



Genesys Quality Management 8.1

Implementation Guide

The information contained herein is proprietary and confidential and cannot be disclosed or duplicated without the prior written consent of Genesys Telecommunications Laboratories, Inc.

Copyright © 2009–2013 Genesys Telecommunications Laboratories, Inc. All rights reserved.

About Genesys

Genesys solutions feature leading software that manages customer interactions over phone, Web, and mobile devices. The Genesys software suite handles customer conversations across multiple channels and resources—self-service, assisted-service, and proactive outreach—fulfilling customer requests and optimizing customer care goals while efficiently using resources. Genesys software directs more than 100 million customer interactions every day for 4000 companies and government agencies in 80 countries. These companies and agencies leverage their entire organization, from the contact center to the back office, while dynamically engaging their customers. Go to www.genesyslab.com for more information.

Each product has its own documentation for online viewing at the Genesys Technical Support website or on the Documentation Library DVD, which is available from Genesys upon request. For more information, contact your sales representative.

Notice

Although reasonable effort is made to ensure that the information in this document is complete and accurate at the time of release, Genesys Telecommunications Laboratories, Inc., cannot assume responsibility for any existing errors. Changes and/or corrections to the information contained in this document may be incorporated in future versions.

Your Responsibility for Your System's Security

You are responsible for the security of your system. Product administration to prevent unauthorized use is your responsibility. Your system administrator should read all documents provided with this product to fully understand the features available that reduce your risk of incurring charges for unlicensed use of Genesys products.

Trademarks

Genesys, the Genesys logo, and T-Server are registered trademarks of Genesys Telecommunications Laboratories, Inc. All other trademarks and trade names referred to in this document are the property of other companies. The Crystal monospace font is used by permission of Software Renovation Corporation, www.SoftwareRenovation.com.

Technical Support from Genesys

If you have purchased support directly from Genesys, please contact Genesys Technical Support at the regional numbers provided at the end of this document. For complete contact information and procedures, refer to the [Genesys Technical Support Guide](#).

Ordering and Licensing Information

Complete information on ordering and licensing Genesys products can be found in the [Genesys Licensing Guide](#).

Released by

Genesys Telecommunications Laboratories, Inc. www.genesyslab.com

Document Version: 81gqm_implementation_4-2013_8.1.511.00



Table of Contents

Chapter 1	Introduction	7
	Document Purpose	8
	Audience	8
	Document Version	8
	Typographical Conventions	9
	Expected Knowledge	9
	Browser Recommendations and Technical Requirements	10
	Internet Explorer Security Settings:	11
	Technical Requirements for Playing Audio and Video Media	12
Chapter 2	Important Pre-requisites for Installation	13
	Checklist for All Installations	14
	Checklist for all types of CUCM Recording	14
	Checklist for Passive Recording on Cisco	14
	Checklist for Active Recording on Cisco	14
	Checklist for Genesys GIM, MSR and EPR	15
	Checklist for Genesys EPR	15
	Checklist for Active Recording with Avaya Communications Manager	16
	Operating System	16
	License checklist	16
Chapter 3	GQM Setup and Configuration	17
	Beginning the Setup and Configuration Process	19
	Configuration from a Cache File	21
	Manual configuration	23
	Selecting GQM Services	24
	Service List	25
	Cisco JTAPI, Genesys MSR and EPR	28
	Contact Center Integration	29
	Key Manager	30
	Databases	31

Oracle Configuration	32
GQM Server IP Address	34
Single Server Configuration	35
Integration Modules and Drivers	36
Cisco Unified Communications Manager	37
Downloading JTAPI Library from CUCM (JTAPI Signaling)	39
Entering the settings for the Genesys IM	41
Entering the Settings for Genesys EPR	43
Entering the Genesys MSR Settings	45
Entering the Avaya Settings	47
Packet Sniffing	49
PostgreSQL - Database Locale Settings	50
PostgreSQL - Remote Database Connections	52
SMTP Server	56
Increase Tomcat Server Memory	57
Call Recording Automatic Startup	58
Generate Self-signed Certificate and Keys	59
Restarting Call Recording	60
Verifying the Configuration	61
Completing Configuration	62
Starting Call Recording Services	64
Important Note on Synchronization	66
Setting a Custom Locale for the Web Server	67
Chapter 4 Licensing and Activating GQM	69
Launching the Call Recording Web GUI	70
Activating Call Recording	72
Uploading the Un-Activated Call Recording License File	74
Activating an Un-Activated Version of Genesys Call Recording	76
Restarting Call Recording	78
Activating Quality Manager	79
Open Quality Manager in a Web Browser	80
Log In as Administrator	81
Uploading the Un-activated Quality Manager License File	82
The Activation Key	83
Uploading the Activated Quality Manager License File	84

	Configuring Quality Manager in the Call Recording GUI	85
	Basic Settings	86
	Rounding Strategy	88
Chapter 5	Configuring Genesys Driver for Recording	89
	Setting up Genesys Driver	90
	Setting the Operation Mode in Genesys Driver	91
	Setting up Tenant Specific Parameters	93
	Adding Tenant Information	94
	Default Tenant Configuration	95
	DN Activity Detection	96
	Configuring DN Activity Detection	98
	Configuring Notification of Recording	99
	External Data Available from CIM	101
	Setting Genesys Driver Encoding for Attached Data	102
	Basic Call-related Data	103
	Call-related User Data	106
	User data configuration	107
	Agent Configuration Data	108
	Extension Data	111
	Other Genesys Driver Data	112
	Configuring Full Agent Name Assembly	113
	External Data	114
Chapter 6	Integrating Genesys CIM with GQM Using GIM	117
	Genesys Passive Recording	118
	Installing the Genesys Integration Module	119
	External Data Available from Genesys CIM for GIM	120
	Setting GIM Encoding for Attached Data	121
	Configuring the Integration Module	122
	Configuring the Application Names and Address for GIM	123
	Configuring the T-Server and Configuration Server for GIM	124
	Configuring the DN Range for Attached Data	126
	Configuring Notification of Recording for GIM	128
Chapter 7	Configuring Avaya Driver for Recording	131

	Setting up Avaya Driver	132
	Viewing and Configuring the AES Server Settings	133
	Configuring the TSAPI Interface	135
	Configuring the DMCC Interface	136
	Adding and Configuring the Recorder Groups	137
	Configuring the Recorder Settings	139
	Settings for Multi Server Installations	140
	Configuring the Terminal Activity Detection	141
Chapter 7	Fixpayloads	143
Chapter 8	Request Technical Support	145

Chapter

1

Introduction

This chapter provides an overview of this document, identifies the primary audience, introduces document conventions, and lists related reference information.

This chapter contains the following sections:

[Document Purpose](#)

[Audience](#)

[Document Version](#)

[Typographical Conventions](#)

[Expected Knowledge](#)

[Browser Recommendations and Technical Requirements](#)

[Internet Explorer Security Settings:](#)

[Technical Requirements for Playing Audio and Video Media](#)

Document Purpose

This document describes the basic implementation of the Genesys Quality Management 8.1.5x solution and operating system on one server. Advanced configuration and integration with third party applications are described in other documents for example the *Call Recording Administration Guide*.

