete by clicking on the check box next to respective endpoints and then click on the "Delete IP Phone" icon to delete the chosen endpoints.

Monitor Configuration

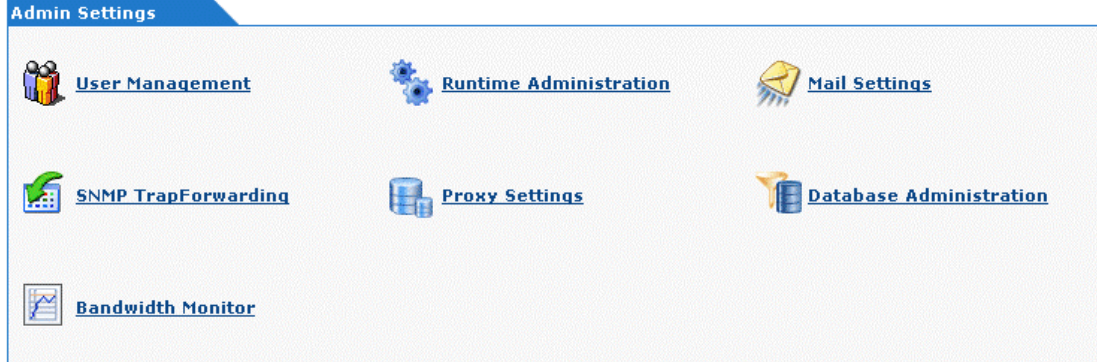
Click on the "Monitor Configuration" icon to provide other settings to configure the manner in which VQManager selects endpoints to be added to the "Monitored Endpoints" list:

- You can import the endpoint details from a text file that contains the phone IDs of the endpoints to be monitored. The entries can be comma separated or new-line separated.
- You can manually input the phone IDs to be monitored, multiple entries to be separated by commas.
- By enabling auto-discovery of endpoints, you can choose whether VQManager should monitor all "Outbound Calls" from the listed Monitored Endpoints or all "Inbound Calls" to the listed endpoints or "Both" inbound and outbound traffic from the listed endpoints.

Note:

Reports on VoIP terminals(Endpoints) and other reports (Live Report/ Calls Report/ Duration Report) are generated only for the calls made by the monitored endpoints

Admin Settings



User Management, Runtime Administration, Mail Server Settings, SNMP Trap forwarding, Proxy Settings, Database Administration and Bandwidth Monitor have been classified under the category Admin Settings.

User Management

By default, VQManager comes with two pre-defined users - admin and guest. Apart from this, you can create as many users as you desire and define appropriate access levels for the user. This section explains about the admin and guest users, their respective privilege levels and how to create users.

As stated above, you can create as many users as you desire and define appropriate access levels for the user. For example, you can create a user "ABC" and authorize him with all admin privileges or make him an ordinary user with ordinary privileges.

From the User Management tab, you can

- View all the existing users
- Create new users
- Edit the Access Level and Email ID for the various users and delete unrequired users

To view the existing list of users

- Click "Admin" >> "Admin Settings" in Web Client
- Go to "User Management" in the "Administration" tab on the left-hand side of the UI
- The list of users will be displayed with respective login names, access levels and email IDs

Note: The default login name and password for a new installation of VQManager is 'admin' and 'admin' respectively. The default email ID has been configured as aaaadmin@adventnet.com. After logging in to the VQManager, change the email ID for admin user.

To Add New Users

- Click on the "Admin" tab
- Click on the "User Management" icon
- In the UI that opens, click the "Add User"
- Enter the desired "Login Name"; this name will be used to log in to the VQManager web interface
- Enter "Password"; the password should be at least 5 characters long
- Type the password once again in the "Confirm Password"
- Define "Access Level" for the new user - Administrator/Operator:
 -
 - Users falling under "Administrator" category shall have unlimited privilege and access over all functionalities of VQManager.
 - The users falling under "Operator" category will not have any 'write' / 'edit' / 'delete' functions enabled in the UI. The 'Operator' will only see the "Edit Account Settings" and "Skin Selector" options in the Admin tab and cannot perform operations like adding/editing/deleting alarms and report profiles, configuring of QoS Min/Max thresholds, deleting of unmonitored calls and upgrading of the license
- Enter the "Email Address" for this user
- Click on the "Create" button to create the new user account

Runtime Administration

Setting Log Levels

In the event of any issues, VQManager server logs help us in getting to the root of the issue. Printing of log messages can be controlled through the eight log levels. This section explains various log levels and how to set desired levels.

Printing of log messages can be controlled through the four log levels - VERBOSE, DEBUG, INFO and SEVERE.

SEVERE represents the highest severity with highly critical messages alone getting printed in the logs. 'VERBOSE' represents the lowest level - all messages get printed. The default Log Level is 'INFO'.

To modify Log Levels,

- go to "Admin" tab
- click "Log Levels"
- in the UI that opens, select the desired log level from the drop-down
- click "Save"
- the desired log level is set

Mail Settings

VQManager sends various notifications to the users (for example, reports) using an SMTP mail server running in your network. This section explains how to specify the SMTP server details and entering email IDs.

To specify SMTP Server details,

- Go to "Admin" >> "Admin Settings"
- Click "Mail Settings" icon under "Settings" section; Alternatively, you can click "Mail settings" in the "Administration" tab on the left-hand side of the UI
- Enter SMTP server name in the text field
- Enter SMTP port
- Enter username and password, if your SMTP settings require authentication
- Click "Save Settings", if you have changed SMTP settings

By default, the SMTP server runs in the port 25. You can specify any other SMTP server also.

To specify outgoing Email IDs,

- in the text field for 'From' address, specify the email id of the originator of the email; by default, the from address is specified as 'noreply@vqmanager.com'.
- add as many email IDs of intended mail recipients as required in the text field for 'Notify To'
- this serves the purpose of an address book and would come in handy wherever send email option is provided (for example, sending reports, alarms). You can just choose IDs from this list
- if you want to remove any ID from the recipients list, do so by choosing the ID and clicking the "remove" button
- click "Save Settings" to give effect to the settings

To test Mail Server Configuration,

After configuring the 'Mail Settings', you can test if connection could be established with your server. To test, just click the button "Test" of "Test Mail Server". VQManager will attempt to establish connection with your mail server. If the configuration is proper and if VQManager is able to establish a connection, you will see the message "Mail Server connection established successfully".

SNMP Trap Forwarding

The administrator can enable the VQManager to generated SNMP traps on specific alarms. This will help in integrating the VQManager alarms with any higher-level NMS like ManageEngine OPManager. The VQManager allows the administrator to set up the list of SNMP trap listeners to forward the SNMP traps. By specifying the required SNMP parameters (viz., hostname, port, community, version etc.), the embedded

VQManager SNMP agent can generate appropriate SNMP traps and forward to the defined entries. Currently the VQManager SNMP agent can generate a SNMP V1 and SNMP V2C traps.

Configuring SNMP Trap Forwarding entries:

To receive the SNMP traps generated by the VQManager, the administrator has to configure the list of SNMP Trap listening Manager list in the UI.

Adding SNMP Trap Forwarding Entry

- Go to "Admin" tab
- Click on "SNMP Trap Forwarding" icon
- Click on "Add Trap Forwarding Entry" on the right hand side of the UI
- Enter the various details: Host Name, Trap Port, SNMP version, Community, Timeout duration and the number of Retries onto the respective text field
- Click on "Add" button to create the SNMP Trap Forwarding Entry

To View a SNMP Trap Forwarding Entries

- Go to "Admin" tab
- Click on "SNMP Trap Forwarding" icon to view the various SNMP Trap Forwarding Entries

Note: VQManager does not have any pre defined default SNMP trap forwarding entry. Administrators have to add the SNMP trap forwarding entry before viewing it

Editing SNMP Trap Forwarding Entry

- Go to "Admin" tab
- Click on "SNMP Trap Forwarding" icon
- Click on the "Edit" icon against the SNMP Trap Forwarding entry, which requires changes
- The details of the SNMP trap forwarding entry opens below in the same UI
- Change the required fields and click on "Update" button to save the changes

Deleting SNMP Trap Forwarding Entry

- Go to "Admin" tab
- Click on "SNMP Trap Forwarding" icon
- Click on the "Delete" icon against the SNMP Trap Forwarding Entry, which needs to be deleted
- Confirm the action by clicking "OK" on the confirmation window

Proxy Settings

When you want to send your feedback/log files from VQManager web interface to VQManager support team, Internet access is needed. In your enterprise network setup, you might need to go through a proxy server to access the internet. In such a case, you need to configure the username and password for internet access. This section explains how to carry out proxy configuration.

To configure proxy settings,

- go to "Admin" tab
- click "Proxy settings" icon

The parameters to be configured are:

- **HTTP Proxy Host:** Host name of the proxy server (eg: proxy-server)
- **HTTP Proxy Port:** Port number at which the server is running (eg: 80)
- **Username:** to access the internet
- **Password**

Testing Proxy Server Configuration,

After configuring the 'Proxy Settings', you can test if connection could be established with the proxy server. To test, just click the button "Test" of "Test Internet Connectivity". VQManager will attempt to establish connection with proxy server. If the configuration is proper and if VQManager is able to establish a connection, you will see the message "Proxy Server connection established successfully".

Database Administration

In typical production environments, VQManager would deal with a huge amount of data related to calls. The data gets piled up in the database and over a period of time, it becomes too high and might have a bearing on the performance of VQManager. Periodic database clean-up will help maintain VQManager performance. It is recommended to clean-up data older than a week, unless there is strong requirement to keep the data.

Database Clean-up

By default, VQManager cleans up data older than 1 week. The clean-up is done by default everyday at 1:00 am. After clean-up, the database would only have data for the last one week from clean-up date and time. There would be requirements to clean-up the database less frequently, or during different timings. This section allows one to configure the frequency and time of database clean-up.

Database Administration

Database CleanUp

▼ **Calls**

▶ **SIP Registrations**

Delete Calls data older than and run clean up based on,

Day Week

Run cleanup every day(s) at : (hh:mm)

To Schedule Database Clean-up

- Go to "Admin" tab
- Click the "Database Administration" icon under "Admin Settings" section

You can specify the minimum number of weeks or days whose data is to be kept in the database (by default, 1 week). This can be configured in the two drop-down lists found next to "CleanUp data older than" text. You can choose the number of days/weeks whose data is to be stored in the database from the first drop-down list. The second drop-down list allows you to select the interval - either "week(s)" or "day(s)" to store the data. Select the required interval to store information in the database.

The next two radio buttons "Day" and "Week", select the schedule option for clean-up - day or week.

To schedule clean-up in specific day interval

- If you wish to clean-up the database contents in specific day intervals - say, once in three days, this option would come in handy. You can choose an interval and also specify the time at which clean-up has to be done. To enable this option,
- click the radio button "Day"
- select the day interval
- select the time at which clean-up has to be done
- click "save". The required clean-up schedule is created

To schedule clean-up in weekly interval

- If you wish to clean-up the database contents in specific day intervals - say, once in three days, this option would come in handy. You can choose an interval and also specify the time at which clean-up has to be taken. To enable this option,
- click the radio button "Week"
- select the day of the week on which the clean-up has to be done (for example, every Monday)
- select the time at which clean-up has to be done
- click "save". The required clean-up schedule is created

SIP Registrations Clean-up

By default, VQManager cleans up SIP Registrations data older than 3 days. The clean-up is done by default everyday at 4:00 am. After clean-up, the database would only have registration data for the last three days from clean-up date and time. There would be requirements to clean-up the database less frequently, or during different timings.

Database Administration

Database CleanUp

To schedule registrations data clean-up

- Go to "Admin" tab
- Click the "Database Administration" icon under "Admin Settings" section
- Click on the 'SIP Registrations' slide. You can specify the minimum number of days whose registrations data is to be kept in the database (by default, 3 days). This can be configured in the drop-down list found next to "Delete registrations data older than" text. You can choose the number of days whose data is to be stored in the database from the drop-down list.
- select the time at which clean-up has to be done
- click "save". The required clean-up schedule is created

Bandwidth Monitor

If you want to monitor the traffic details in a particular interface or a group of interfaces of a particular host on a real-time basis, you can configure VQManager to do SNMP-based Bandwidth monitoring. The bandwidth utilization data provided by the interface would be shown as a report. You can configure the VQManager to poll the device on a periodic interval and show the traffic details on real-time basis. Two graphs, Traffic In and Traffic Out would be generated. It collects the bandwidth information and displays them on the UI on demand and it is maintained only for that session (maximum 25 minutes)

To configure SNMP bandwidth Monitoring,

- Go to "Admin" tab in the Web Client
- Click the link "Bandwidth Monitor"
- In the UI that opens, select the required time period for the report - Last 5 minutes, Last 10 minutes etc.
- Enter the hostname whose traffic details are to be monitored
- Enter the name of the interface
- Enter SNMP Port Number (161 by default)
- Enter SNMP Community
- Enter Polling Interval
- Click "Start Polling". You can now monitor the traffic details

General Settings

Operations like selecting a skin for the web client and editing account details have been classified under the category "General Settings".

Edit Account Settings

Users having an account with the VQManager, can change their own password and email ID. The "Edit Account settings" tab facilitates changing of password and email ID. Using this tab, the currently logged in user can change his/her password and email ID alone.

To Change Login Password,

- Go to "Admin" tab
- Go to "Edit Account Settings" in the "General Settings" tab on the left-hand side of the UI
- Enter the old password
- Enter new password
- Confirm the new password
- Click "Save"
- Password is now reset

To Change Email ID of currently logged-in user,

The currently logged-in users have the option to change their email IDs through the option provided in 'Edit Account Settings'

To change the email ID,

- Enter the desired ID in the text field for 'Email Address'
- Click 'Save'
- The new email ID would be in place

Skin Selector

By default, the web interface of VQManager come in 'Refreshy Blue' colour. Users have the option to choose four other skins - Classic Blue, Gray, Green and Saffron.

To change the skin from the default colour to another colour:

- Go to "Admin >> General Settings"
- Click "Skin Selector"
- Just select the required radio button and the required skin would be in place

Reports

Contents

- Overview
- Custom Reports
- History Data - Multiday Reports Summary
- Top Users (URL/PhoneID)
- Top Hosts (IP Address)
- Concurrent Calls Report
- Scheduled Reports

Overview

The 'Reports' section provides you the information on 'what is going on' in your VoIP network and how your VoIP network is performing. The status and summaries of the different activities are provided in the form of tables and graphs, which assist the administrators in making well-informed decisions and taking precautionary measures.

Broadly, VQManager provides four types of reports:

- Custom Reports
- Reports on Top Users
- Reports on Top Hosts
- Concurrent Calls reports

Custom Reports

Custom reports allow the user to select calls based on either the Initiator's or participant's or both their URLs, Names, IP Address and MOS scores. Reports on calls based on Call Status can be produced for exact Status Code or for the type of calls such as completed, unsuccessful etc.