The instructions in this document are expressly aimed at ZOOM Certified Implementation Engineers and should not be attempted by unqualified persons.

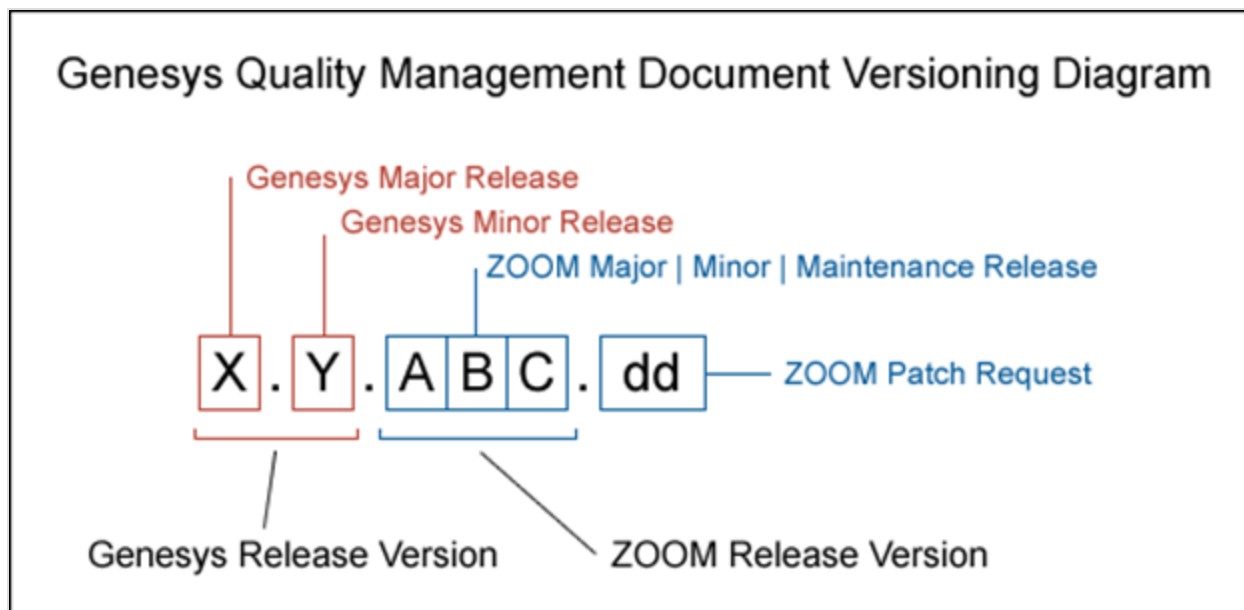
Audience

This document is intended for the technicians responsible for system installation and its preparation, on behalf of administrators who will then configure and administrate the system

Document Version

The Genesys Quality Management products are provided by a partnership between Genesys and ZOOM International. The Genesys Quality Management products use a versioning format that represents a combination/joining of the versions used by these two separate entities. Although the Genesys Quality Management products and documentation use this combined versioning format, in much of the software and logs you will see the ZOOM versioning alone. You need to be aware of this, for example, when communicating with Technical Support.

The version for this document is based on the structure shown in the following diagram:



Typographical Conventions

Names of functions and buttons are in bold. For example: **Upload**.

File names, file paths, command parameters and scripts launched from the command line are in non-proportional font.

Referred documents are in italics. For example: see the document *This is a Document* for more information.

Code is placed on a gray background and bordered

Hyperlinks are shown in blue and underlined:

<http://genesyslab.com/support/contact>.

Expected Knowledge

Readers of this document are expected to have the following skills or knowledge:

- Basic knowledge of the options and possible configurations of Genesys Quality Management as stated in the Datasheet
- Knowledge of *Red Hat Enterprise Linux* installation and configuration

- Unix system administration skills
- Network administration skills

Browser Recommendations and Technical Requirements

A minimum screen resolution of 1024 x 768 is necessary to use the GQM applications comfortably.

The following supported browsers are recommended for the Web GUI. The Windows Media Player is needed for Call Recording. The Java plugin is required for Universal Player in Quality Manager.

The browsers for PCs are shown in order of preference. The fastest performing browsers are first:

1. *Google Chrome*: Please download the latest version. Check issues using the latest browser version before reporting them. The user must install the *Windows Media Player* plugin below:

<http://www.google.com/support/chrome/bin/answer.py?hl=en&answer=95697>

2. *Internet Explorer 9*

3. *Internet Explorer 8* with *Google Chrome Frame* plugin. The *Google Chrome Frame* plugin can be obtained here:

<http://code.google.com/chrome/chromeframe/>

4. *Internet Explorer 7* with *Google Chrome Frame* plugin. This version of IE should be upgraded to IE9 as soon as possible.

5. *Firefox 3.6.16+* Admin rights required for installation. The user must install the *Windows Media Player* plugin below:

<http://www.interoperabilitybridges.com/windows-media-player-firefox-plugin-download>

6. *Opera 9+*

7. *Safari 5*

8. *Internet Explorer 8* without the *Google Chrome Frame* plugin. The performance is slow.

The following browsers are not recommended:

Internet Explorer 7 without the *Google Chrome Frame* plugin runs too slowly.

Internet Explorer 6 is not supported.

Use Safari or Firefox with Mac OS 10.

Important:

Web browsers require a media player plug-in (*Windows Media Player* 9+ for Windows PCs, *VLC* for Macs and Linux) for audio and video media review, and at least *Adobe Flash Player* 9.x runtime installed for viewing reports.

Internet Explorer Security Settings:

Windows XP

The following recommendations are encouraged for the Web GUI running on Windows XP:

- Check that the Call Recording URL is included in the "Trusted sites". If not, include it there. If the user doesn't have administrator privileges, contact the system administrator or set security level of the zone that contains the server to Low.
- Check that there is no proxy enabled in the web browser. If there is, try to disable it. The proxy can affect the functionality.
- Set the security level of trusted sites to Low.

Windows 7

The following recommendations are encouraged for the Web GUI running on Windows 7:

- Check that the Call Recording URL is included in "Trusted sites". If not, include it there. If the user doesn't have administrator privileges, contact the system administrator or set security level of the zone that contains the server to Low.
- Check that there is no proxy enabled in the web browser. If there is, try to disable it.
- Set the security level of trusted sites to Low.
- Disable protected mode for all zones. If protected mode is Enabled for the internet zone, it affects the functionality, even if the server is in trusted sites, this is for Internet Explorer only.

Technical Requirements for Playing Audio and Video Media

The following media players are recommended for successful video and audio playback.