Reports Concurrent Calls Report

▼ Custom Reports

Add Report Profile
1 - 6 of 6

- ▶ [Top Users \(URL/PhoneID\)](#)
- ▶ [Top Hosts \(IP Address\)](#)
- ▶ [Scheduled Reports](#)

Name	Created Time	View Profile	Delete
unmonitor_7days	Wed, 29 Apr 2009 14:46:45		
ErrorCalls	Tue, 28 Apr 2009 20:03:18		
7dayerrorcalls	Fri, 24 Apr 2009 19:50:52		
GoodQualityCallsReport	Mon, 1 Sep 2008 10:25:49		
UnsuccessfulCallsReport	Mon, 1 Sep 2008 10:22:52		
SuccessfulCallsReport	Mon, 1 Sep 2008 10:16:23		

View Custom Reports

- Go to "Reports" tab
- Under "Custom Reports" section, click on the custom report you want to view.
- To further drill down on reports click on the appropriate link

Adding a new Custom Report

- Go to "Reports" tab
- Click on the "Add Report Profile" link available on the Right hand side of the "Custom Reports" section
- Give a unique "Report Name" for the report to be created
- Select the duration from the drop down menu. You can use pre defined custom duration to create report for Today, Yesterday, Last 7 Days, Last 30 Days. Alternatively, you can define your own custom duration by selecting the dates between which you want the Reports to be generated.
- Select the report generation criterion from the first drop-down that has "URL" as its default. You can select from different criteria - URL / IP Address / Name / Call Status / MOS.
- The next drop-down list with "Initiator" as its default gives you the option of choosing from which end the reports are to be generated - Initiator / Participant / Both / Any

Note: The "Call Status" is independent of Initiator or participant.

- Select the filtering criteria according to the report generation option selected:
 - For " URL" and "Name" select one of "Contains / Does Not Contain / Starts with / Ends With"
 - For IP address, select one of " equals/ between"
 - For Call Status, select one of " equals/like"
 - For MOS, select one of " >= or <="

- In the final text-box, provide the values for the condition (URL / IP Address / Name / Call Status / MOS) to complete the custom report profile

Note: For report generation on 'Call Status', on selecting filtering criteria 'like', a drop-down list containing distinct call types is shown. You can select the required condition from this drop-down list. For reporting on Status Code specific calls, use the filtering criteria 'equals' and provide the exact Status Code in the text-box.

- To add multiple criteria click on the "Add Criteria" and follow the instructions given above
- If you want the filtering of reports on the basis of all the criteria mentioned by you, then select "Match all of the following", and when the filtering has to be done on any one of the criterion select "Match any of the following"
- You can choose the field you want in column, by clicking on the "Column Options" link on the right hand side of the UI
- A pop up window opens which lists the various column fields
- Check the fields required by you and un-check the ones that are not required.
- To order the columns according to your priority, select the field from the list and use the arrow buttons to move it Up / Down the order.

Note: Default rows in the columns are Initiator, Participants, Call Initiation Time, Code and MOS. These can be removed by un-checking them.

Setting Scheduled Generation and E-mailing of Custom Report

- Click on the check-box next to "Schedule&Email Options"
- To set the frequency of generation and emailing of the report, select one of the radio buttons – Hourly / Daily / Weekly / Monthly / Only Once. By default the reports are set to generate 'Only Once'
- Provide the time at which the reports are to be generated by entering the time in the "Generate report at/on" field:
 - If you are generating the report "Only Once" then provide the time at which the report is to be generated. The format is yyyy-mm-dd(date) 00:00(time). You can also click on the calendar icon next to the text-box to select the date and time. Choosing the date is similar to that in the main calendar as explained in "Setting the Client View Port". To choose the time, select on the hours or minutes and drag the mouse to the right to go ahead in time and drag to the left to go behind in time. Alternately, you can also keep clicking on the hours or minutes to go ahead in time. To go behind in time, keep clicking on the time with the shift button pressed down.
 - If you are generating the report 'Hourly', then provide the time at which this is to be done from the drop-down list for "Hrs" and "Mns"
 - If you are generating the report "Daily", provide the time in "Hrs" and "Mns" from the drop-down list
 - If you are generating the report on a "Weekly" basis, provide the day, "Hrs" and "Mns" from the drop-down list.
 - If generating the report on a "Monthly" basis, provide the "Date", "Hrs" and "Mns" from the drop-down list.
- The reports can be exported as pdf / xls / csv files. Select the type of file you want to export from the drop-down list, which has "pdf" as the default type.
- Provide the list of email Ids separated by commas to which the report is to be sent. Next to this text-box there is a drop-down list of "E-mail Ids" that has saved the frequently used E-mail Ids. You can select the E-mail Ids from this list too.
- Set the maximum file size "KiloBytes(KB)" that can be sent as attachment through E-mail. If the file size exceeds this set value, then the link for the file will be sent in the E-mail instead of the file as an attachment.

Add Report Profile

Report Name * during Today

Match all of the following Match any of the following [Select Columns](#)

URL for initiator contains

+ Add Criteria

Schedule & Email Options

Hourly Daily Weekly Monthly Only once

Generate report only once at the below specified time

Generate report at:

Export as:

Email To:

Note: If file size exceeds KiloBytes(KB), the URL of the file will be sent in the mail rather than an attachment

- After defining the criterion and scheduling the Generation and E-mailing, click on "Add" button to create the new report profile

Editing the Custom Report

- Go to "Reports" tab
- Under the "Custom Report" section click on the view icon adjacent to the report name, which you intend to edit.
- In the UI that opens you will be able to see the Summary for "New Report Profile"
- Click on the "Edit" button on the bottom of the page.
- Edit the changes you want to make and Click on the "Update" button to confirm the changes

Deleting the Custom report

- Go to "Reports" tab
- Under the "Custom Report" section click on the "Delete" icon adjacent to the report name, which you intend to delete.
- Once clicked a confirmation message pop up, asking you to confirm the deletion of the respective report
- Click "OK" to confirm the deletion

History Data - Multiday Reports Summary

The 'Multiday Reports Summary' view provides the summary of custom report profiles that are created for 'Last 7 days' or 'Last 30 days'.

Day	Call Count
Wed, 29 Apr 2009	1955
Tue, 28 Apr 2009	3732
Mon, 27 Apr 2009	2344
Sun, 26 Apr 2009	1425
Sat, 25 Apr 2009	1348
Fri, 24 Apr 2009	267
Thu, 23 Apr 2009	0

- For example, create a 'Custom Report' on 'Error Calls' for the 'Last 7 days'. From 'Reports' tab, click on 'Add Report Profile'. Create the report profile with the name 'ErrorCalls_7days' during 'Last 7 days' based on the criteria 'Call Status' like 'Error Calls'. Click on 'Add'.
- Now, from the 'Custom Reports' section, click on the 'ErrorCalls_7days' report profile. This will bring up the view having the call count details of the 'Error Calls' for each day. By clicking on the call count number link corresponding to a particular day, you can see the list of all the error calls for that day.

Top Users (URL/PhoneID)

This group of reports provides details regarding the flow of calls in the network - both incoming and outgoing. Reports in the form of graphs and tables are generated depicting:

- the users who made or received a large number of calls
- the users who made or received calls for long durations
- the users who consumed most bandwidth in terms of octets transferred
- the users who had good/poor quality QoS experienced in their calls

The reports have URL (for Users) represented along the X-axis and the number of calls/duration of calls/octets transferred/QoS values represented along the Y-axis. You can choose to view the top 10, 15, 20 or 25 talkers (users). By default, data pertaining to the current day would be displayed in the reports.

Reports Concurrent Calls Report

▶ Custom Reports

▼ **Top Users (URL/PhoneID)**

▶ Top Hosts (IP Address)

▶ Scheduled Reports

Top Users Reports by URL/PhoneID

<p>📊 Calls</p> <p>Outgoing Calls</p> <p>Incoming Calls</p> <p>Outgoing and Incoming Calls</p>	<p>📊 Duration</p> <p>Outgoing Calls Duration</p> <p>Incoming Calls Duration</p> <p>Outgoing and Incoming Calls Duration</p>
<p>📊 Octets</p> <p>Outgoing Octets Count</p> <p>Incoming Octets Count</p> <p>Total Octets Count</p>	<p>📊 Quality</p> <p>Poor Quality Users Report</p> <p>Good Quality Users Report</p>

- Available Reports" list by clicking on the respective checkbox
- Once selected, the reports will be added automatically to the "Selected Reports" list
- Use the "Remove" link to remove any reports from the "Selected Reports"

Setting scheduled generation and e-mail for selected reports,

- To set the frequency of generation and emailing of the report, select one of the radio buttons – Hourly / Daily / Weekly / Monthly. By default the reports are set to generate "Daily"
- Provide the time at which the reports are to be generated by entering the time in the "Generate report at/on" field
- If you are generating the report 'Hourly', then provide the time at which this is to be done from the drop-down list for "Hours" and "Minutes"

- If you are generating the report "Daily", provide the time in "Hours" and "Minutes" from the drop-down list
- If you are generating the report on a "Weekly" basis, provide the day, "Hours" and "Minutes" from the drop-down list
- If generating the report on a "Monthly" basis, provide the "Date", "Hours" and "Minutes" from the drop-down list
- Provide the list of email Ids separated by commas to which the report is to be sent. Next to this text-box there is a drop-down list of "E-mail Ids" that has saved the frequently used E-mail Ids. You can select the E-mail Ids from this list too. The reports will be extracted as 'pdf' files and e-mailed to the desired recipients
- After giving all the details, click on "Add" button to create the new scheduled report
- You can view the added reports by clicking the "Scheduled Reports" link from "Reports" tab

Editing the scheduled report,

- Go to the "Reports" tab
- Under "Scheduled Reports", click on the "Edit" icon adjacent to the scheduler name, which you intend to edit
- Edit the changes and click "Update"

Deleting the scheduled report

- Go to the 'Reports' tab
- Under "Scheduled Reports", click on the "Delete" icon adjacent to the scheduler name, which you intend to delete
- On clicking the icon, a confirmation message pops up asking you to confirm the deletion of the respective scheduled report. Click "Ok" to confirm the deletion

Data Export

The report generated by VQManager can be exported in CSV, PDF or as an email attachment. This feature lets the administrator export data to support long-term data storage and offline analysis.

To export reports click on the appropriate icon (CSV / PDF / Email) found at the top right side of the tabular columns. For CSV / PDF exporting, a the browser screen opens, on clicking the icon, prompting you to save or open the document directly.

When exporting the report as email attachment (pdf); specify the email ID (From, To, CC). A customized Subject and message can be incorporated. Type the email ID in respective field. Any new email ID will be automatically saved in mail settings.

Note: Email can be sent only after configuring the "Mail Setting Server". For configuring mail server and setting email ID's refer to "Mail Settings"

Concurrent call licensing

- The licensing model
- Is your licensing sufficient?
- How many dropped calls due to licensing limit?
- Concurrent call features

The licensing model

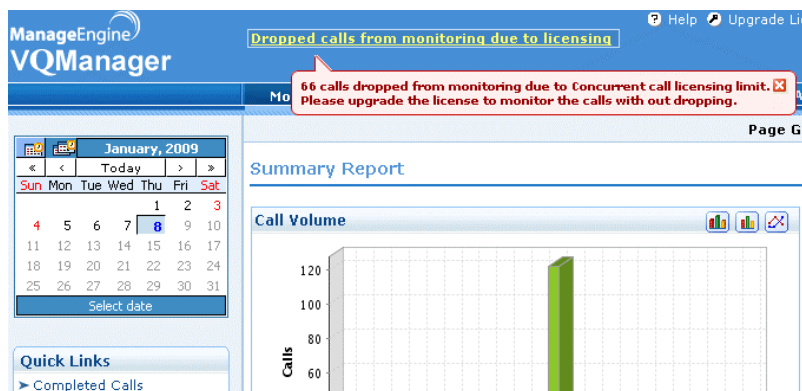
In addition to the licensing model based on Number of Endpoints/IP Phones, VQManager also provides a licensing model based on 'Concurrent Calls'. 'Concurrent calls' is defined as the number of simultaneous active calls captured by VQManager at any point of time. The 'Concurrent calls' based license is meant only for Service Provider customers who offer VoIP monitoring service to their end-user customers. This licensing model is based on the maximum number of concurrent calls in the network. For example, if a customer purchases a license for 100 concurrent calls, he/she can monitor at most 100 concurrent calls 'live' in their VoIP network at any point of time. Calls beyond that will not be monitored. For monitoring more calls, the customer will have to upgrade the license to a higher number of concurrent calls. This type of licensing is based on annual subscription, which means that usage of the product will be valid only for one year, beyond which the subscription has to be renewed.

Is your license sufficient?

After applying the concurrent call license, VQManager monitors all the calls happening in the network and at any instance, if the maximum concurrent call limit exceeds the licensing limit, VQManager drops the excess calls from being monitored. VQManager notifies on such dropped calls by displaying the message 'Dropped calls from monitoring due to licensing' on the VQManager web-client above the product's tabs.

How many dropped calls due to licensing limit?

VQManager provides information on the number of dropped calls in a tool tip which says 'x calls dropped from monitoring due to Concurrent call licensing limit. Please upgrade the license to monitor the calls with out dropping.'



Concurrent call features

Concurrent call report

VQManager provides a summary report on concurrent calls being monitored under 'Reports' tab -> 'Concurrent Calls Report'. Here one can find how many concurrent calls are happening in the network at any point of time.

Concurrent call alarms

There exists an option to trigger an alarm based on number of concurrent calls, this helps in notifying if number of concurrent calls greater than 'x' value and number of occurrences more than 'y' value to the user through an e-mail or by sending SNMP traps

Known Issues

The following are the Known Issues in VQManager:

- At present, VQManager supports the SIP, H.323 and Skinny signaling protocols only
- As of now, it is not possible to sniff VoIP packets on multiple interfaces
- Monitoring of conference calls are not supported
- The default Admin and Guest user accounts created by VQManager MUST be present for proper functioning of VQManager. These two accounts are not to be deleted. Other accounts created by the users can be deleted.
- At present, VQManager does not have provisions to verify the authenticity of RTCP information sent by the endpoints
- Currently, VQManager supports the CDRs generated by Cisco Call Tracker, Cisco Unified Communications Manager 6.1, Cisco Call Manager 4.0 & 5.0, Shoretel 6.1, Vovida Vocal, Asterisk, Avaya S8700, PortaOne, Swyx 6.0 and Tekelec 5.6
- The call flow diagram works only for sniffed calls
- Incomplete call Alarm Profile does not work for the CDR imported calls
- SIP messages over TCP are not supported
- In alarm detail view the number of call represented by the Total Call link may occasionally differ from the total number of calls displayed in Call Summary UI
- As of now, only SIP messages that take place through port configured in the "Sniffer Configuration" is supported - this should either be the source or destination port for the SIP traffic.
- When running the server in an external domain, at times, the alarm details page in web client appear scrambled in Firefox
- Browsing for a CDR file (for importing CDR through FTP) throws "Unparseable date" exception in Linux machines with different locale than that of the server machine
- In "Mail Settings" (Admin tab), after testing the mail server setup (using the test option), if you immediately carryout certain changes in "Email Notification Settings" and try to "Save Settings", the changes do not get saved. However, when you carryout changes in "Email Notification Settings" separately and click "Save Settings", the changes will be saved
- When more columns are added to the calls list, the reports generated in PDF report would look cramped. A maximum of 10 columns can be displayed without looking cramped in the PDF reports.
- In 'Custom Reports' and 'Predefined Reports', there may be inconsistency in importing calls data processed from CDRs
- While choosing the custom time period, like, from 2009-04-20 05:00 to 2009-04-21 23:59 or from 2009-04-20 05:00 to 2009-04-21 21:59) in Call Lists, the e-mail option will not work. The page shows 'No data available'.
- The password for the user accounts cannot be more than 10 characters long.