The media players are listed in order of preference, for the reasons supplied below:

1. *Microsoft Windows Media Player*: Plays all audio and video media on the Windows 7 OS. Previous versions of Windows, for example, Vista and XP, need additional codecs to play video media.
Download the K-Lite Codec Pack (BASIC or BASIC Mirror versions) from: http://www.free-codecs.com/K_Lite_Codec_Pack_download.htm.
2. *VLC*: Plays combined video and audio recordings, including dual-screen recordings of 1920x1080 or larger. It is not integrated into browsers, for example, *Internet Explorer* and *Firefox*, for audio playback. *VLC* is recommended for Macs and Linux-based systems for combined audio and video reviewing. *VLC* can be downloaded at: <http://www.videolan.org/vlc/>.
3. *QuickTime*: Plays audio and is integrated into *Internet Explorer*, but does not support playing mp3 audio and H.264 format video together for combined audio and video playback.

Chapter

2

Important Pre-requisites for Installation

Before you start installing GQM you must :

- Configure the call center platform (Avaya Communications Manager, Genesys CIM) for integration to GQM, if integration is required.
- install a licensed version of the Red Hat Linux (RHEL) 6.2 operating system according to instructions in the Pre-implementation Guide.
- Pre-configure CUCM in your call center (if required).
- Pre-configure SPAN ports (if required).

All these pre-implementation procedures are covered in detail in the Pre-implementation Guide.

To ensure a successful installation result, check that the relevant items in the following checklists have been performed during the pre-implementation phase:

Checklist for All Installations

- Has your administrator assigned the IP address and net mask for the eth0 Network Interface Card (NIC) on the GQM server?
- Is there network connectivity between the soft switches and the GQM server?
- Has your administrator assigned the gateway, primary, and secondary DNS addresses for the GQM server?
- Has your administrator assigned a hostname for your GQM server?

Checklist for all types of CUCM Recording

- Have you created an application user and password for JTAPI communications for your GQM server?
- Have you added groups and role permissions to the application user? This user must have privileges to see all users to be recorded or monitored.

Checklist for Passive Recording on Cisco

- Have you pre-configured the SPAN ports?

Checklist for Active Recording on Cisco

Have you:

- Created a recording profile?
- Enabled BIB (Built in Bridge) to allow monitoring or recording on all phones and devices to be recorded?
- Enabled recording for each line? A phone or device can have several numbers, each number must be configured separately.
- Configured the recording profile and trunk route pattern according to the CUCM active recording configuration?

Checklist for Genesys GIM, MSR and EPR

Have you pre-configured the SPAN ports (if required)?

Have you added the `CallREC_GIM` Application Template into the Configuration Manager?

Do you have:

- The T-Lib primary server address?
- The T-Lib backup server address?
- The Config primary server address?
- The Config backup server address?

Have you added a new person (username and password) in the Genesys Configuration Manager for Call Recording to communicate with Genesys?

Have you set up an application name in Genesys Call Manager for GIM?

Checklist for Genesys EPR

Have you set the `rtp-info-password` in the Genesys T-server configuration?

Checklist for Active Recording with Avaya Communications Manager

Do you have:

- The AES server Address
- The CM server address
- A TSAPI user name and password
- A DMCC user name and password
- The IP Station security code

Operating System

Have you installed the Red Hat Linux operating system?

License checklist

Have you received a license file from Genesys Support?

Important:

You must satisfy all pre-requisites that relate to your installation before installing GQM.

Chapter

3

GQM Setup and Configuration

This chapter describes the Setup and Configuration process

This chapter contains the following sections:

[Beginning the Setup and Configuration Process](#)

[Configuration from a Cache File](#)

[Manual configuration](#)

[Selecting GQM Services](#)

[Oracle Configuration](#)

[GQM Server IP Address](#)

[Single Server Configuration](#)

[Integration Modules and Drivers](#)

[Packet Sniffing](#)

[PostgreSQL - Database Locale Settings](#)

[PostgreSQL - Remote Database Connections](#)

[SMTP Server](#)

[Increase Tomcat Server Memory](#)

[Call Recording Automatic Startup](#)

[Generate Self-signed Certificate and Keys](#)

[Restarting Call Recording](#)

[Verifying the Configuration](#)

[Completing Configuration](#)

[Starting Call Recording Services](#)

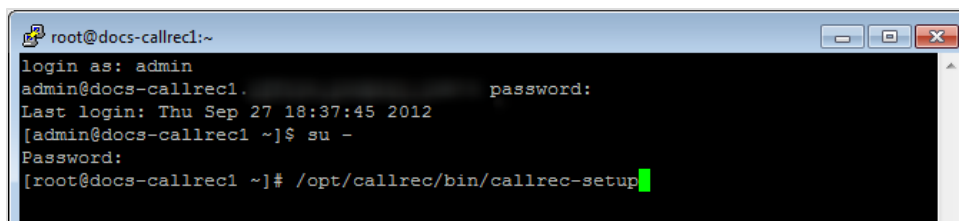
[Important Note on Synchronization](#)

[Setting a Custom Locale for the Web Server](#)

Beginning the Setup and Configuration Process

Access the Call Recording server via an ssh client for example PuTTY.

To begin the setup and configuration process on the Call Recording server:



```
root@docs-callrec1:~  
login as: admin  
admin@docs-callrec1. password:  
Last login: Thu Sep 27 18:37:45 2012  
[admin@docs-callrec1 ~]$ su -  
Password:  
[root@docs-callrec1 ~]# /opt/callrec/bin/callrec-setup
```

Figure 1: Logging In and Starting GQM Setup

1. Type your administrative login and password, login: `admin`, password: `zoomcallrec`.
2. Switch to the root user account by typing `su -` and enter the password (default: `zoomcallrec`):

Important:

You are strongly recommended to change the root password from the default to a new one of your own.

3. Type `/opt/callrec/bin/callrec-setup` at the command line and press **Enter**.

GQM setup starts, asking if you want to start Call Recording (GQM) configuration.

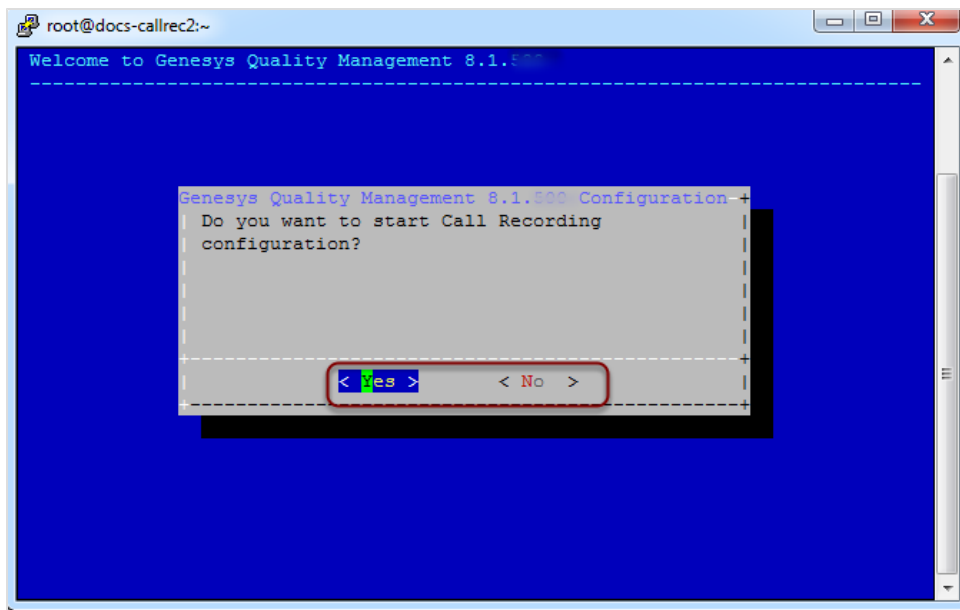


Figure 2: GQM Setup Confirmation

4. Select **Yes** to continue or **No** to abort setup.

Important:

If you need to change any of these settings later, you can either run this setup again (the setup remembers the values entered earlier) or edit them manually, either through the Call Recording Web GUI Admin Interface (preferred) or directly in the configuration files.

If you want to edit these values manually outside setup, please refer to the Call Recording Administration Guide for more information.

Configuration from a Cache File

If your configuration information is saved in a cache file, you can save time by using this file to configure GQM.

Important:

For first-time installations without a cache file, please proceed to [Manual Configuration](#).

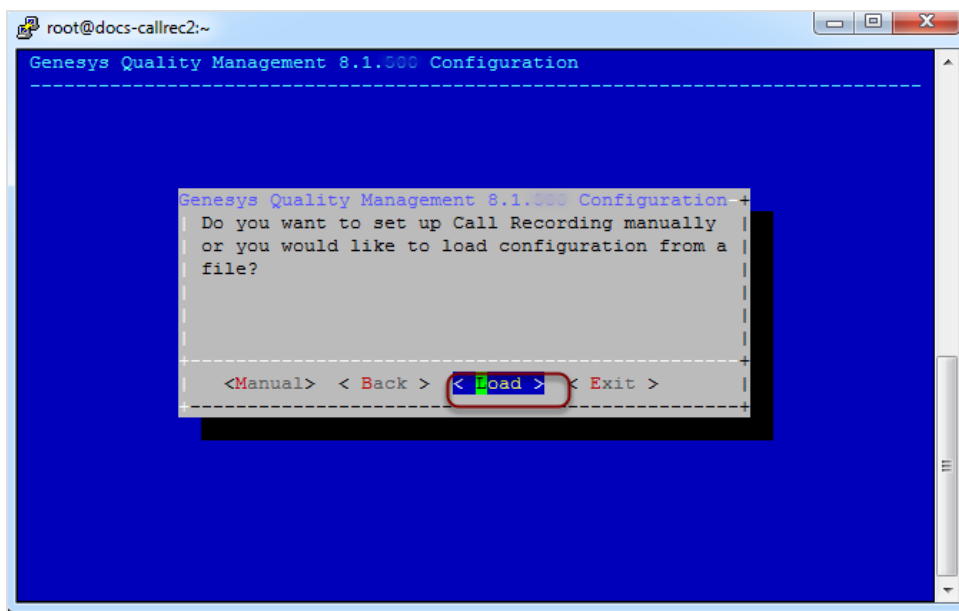


Figure 3: Configuration from a Cache File

Select **Load**.

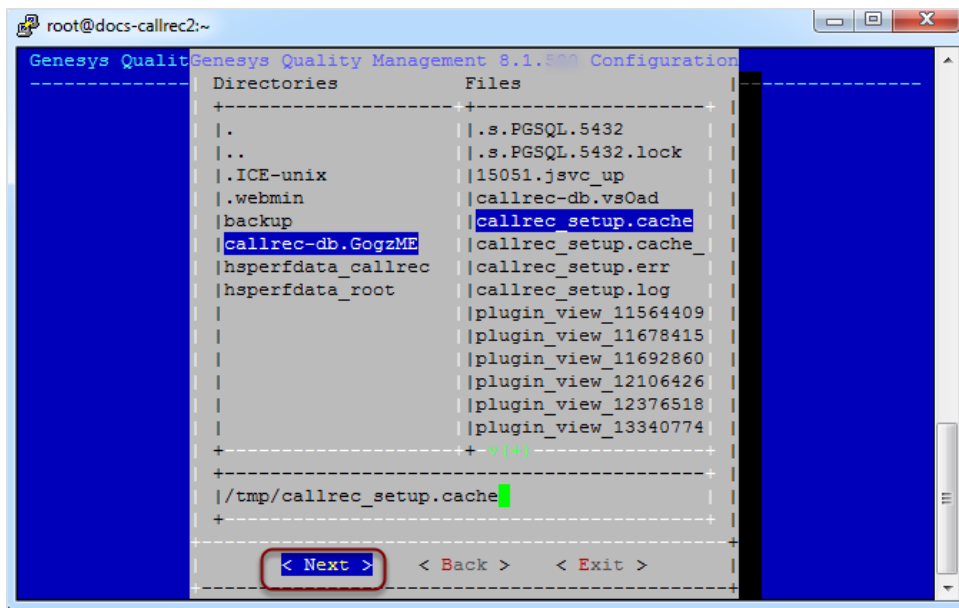


Figure 4: Selecting the Cache File

1. Navigate to your cache file.
2. Click **Next**.

GQM setup uses the cache file to load your configuration settings.

The GQM Configuration Verification screen appears.

- Verify your settings, and click **Next** to complete the configuration.
- Refer to [Completing Configuration](#) in the Manual Configuration section.

Manual configuration

Important:

If you have configured GQM from a cache file, you do not need to manually configure GQM.

GQM configuration and setup requires information about the operating environment to function properly. Before you begin, be sure you have all the IP addresses, user names, and passwords for your existing infrastructure.

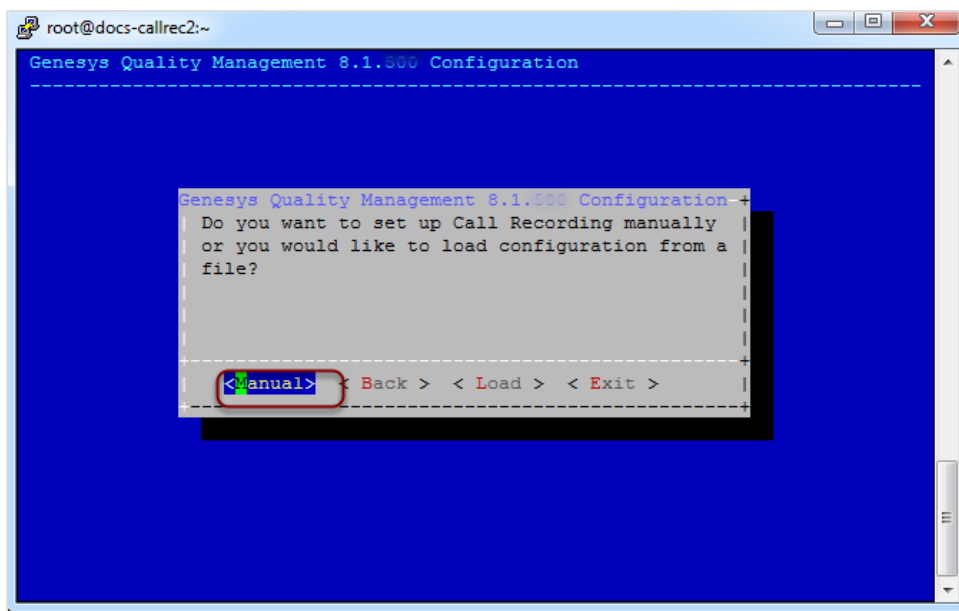


Figure 5: Selecting Manual Configuration

Select **Manual** to begin manual configuration.