Troubleshooting Tips

Contents

- Installation, Startup and Shutdown
 - Web Interface
 - Miscellaneous
-

Installation, Server Start Up & Shutdown

- **Having GCC libraries incompatibility problems while installing VQManager in Linux distributions?**
 - Installation of VQManager 6.1 and above versions requires the standard C++ libraries (libstdc++) and GCC (4.0 or above) core libraries (libgcc). The following list contains the minimal Linux distributions that contain these libraries.
 - Red Hat Enterprise Linux 4.4
 - Mandriva 2006
 - Debian 4.0
 - Ubuntu 5.10
 - CentOS 5
 - SuSE Linux 10
 - Fedora Core 4
 - If you have the above mentioned or higher versions of Linux distribution and still have issues installing VQManager, kindly check if the libraries have been installed. You can confirm it by checking the presence of libstdc++.so.6 under the /usr/lib directory and libgcc_s.so.1 under the /lib directory. If they are not available, kindly install the libgcc and libstdc++ libraries from your Linux distribution CD.
 - If you have a lower version of Linux distribution and still wish to run VQManager, you need to compile and install GCC 4.0 or above. Follow the below mentioned steps to install GCC.
 - Download the GCC Core and GCC g++ version 4.0 or above from <http://ftp.gnu.org/gnu/gcc> and extract it to, lets say GCC_SOURCE_DIR.
 - Create two directories for building and installing GCC: `mkdir GCC_4_0_INSTALL ; mkdir GCC_4_0_COMPILE`
 - Move to the compile directory: `cd GCC_4_0_COMPILE`
 - Invoke the configure script: `<Absolute path of GCC_SOURCE_DIR>/configure --prefix=<Absolute path of GCC_4_0_INSTALL>`
 - After configuring, compile and install the GCC using the command "`make && make install`"
 - Run the command: `echo '<Absolute path of GCC_4_0_INSTALL>/lib' >> /etc/ld.so.conf`
 - Run `/sbin/ldconfig` to add the GCC install directory to the Linux library path.

- Install VQManager 6.1.
- **How to enable VQManager in Windows Vista?**

To enable the VQManager work correctly in the Windows Vista machine, the **WinPcap 4.1** needs to be manually installed. As this is still in beta version, this is not packaged along with the VQManager installer. You can get the WinPcap from the following location:
http://www.winpcap.org/install/bin/WinPcap_4_0_2.exe . This package needs to be installed after the VQManager installation so that the dlls are updated properly.

Server-startup fails

Cause: During the previous run, if you had terminated the server abruptly or there was an unclean shutdown, some of the server processes would not have been terminated and the MySQL server instance would continue to run in the system.

Solution: Forcefully terminate the MySQL Server instance (mysqld-nt.exe in Windows, mysqld in Linux).

Installation fails

Installation fails in Windows machine :

- Please check if you have administrator privileges to operate your Windows machine.
- Please take a screenshot of the error message that appears in the console when the installation fails.
- Also, zip the ' **logs** ' directory from **<VQManager_home> \logs** directory. (By default **<VQManager_home>** will be "**C:\AdventNet\ME\VQManager** ")
- E-mail the screenshot, the zipped '**logs**' directory and also the complete details of the system configuration to our support mail alias : vqmanager-support@manageengine.com

Installation fails in Linux machine :

- **Are you using 64 bit processor?**
 - VQManager currently works with only 32 bit processors irrespective of the Linux flavour used. For VQManager to work in your 64 bit machine, you will need to install the appropriate 32 bit java library packages for your machine. After installing the 32 bit libraries, try installing VQManager again.
- **Installation fails even in 32 bit processor Linux machine**
 - Check md5sum value of bin (**md5sum ManageEngine_VQManager.bin -->** For that you need to open a command prompt where ManageEngine_VQManager.bin is saved). For

example, if you are installing the build 6.1.2, then confirm that the md5sum value of the bin installer is the same as **3bb73a3d69ee83a973a07bafa62836d7**. If you are installing a build above 6.1.2, then please check the md5sum value from the below link
<http://www.manageengine.com/products/vqmanager/download.html>.
 If the md5sum value is not the same, please download a fresh copy of the bin installer and try installing it again.

- The installation may also fail due to insufficient space in temp directory. To overcome this problem create a directory say " **temp** " in the partition having enough space and pass the absolute path of the temp directory as a argument to the binary file. For example, In command prompt,
 \$: **mkdir /root/temp**
 \$: **./ManageEngine_VQManager.bin -is:tempdir /root/temp**
- If you are still not able to install VQManager, please generate a log file by following the below procedure and e-mail this file to our support mail alias : vqmanager-support@manageengine.com
 - Create a text file with the same name as that of the installer with extension as " **.sp** ".
 - For a binary file `ManageEngine_VQManager.bin` , create a text file named **ManageEngine_VQManager.sp** .
 - **Open** the `ManageEngine_VQManager.sp` text file in a editor and add `is.debug=1` as the content. **Save** the `ManageEngine_VQManager.sp` text file in the same directory, where the binary file resides. Change to the directory where the binary file is present.
 - Invoke the installer as **`./ManageEngine_VQManager.bin -is:javaconsole -is:log log.txt`**
 - The above command will create a text file named `log.txt` under the directory where **`ManageEngine_VQManager.bin`** installer file is present.
- Also send us the complete details of your system configuration.

- **When I uninstall the product in windows, some folders are not getting deleted.**

Cause: This usually happens when you try to uninstall the product immediately after shutting down the server.

Solution: Ensure that you uninstall the product only after the MySQL Server Instance (`mysqld-nt.exe` process in Windows Task Manager) has been terminated completely after the server shutdown.

Web Interface

- **I am unable to access VQManager Server through the Web Interface. Why?**

Cause	Solution
Incomplete server start-up	Ensure that the server has successfully started. This can be verified by the presence of the message "Connect to: [http://localhost:8647]" in the console. Connect to the web client after seeing this message.
Wrong URL	VQManager server and the Web Interface communicate through http. So ensure the URL contains HTTP. http://<hostname>:port/ For e.g. http://localhost:8647
Do you see any failure messages in the Server Console?	Send the log files to the VQManager Support team, through the Support tab in "Support File Creation"

- **My Web Interface looks crippled**

Cause	Solution
Incompatible Browser	Refer to the System Requirements, and check whether your browser is supported.
JavaScript not enabled	JavaScript has to be enabled in your browser for you to work with the Web Interface.

Miscellaneous

- **I am not able to see any calls on the UI.**

This requires a number of checks:

- Verify whether the sniffer "Interface Name" (found in "Admin" tab -> "Sniffer" icon) that the client is listening to, is receiving all the VoIP traffic in your network. Select the right interface that receives all the VoIP traffic (refer to "Configuring Sniffer").
- To have all VoIP traffic flowing to this interface that VQManager listens on, you will have to enable port-mirroring in your network switch to mirror all traffic to this sniffer interface. This link has information on configuring port-mirroring in a number of managed switches like 3Com, Cisco Systems, Linksys, NETGEAR, Avaya etc.
- Make sure a VoIP Call is started in the network. Only after updating the Sniffer Configuration will VQManager show call data for the calls. Refresh the page to check for any call information to be displayed
- If no call information is displayed, check the default SIP Port Configuration in the sniffer configuration. By default the SIP Port Configuration is "5060"
- Check the default Skinny Port Configuration. By default the Skinny Port

- Configuration is "2000"
 - Check the default H.323 Port Configuration. By default the H.323 Port Configuration is "1720"
 - If the VoIP Network has VLAN setup then update the "Filter Strings" to tcp || udp || vlan
 - If still no call information is seen, check whether the protocol used is SIP or Skinny or H.323. VQManager currently supports the SIP, Skinny & H.323 protocols only
- **I am getting the following error, though I am running my Windows system with administrator privilege:**

"Insufficient privilege. Unable to find the interface details. Please run the server in administrator privilege mode and try again."

Cause: The above error occurs if the sniffer is unable to determine the list of network interfaces in your machine. This could be the case of incompatible Winpcap libraries loaded in the system

Solution: To resolve this, verify the version of **npf.sys** file in your machine. This is available in the **c:\windows\system32\drivers** folder. Right click on the file and look into the 'Version' tab. If the version shown is **4.0.2** or above then it is compatible with VQManager, otherwise you may need to install a fresh copy of WinPcap to make the VQManager work properly. Please install the new WinPcap **AFTER** installing VQManager.

- **I do not see any QoS information in VQManager UI**

Cause: Your network is not generating any RTCP packets or only one end is generating RTCP packets.

Solution: VQManager can calculate QoS metrics based on RTP packets also. Ensure that "**RTP based QoS Calculation**" option is enabled. Go to Admin tab, click on Sniffer link to view the Sniffer Configuration. To edit the setting click on the "**Edit**" button below.

- **In the Monitored Endpoints UI (Free and Licensed Users), add IP Phone shows "maximum number has been reached" though the actual count is less than the licensed amount**

Cause & Solution: This can happen when the server has discovered an IP phone during its processing. Refresh the page to get the latest user list.

- **I did not receive any e-mails configured in Alarm Notification and Reports**

Cause: This usually happens when the Mail Server Settings are not configured properly.

Solution: Configure the Mail Server Settings. Refer Mail Server Settings section for more details.

- **I get "The sendSupportFile ProxySettingsError occurred." error message when sending the support information file**

Cause: This usually happens when the Proxy Settings are not configured properly.

Solution: Configure the Proxy Settings. Refer Proxy Settings section for more details.

- **There is no link for "Monitored Endpoints" in the Admin tab and I am running the VQManager trial edition.**

Cause & Solution: In the trial edition, there is NO limitation on the number of IP Phones to be monitored. You can monitor VoIP calls from all your IP Phones. Therefore, the "**Monitored Endpoints**" link does not appear when the product is run in trial version mode. Once, the trial version expires, you'll have an option to choose the IP Phones to be monitored.

- **I encounter problems in reinitializing VQManager**

Cause: Reinitialize script/batch file is to be invoked only when the server is not running. At times, a lock file named **.lock** gets created under **<VQManager_Home>/bin** directory . This creates problems when reinitializing the server even when it is not running.

Solution: Make sure you are not attempting to reinitialize while the server is running. Navigate to **<VQManager_Home>/bin** (by default, VQManager is installed in C:\AdventNet\ME\VQManager) directory and check if **".lock"** file had been created. If so, remove it.

SIP CODES

Informational Responses

Status Code	Message
100	Trying
180	Ringing
181	Call being forwarded
182	Queued
183	Session progress
200	OK

Success Responses

Status Code	Message
300	Multiple choices
301	Moved permanently
302	Moved temporarily
303	See other
305	Use proxy
380	Alternative service

Client Error Responses

Status Code	Message
400	Bad request
401	Unauthorized
402	Payment required
403	Forbidden
404	Not found
405	Method not allowed
406	Not acceptable
407	Proxy authentication required
408	Request timeout
409	Conflict
410	Gone
411	Length required
413	Request entity too large
414	Request URL too large
415	Unsupported media type

420	Bad extension
480	Temporarily not available
481	Cell Leg or Transaction Does Not Exist
482	Loop Detected
483	Too Many Hops
484	Address Incomplete
485	Ambiguous
486	Busy Here

Server Error Responses

Status Code	Message
500	Internal server error
501	Not implemented
502	Bad gateway
503	Service unavailable
504	Gateway time-out
505	Version not supported

Global Failure Responses

Status Code	Message
600	Busy everywhere
603	Decline
604	Does not exist anywhere
606	Not acceptable

For a more detailed explanation of the SIP codes, refer to:
<http://www.faqs.org/rfcs/rfc3261.html>

VOManager custom codes

Status Code	Description
SIP - Request Packets	
2002 Invite	Indicates that the client sends a invite request for a call establishment to the SIP server and waiting for the response from the SIP server.
2004 Cancel	Client can ask the SIP server to cancel a request which it sends previously by sending Cancel request. (Ex. Client can ask the SIP server to cancel a call INVITE request which it sends previously for a call establishment by sending the CANCEL request.)
SIP - Registration Requests	
1010 Registering	The Registering status states that the client has requested the SIP registrar for registration and waiting for the response from the SIP-Registrar.
1011 Registered	Client is registered with the SIP Registrar

1012 UnRegistering	The UnRegistering status states that client has requested the SIP registrar for unregistration and waiting for the response from the SIP-Registrar.
1013 UnRegistered	Client is unregistered with the SIP Registrar.
Other Codes	
999 Active	By receiving the OK packet for the Invite request, the call is moved to Active state.
1000 Completed	By receiving the SIP-BYE packet(call tear down packet), a call is marked as Completed call
8000 Marked as Unmonitored By User	If the user manually marks the active calls to the Unmonitored state(using the 'Mark as Unmonitored' button in the 'Active Calls' list, these calls will be moved to the 'Unmonitored calls' category)
8001 Unmonitored due to Server Restart	If the VQManager server was re-started, the calls which were in the active state at the time of re-start will be grouped in the 'Unmonitored calls' category.
8002 Unmonitored due to Sniffer Restart	If the Sniffer was re-configured manually while some calls were active, then these active calls will be grouped in 'Unmonitored calls' category.
8003 Unmonitored due to no media transmission	If no signalling packets were received by VQManager for a certain time interval then the call would be moved to the 'Unmonitored calls' category.
8004 Unmonitored due to licensing	In concurrent call based licensing, if more calls are initiated at the same time and the number of active calls equals the concurrent call licensing limit, then all the excess initiated calls will be moved to this unmonitored state
8100 Media Transmission Stopped	If the call is established successfully and initially there is some RTP/RTCP packet transfer and then the RTP/RTCP packets reception or the signaling termination packets reception stopped for a certain time interval, then the call will be marked as 'Media Transmission Stopped' and moved to the 'Completed Calls' category.

Contacting Technical Support

The **Support** tab gives you a wide range of options to contact the Technical Support team in case you run into any problems.