Selecting GQM Services

GQM offers a number of services. The services available for configuration depend on your license and environment. See the next section for a full list of services.

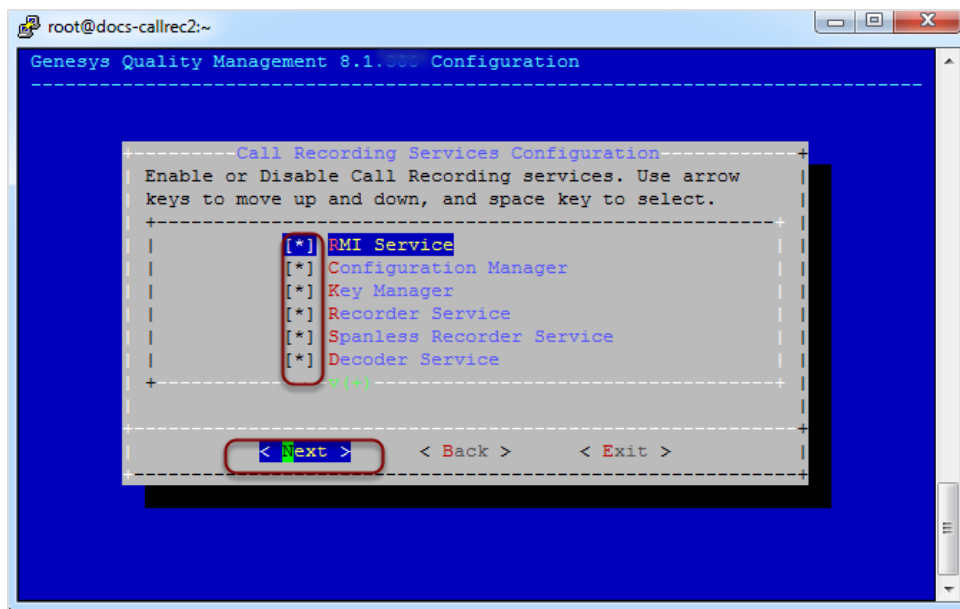


Figure 6: Selecting GQM Services

Use the arrow keys to scroll up and down through the list.

Please see the [Service List](#) section to evaluate which services may be combined. Ensure that each individual item is selected or not selected according to your requirements. For example, if you have purchased Quality Manager then you must select the Quality Manager service.

1. Use the space bar to select or unselect services.
2. Select **Next** when you have finished selecting the services.

Service List

The following table lists the GQM services that are available for selection.

Service	Type	Notes	Proviso
RMI Service	Core	RMI Service is always installed so that the modules within Call Recording can communicate with each other. Contains the naming service.	
Configuration Manager	Core	Configuration Manager is installed in all cases apart from clustered recorder and decoder servers and provides a standard configuration file system.	
Key Manager	Security	Provides call and screen key encryption and decryption to comply with PCI DSS.	
Recorder Service	Recorder	Records calls from network SPAN ports.	Do not select for MSR.
Spanless Recorder Service	Recorder	Records calls using Active recording technology.	You must select the Spanless Recorder Service for MSR do not select the Recorder Service
Decoder Service	Decoder	Decodes the PCAPs and encodes the media to MP3 files.	
Core Service	Core	Provides the business logic for all recording operations. Core service is always installed on a single server installation. Every cluster must have one server with core installed.	
Cisco JTAPI Service	Active Driver	Enables Call Recording to use attached data from CUCM.	If you select this service do not select EPR, or MSR. You must already have access credentials to CUCM to configure this service. Please see Implementation Guide for details.

Service	Type	Notes	Proviso
Cisco Skinny Service	Protocol	Enables Call Recording to sniff Cisco Skinny protocol data for information about calls.	If you select this service do not select EPR, or MSR services.
Genesys EPR Service	Active Driver	Connects to Genesys T-Server for Enhanced Passive Recording This driver also provides Genesys CIM integration.	If you select this service do not select MSR, JTAPI, SIP, Skinny, or GIM services. You must add a new user (username and password) for Call Recording to communicate with Genesys Configuration Manager.
Genesys MSR Service	Active Driver	Connects to Genesys T-Server for Media Stream Replication services. This driver also provides Genesys CIM integration.	If you select this service do not select EPR, JTAPI, SIP, Skinny, or GIM. You must add a new user (username and password) for Call Recording to communicate with the Genesys Configuration Manager.
Avaya Service	Active Driver	Connector to Avaya Communication Driver. You may combine this driver with the GIM service if you require integration with Genesys CIM to provide attached data.	If you select this service do not select EPR, MSR, JTAPI, SIP, or Skinny Services. You must have user for communication with TSAPI and a user for communication with DMCC.
SIP Service	Protocol	SIP service enables Call Recording to sniff SIP data information about calls.	If you select this service do not select EPR, or MSR services.
Speech Recording Service	Speech Recording	Main speech analysis and search application.	
Web Service	GUI	Tomcat server for Call Recording and Quality Manager GUI.	
Apache HTTPD		For large installations. Provides load balancing when there are a lot of users and multiple Tomcat servers.	
Genesys IM Service	Integration Module	Genesys CIM integration, often used with the SIP service	If you select this service do not select EPR, or MSR. You

Service	Type	Notes	Proviso
			must add a new user (username and password) for CallREC to communicate with Genesys in the Genesys Configuration Manager.
Synchro Service	Synchro	Call and Screen synchronization tool for cluster configurations.	
Screen Capture Service	Screen Recorder	Server-side screen recording component.	
Media Encoder Service	Encoder	Encodes raw screen data into MP4 files .	
Tools Service	Tools	Maintenance (MLM) tools scheduling service.	
Fixpayloads Service	Payloads	Enables the recovery of couples where there are different Codecs in each stream.	
Instreamer Service	Other	Barix Instreamer service provides interface to record analogue lines.	
Database Service	Database	Embedded PostgreSQL database.	If you select this service do not select Oracle Database Client
Oracle Database Client	Database	Client for connecting to external Oracle databases.	If you select this service do not select Database Service
Quality Manager	Quality Manager	Main Quality Manager web application	

Table 1: Available QM Suite Services

Some of these services, for example Quality Manager, require license activation. For information concerning licenses please contact your Genesys Sales Representative for more details.

Cisco JTAPI, Genesys MSR and EPR

If you select the JTAPI service, you must already have a Call Recording username and password enabled in your Cisco Unified Communications Manager (CUCM). See the section on Cisco CUCM Preparation in the *QM Pre-installation Guide* for more details.

Similarly, the Genesys MSR and EPR service require pre-defined Call Recording user credentials to be enabled in your Genesys Configuration Server.

Contact Center Integration

The list of chosen GQM services also determines the choice of Call Center integration you require (if any). The following integration modules may be enabled at this point. As with signaling, configuration occurs later on in the installation process:

- Genesys Contact Center Suite, CIM
If Genesys CIM is being used with Genesys T-Server, use Genesys Driver for MSR (Media Stream Replication) or EPR (Enhanced Passive Recording) service for more stable and powerful integration.

Important:

If selecting the Genesys Driver for the MSR (Media Stream Replication) or EPR (Enhanced Passive Recording) service, ensure that all other protocol adapters and drivers are unselected (that is. JTAPI, SIP, Skinny, GIM)

Key Manager

The Key Manager service is selected by default, but only used to manage authentication keys and certificates as part of the PCI-DSS licensed feature. If your installation does not need PCI-DSS compliance, then this service can be disabled. See the GQM Security Guide for more information about PCI DSS compliance in Genesys GQM.

Databases

GQM supports two popular database systems for differing implementation scenarios. You may select either PostgreSQL, or Oracle, during setup.

- **PostgreSQL**
 - Is suitable for small to medium call centers.
 - Is configured during setup as a local embedded database.
 - Select **Database Service** in the services list (and unselect **Oracle Database Client**).
- **Oracle**
 - Is suitable for large and enterprise call centers.
 - The client connection to an external database is configured during setup.
 - Select **Oracle Database Client** in the services list (and unselect **Database Service**).
 - For more information about installing GQM with Oracle, including data migration, refer to the Using Oracle guide.

Oracle Configuration

If the **Oracle Database Client** service was selected, a screen now appears requiring Oracle database parameters. If you have selected the PostgreSQL database, please skip this step.

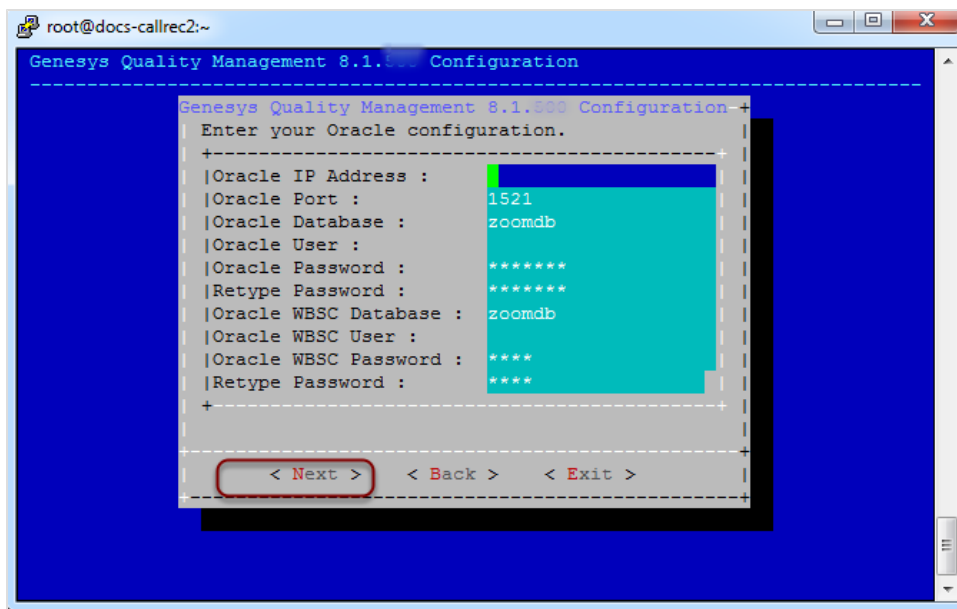


Figure 7: Oracle Database Configuration

The following Oracle connection parameters are shown:

1. Type the following:
 - **Oracle IP Address**. (This can also be the Oracle server's fully qualified domain name, for example).
Type the **Oracle Database** (the Call Recording database or service name). This can also be in the following format:
`//SERVER:PORT/SERVICE_NAME`
 - **Oracle User** (the Call Recording schema user),
 - **Oracle Password** (the Call Recording schema user password). Enter the password twice.
 - **Oracle WBSO Database** (the Quality Manager database or service name). This can also be in the following format:
`//SERVER:PORT/SERVICE_NAME`
 - **Oracle WBSO User** (the Quality Manager schema user).

- **Oracle WBSC Password** (the Quality Manager schema user password). Enter the password twice.

2. Click **Next** to continue.

See the *Using Oracle* guide for more information about Oracle-related installation, parameters and setup procedures.

GQM Server IP Address

Insert the GQM server IP address, which is shared by all GQM components in a standalone server deployment. This IP address is used in a number of network settings in system configuration.

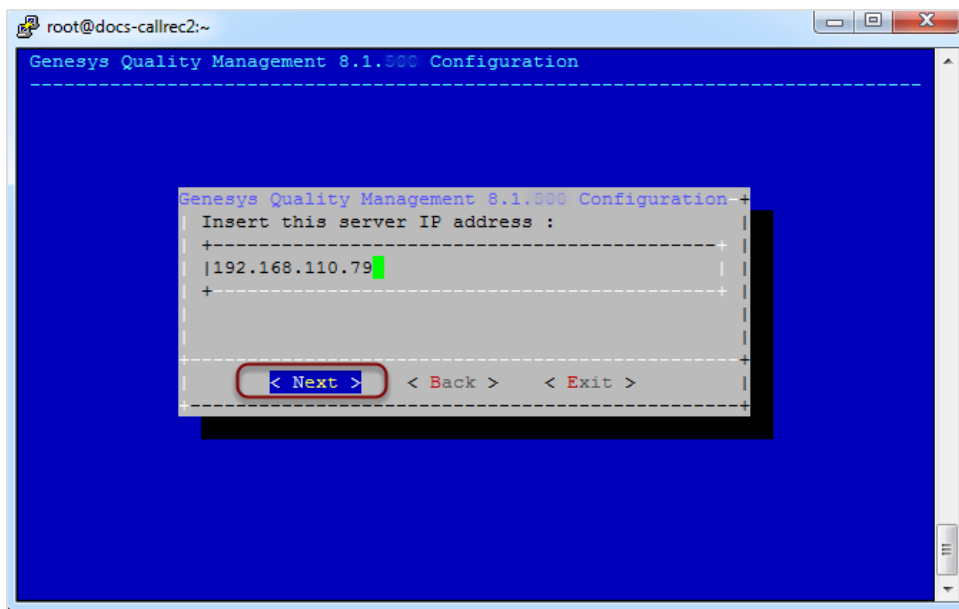


Figure 8: QM Suite Server IP Address

1. Type the IP Address.
2. Select **Next**.

Single Server Configuration

Important:

GQM is typically installed on a single server. You can also install GQM in Cluster and Redundant configurations. This implementation guide only covers single server installation. To install GQM on multiple servers, please contact Genesys Support:

<http://genesyslab.com/support/contact>

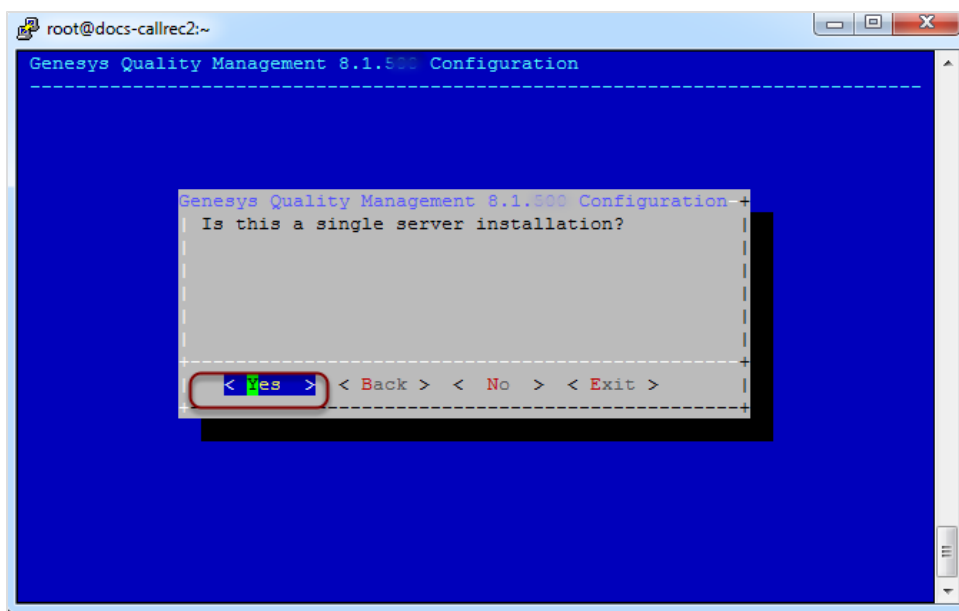


Figure 9: Selecting Single Server Configuration

- Select **Yes** to begin the single server installation.
- Selecting **No** requires additional configuration steps that depend on your network topology and environment, and which cannot be properly documented in this implementation guide. Refer to the Planning Guide for more information.

Integration Modules and Drivers

At this point in the installation process, any contact center integration modules that were selected (enabled) during the GQM Services step are configured. Depending on your selection, the following steps will appear (you may skip this section if no integration was specified).

Cisco Unified Communications Manager

If you did not select the JTAPI signaling service earlier, this will not appear during installation.

To utilize JTAPI signaling, you must identify your Cisco Unified Communications Manager (CUCM) configuration.

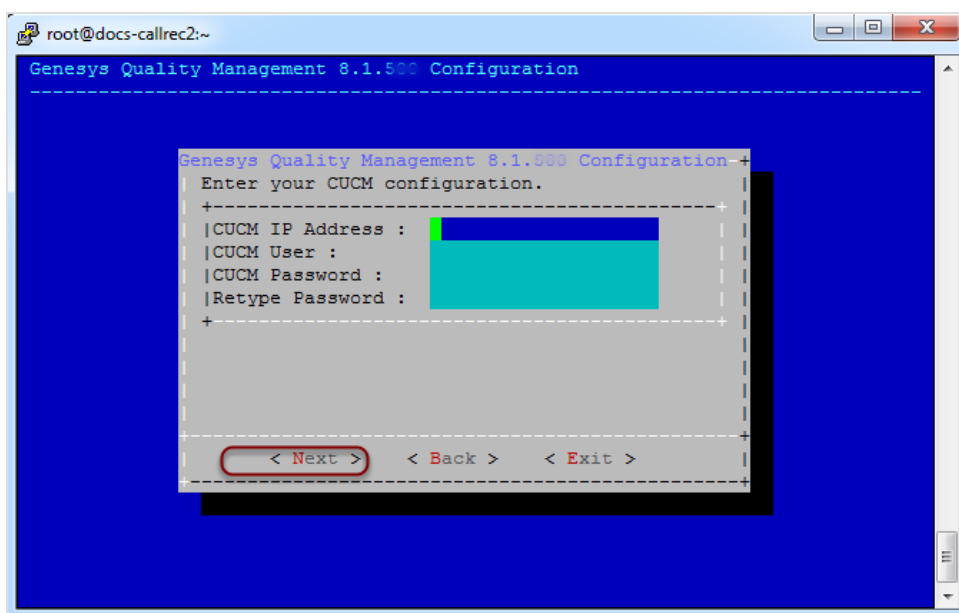


Figure 10: CUCM Configuration

1. Type:
 - Your **CUCM IP Address**.
 - A valid **CUCM User name**.
 - A valid **CUCM Password**.
 - Retype the valid **CUCM Password**.
2. Select **Next**.

Important:

More than one CUCM IP address can be entered, separated by commas, for example:

192.168.123.12,192.168.123.14

Both CUCM Publisher and Subscriber IP addresses can be entered in this way, ensuring the Subscriber will be used if the Publisher IP fails.

Downloading JTAPI Library from CUCM (JTAPI Signaling)

If the JTAPI signaling service is not selected, it does not appear during installation.

After the CUCM configuration settings are entered, the system prompts to download the Cisco JTAPI library from CUCM.