Link	Description
Request Technical Support	Click this link to submit a form from the VQManager website, with a detailed description of the problem that you encountered
Support File Creation	Click on the " create" button to open up a support form that can be sent to the Technical Support team. A ZIP file containing all the server logs will also be attached to this form. If required*, you can also generate and attach a packet capture of your network traffic. You can then send this form and ZIP file to vqmanager-support@manageengine.com . In the form provide your E-Mail ID and press the send button.
Troubleshooting Tips	Click this link to see the common problems typically encountered by users, and ways to solve them
User Forums	Click this link to go to the VQManager user forum. Here you can discuss with other VQManager users and understand how VQManager is being used across different environments. The latest discussion posts are displayed here too.
Need a Feature	Click this link to submit a feature request from the VQManager website
Toll-free Number	Call the toll-free number +1-925-924-9500 to talk to the VQManager Technical Support team directly

Add packet capture file to support log information

Support File Creation

To send the file to VQManager Technical Support team, provide details below and click 'Send'.

To : vqmanager-support@manageengine.com

Email:

Name:

Phone:

Comments:

Add packet capture file to support log information

Interface Name:

Time of Capturing : or Maximum of packets

Filter String:

Note: Support file creation may take sometime depending on the load of the server and the size of the log files. Keep this window open and let the server run while support log file creation is in progress.

A packet capture file containing a few complete calls taken on the VQManager-listening-interface(NIC) helps the support team analyze if the interface(NIC) properly receives the complete signaling traffic (SIP/Cisco Skinny/H.323) and media traffic(RTP/RTCP). To create the packet capture file and send it to the support team, please follow the below steps.

- In VQManager webclient, under the 'Admin' tab --> 'Proxy Settings', please make sure that your proxy server settings are configured correctly.
- Under the 'Support' tab, click on 'Create the latest support information file'.
- Enter the details in the support form window that opens up.
- Check the 'Add packet capture file to support log information' option. By default, the interface which VQManager's sniffer is currently listening to will be chosen.
- For 'Time of Capturing' choose a value from '30 secs' to '15 mins' from the dropdown menu and for the 'Maximum of' packets option, choose a value from '5000' and '500000' packets from the dropdown menu. The default filter string will be "tcp || udp || vlan".
- Support File Creation and sending process will take time depending on the load on the server and the size of the log files. Please do not close the support form window till the process is complete.

Once the support log files and packet capture are sent to our support team, we will analyze it and report on our observations.

At any time, you can click the **Feedback** link in the top pane, to send any issues or comments to the VQManager Technical Support team. You can also send an email to vqmanager-support@manageengine.com to let us know about your problem.

Note:

*A packet capture is sometimes needed by the VQManager Technical team to fully troubleshoot any reported issues by replaying and analyzing the same in the test labs. You can also generate and attach a packet capture of your network traffic while sending the support file. This is done by enabling the check box Add packet capture file to support log information in the support file creation form. Select the interface(NIC) you want to capture traffic from, by default this interface is the one that the VQManager sniffer is configured with. By default a 30 second capture(or a maximum of 5000 packets) is generated and attached. You can have a bigger capture by selecting a longer duration of capture or limiting the capture to a higher number of packets. The default string used for the capture is `tcp || udp || vlan` and this can be changed by using similar syntax as those used in WinPcap or Pcap captures.

Release Notes

Release Notes for VQManager 6.2.1

- Release Notes for VQManager 6.2
- Release Notes for VQManager 6.1.2
- Release Notes for VQManager 6.1.1
- Release Notes for VQManager 6.1
- Release Notes for VQManager 6.0
- Release Notes for VQManager 5.2

Release Notes for 6.2.1

Enhancements

- Enhanced endpoints processing for better performance and improved the page loading time 2x times faster.
- Provided option for importing PhoneIDs of the Endpoints/IP Phones/Subscribers list
- Improved the QoS calculation by ignoring the RTP duplication packets
- Introduced a new navigation component for easy access of huge volume of records for all list views

Bug Fixes

- Issue in SIP header processing for SIP-BYE packets is fixed
- Fixed the issue with Cisco Unified Communication Manager (CUCM) 6.x , 7.1 CMR record processing

Release Notes for VQManager 6.2

New Features

Licensing

- New Licensing model based on 'Concurrent Calls' exclusively for 'Service Providers'.

Reports

- Ability to create 'Schedulers' for predefined reports and e-mail them as PDF files.

Web Interface

- New User interface for 'Reports' tab for better usability.
- New history(summary) view added for multiday Calls and Registrations data.

- Added Concurrent calls reports in the Quick links across all tabs for easy one-click access.
- Added 'Multiday views' in Custom reports.

Others

- Added support for processing Avaya S8700 CDRs, Cisco Unified Communications Manager(CUCM) 6.1 and 7.0 CDR formats.
- New and improved data storage mechanism and database schema to cater to huge volume of data stored across multiple days.
- Improved Server side processing of raw packets by introducing buffering mechanism.
- Product is made as multi-threaded application for effective utilization of the available RAM and processor of server box.

Enhancements

- Optimized Database writing queries.
- Handling duplicated RTP/RTCP media packets to avoid incorrect QoS metrics calculations.
- Separate 'SIP Registrations' processing logic to reduce the overhead in Call Processing thread.
- Support for monitoring calls from tel:
- Improved page loading time for 'SIP Registrations'.
- Improved usage of MyIsam tables along with InnoDB for better performance in DB Write & Read operations.
- Introduced new logic for data collection for Custom reports for optimal performance.
- Improved SIP and SCCP packet processing to cater to different VoIP Environments.
- Proper handling of H.323 calls with 'UndefinedReason' call termination packets.
- Efficient 'Database Clean up' policy with 1/100 th reduction in cleanup time, especially for huge volumes of data stored in DB.

Bug Fixes

- User Interface alignment bugs fixed.
- Fixed few use cases related issues in 'unmonitoring' calls in conference call scenarios.
- Duplication in 'Alarms' fixed.

Release Notes for VQManager 6.1.2

Enhancements

- Included a new, separate clean-up option for registrations. The clean-up policy by default deletes registration data older than 3 days.
- Included a new alarm profile based on concurrent calls.
- No more are calls categorized as 'illegal calls' with status code 9000.
- Redesigned the reports page to make it more readable and for easy access.

Bug Fixes

- VQManager needs at-least one Admin and Operator level account for its proper functioning while creating new users. Hence deleting the default Admin & Guest user is disabled.
- Fixed various User Interface alignment issues.

Release Notes for VQManager 6.1.1

Enhancements

- Introduced enhancement in deriving jitter statistics from the RTP streams to avoid spurious values.
- Introduced enhancement in deriving delay statistics.
- Provision to add more than three criteria while defining a custom report profile.
- Added few default custom report profiles namely *GoodQualityCallsReport*, *SuccessfulCallsReport*, *UnsuccessfulCallsReport*.
- Removed categorization of calls with Status Code 9000
- Themes are modified for better user experience.

Bug Fixes

- Processing of Cisco CDRs received as syslog messages fixed.
- Fixed call processing failure when 'Auto-discovery' is disabled in the 'Monitored Endpoints' section.
- The problem with reporting of monitored endpoints in the bandwidth and voice quality reports is fixed.
- The reports exported as a pdf file having wrong time in the file name is fixed.

Release Notes for VQManager 6.1

New Features

- Support for H.323 protocol
- Concurrent calls reports
- Configuration wizard for easy set-up
- Voice Quality graphs enhanced with drill-down options
- Full support for Cisco CallManager 6.x environments

Enhancements

Performance

- SIP registration views enhanced to load pages faster

Calls Monitoring

- Option to auto-end calls whose RTP flows stopped for 'x' duration
- Option to "unmonitor" calls with no signaling packets for 'x' duration
- User given the option to manually "unmonitor" stale active calls
- Option to delete stale active calls
- Proper processing of calls that originate from PSTN phones and terminating in SCCP Phones
- Displaying the reason for calls to be moved to the unmonitored state for better understanding

Endpoint details

- Additional listing of Endpoints by their phone ID
- Better formatting of Octets transfer in a call

Licensing

- Licensing based on number of unique phone IDs discovered
- Option to import monitored phone IDs from a CSV/TXT files
- Option to export the monitored Phone IDs as CSV

Web Interface

- New log-in screen
- Default Monitor tab view changed to "Summary Report" view

Bug Fixes

- Issue in scheduling the database clean up task has been fixed
- Support for parsing SIP URL with upper and lower case
- Fixed the issue while configuring a MOS Trend based alarm profile with SNMP trap enabled
- Fixed the issue on entering duplicate email ids in a same threshold while creating an Alarm profile creation
- Issue while creating PNG images in Windows Vista machine has been fixed
- Fixed an issue in generating PDF/CSV files for endpoints containing special characters

Miscellaneous

- Option to create and send a packet capture from the VQManager web interface
- Changed the JAVA version bundled with VQManager to JRE 1.5.0._11
- System requirements: Linux distributions used needs standard C++ libraries (libstdc++) and GCC (4.0 or above) core libraries (libgcc)

Release Notes for VQManager 6.0

New Edition

- VQManager Professional Edition released

New Features

- Support for Cisco Skinny protocol
- Windows 64-bit support
- Scheduled export of Custom Reports
- CallFlow information is enhanced with the addition of raw SIP and Skinny packet information.

Enhancements

Performance

- Call processing rate enhanced to cater to higher call traffic loads
- All client views are enhanced to load the pages faster

Calls Monitoring

- Controlling of Refresh rate for Active calls and Live Reports
- Configurable QoS parameters for Call Trend View graph

Endpoint details

- Resource Group Menu bar added in the Endpoint tab's Navigation bar
- Current Status of each Endpoint is not shown in the Endpoints summary list

Alarms

- Alarm categorization based on Severity

Reports

- Call Status based Custom Reports
- Removed Live Reports from the Reports tab

Administrator Operations

- Time Zone setting removed
- Automatic scheduled backup of data is removed

CDR Processing

- Auto-download of new CDR files from directories via FTP
- Support for PortaOne CDRs

Web Interface

- New Monitor page UI with Live & Summary split-up
- Live Reports View to get a snapshot of the current status of the network
- Alarm categorization based on Severity in Monitor Page
- Better representation of Voice Quality and Traffic monitor graphs
- Refresh Page now option
- Frequently Used Devices, Recent Calls, Recent Alarms and Top Talkers views are removed from the Monitor page.
- Revamp of the Syslog server settings page
- Endpoint details are enhanced with a more in-depth information.
- Revamp of the Quick Links section

Bug Fixes

- Fixed the issue of VQManager stopping the display of calls after a week's run
- Calls are moved to unmonitored state if VQManager doesn't detect any activity (like RTP packets) for more than 5 minutes. This avoids showing the completed calls in the active calls page.
- Fixed the issue of the Mail Server Setting not getting effected in the Alarm Generation

Release Notes for VQManager 5.2

New Features

- Support for efficient database administration with provision for scheduled Database backup & cleanup
- Support for running VQManager server as service in Linux

Enhancements

Sniffer

- Support for Network Address Translation (NAT)
- Support for call processing in multi-VLAN networks
- Processing of abbreviated SIP-Headers enabled

Alarms

- Provision for filtering the time component into 'Business Hours' and 'Non-Business Hours' and generating alarms based on the same
- Provision for MOS Trend based alarm generation
- Enhanced SIP error code based alarm profile with provision to 'exclude' SIP code in 'like' condition

CDR Processing

- Support for importing directories in CDR log import
- Support for parsing of the Swyx 6.0 & Tekelec 5.6 CDRs

Web Interface

- Status Code based search enabled in all call list views
- Initiator, Participant URLs and Minimum, Maximum & Average values of QoS metrics have been added as optional columns in all call list views
- Minimum, Maximum & Average values of QoS parameters are shown in all call details and endpoint details
- Provision for setting VQManager time zone based on user's time zone
- Enhanced pre-defined reports with addition of two new reports - Bandwidth Usage Report and Voice Quality Report
- Enhanced licensing policy with support for limiting the endpoints by 'Incoming and Outgoing SIP-URL'

Bug Fixes

- Earlier, in the case of RTP ringing tones, zero values were shown for Packet Count and Octet Count (pcount/ocount). This issue has been fixed.
- Earlier, high packet loss values were shown in the call start up for RTP ringing tones. This has been fixed.
- Hitherto, call flow was depicted until receiving RTCP-bye only. Henceforth, it would extend till receiving SIP-Bye.
- In some instances, Codec was shown as UNKNOWN despite the presence of codec data. This has been fixed now.
- The calls that remained "Active" while shutting down the server, have been moved to the 'UnMonitored Calls' category.
- In the case of calls of very short duration, there were some memory leak in the server. This has been fixed.
- When one tries to import an already imported CDR file again, only the difference between the two versions, if any, would be parsed to avoid duplication of calls.
- Earlier, giving same name for a custom report and a resource group was not allowed. This issue has now been fixed.
- Earlier, the Syslog-CDRs were not persisted in the database. Henceforth, they will be persisted in the database.
- Earlier, there were issues in launching the VQManager web client from the windows tray-icon. This has now been fixed.

Changes

- SIP registrations are not processed by default. It can be enabled through Sniffer Configuration UI
- Login & Admin pages have been revamped

Support - Helps in Troubleshooting

Contents

- Overview
 - Support
 - Voice Back
 - Change password
-

Overview

The Support tab guides you to contact VQManager team, in case, you run into issues while using the product.

Support

- Provides useful information to troubleshoot issues
- When you encounter issues with VQManager and if you wish to report the same to the VQManager support team, log files related the issue would be of great help in getting to the root of the issue. You can create the log files by clicking the "Create" button in the "Support File Creation"
- Latest server log files are created in the form of a zip and the URL for downloading the zip file would be displayed. You can download the zip and send it to VQManager support team
- If the size of the log files are huge, it will take some time to get uploaded

Voice Back - Instant Feedback

VQManager Team is eager to hear your feedback, suggestions and comments about VQManager. You may use the "Voice Back" form present in the top-right corner of the web-interface to send us your feedback. Click "Voice back", fill-in the details and click "Send". Your feedback would reach us.

Change Password

For the currently logged in users, option is provided to change their own password.

To change password,

- click "Change Password" link present in the top-right corner of the web-interface
- in the UI that opens, enter the old password, new password, confirm the new password
- modify the email id (if required)
- click "Save"

Themes

The VQManager is equipped with pre-installed themes to suit your preferences. These themes are multicolor to enhance the contrast and make the visibility better. You can choose any of the themes according to your choice.

Activating Themes.

- Locate the "**Themes**" link on the top right hand side corner of the client.
- Click on the "**Themes**" and select the desired theme.
- The requested theme gets loaded automatically.

Working With VQManager

Contents

- Overview
 - Topics Covered in this section
-
-

Overview

After connecting the web interface with the VQManager server, the VQManager Home Page is displayed. The web interface is arranged in the form of seven tabs. Through these tabs, you can perform various monitoring operations of VQManager. This section provides brief information about each of the tabs.

Before proceeding to monitor the calls in your network, you need to decide the way in which you are going to provide the call information to the VQManager. This section explains this and also deals with the calendar component in VQManager, which plays a powerful role.

Topics Covered in this Section

- Obtaining Call Information
- Setting Client View Port
- VQManager Web Interface
- Monitoring Vital Parameters
- All about Calls
- Alarms - Alerting the Administrator
- Endpoints - Reports on VoIP Terminals
- Administrative Operations
- Reports
- Data Exporting