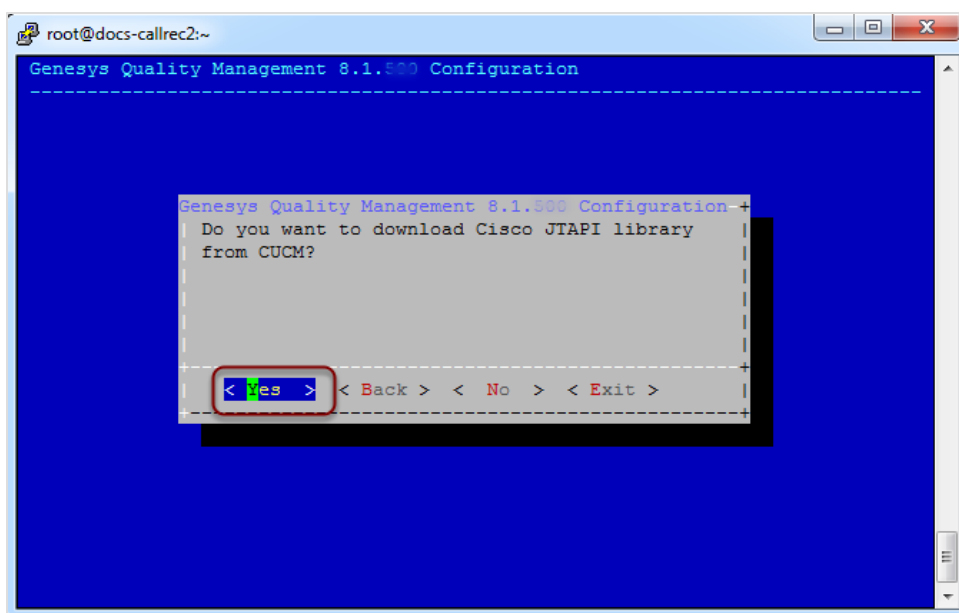


Figure 11: Download JTAPI from CUCM Configuration

Select **Yes**.

The system attempts to download the JTAPI library at the end of the setup procedure. If multiple Cisco Unified Communications Manager servers are specified during setup, each are contacted in turn until a successful download is obtained. No feedback is given if this operation is successful.

Not downloading the Cisco JTAPI library from CUCM, or failure of the automatic download during setup, requires downloading it manually with the following command after setup finishes, but before Call Recording is started do not select the option to restart Call Recording after setup finishes: `/opt/callrec/bin/get-jtapi`.

Important:

Without the JTAPI library, Call Recording cannot record calls using the JTAPI signaling protocol.

Entering the settings for the Genesys IM

If you did not select the Genesys IM service earlier, this will not appear during installation.

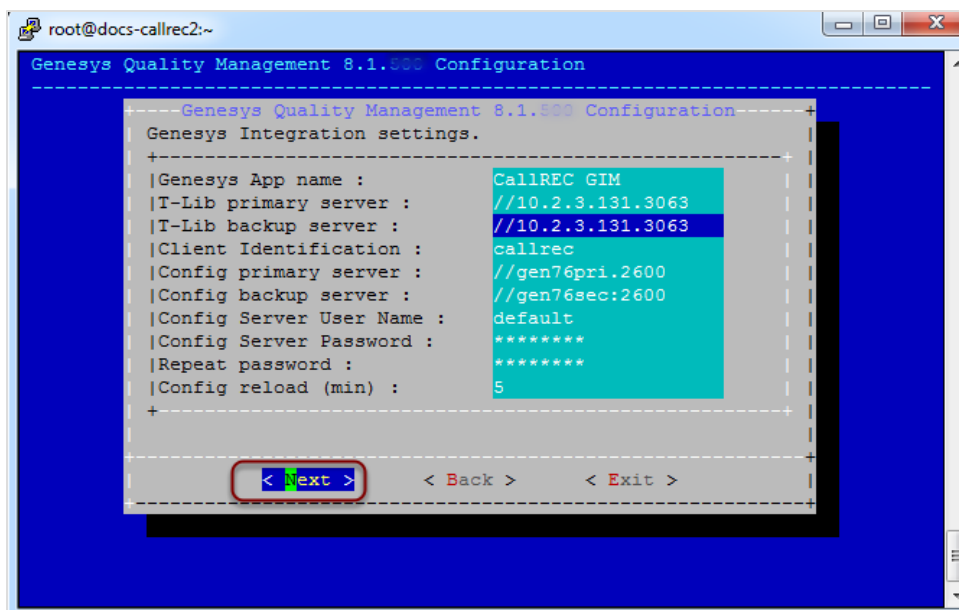


Figure 12: Configuring Genesys GIM

1. Type:

- Your Genesys **App Name**, configured in the Genesys Configuration Manager.
- Your Genesys **T-Lib primary server** and **T-Lib backup server** IP addresses (or fully qualified domain names - FQDN). Use a comma-separated list for more than one.
- An (optional) **User Name** and **Password** for a user account on the T-Lib servers.
- The **Config primary server** and **Config secondary server** IP addresses and port numbers (or FQDN) of your Genesys Configuration Servers. Again, use a comma-separated list for more than one.
- The (required) **User Name** and **Password** of the Call Recording user set up in your Genesys Configuration Server.
Set the **Configuration Reload interval** in minutes. This specifies how often the GIM will re-connect to the Configuration Manager to get the latest configuration data.

Tip:

After entering the **User Name** and **Password**, press the down arrow key to scroll down to the **Repeat Password** and **Config Reload** fields!

2. Select **Next**.

Important:

If no IP port is specified, the default ports are 3063 for T-Lib servers and 2020 for Configuration servers. For compatibility with earlier GIM releases, IP addresses can be prefixed with two slashes “//” and suffixed with the IP port. The backup servers are optional, although strongly recommended for a production installation.

Entering the Settings for Genesys EPR

If you did not select the Genesys EPR service earlier, this will not appear during installation.

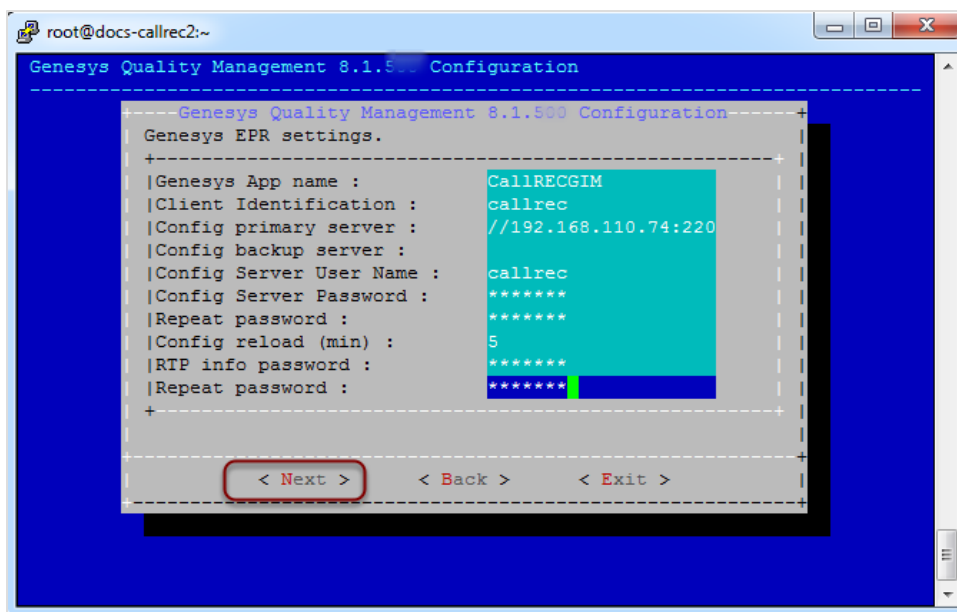


Figure 13: Configuring Genesys EPR

1. Type:

- Your Genesys **App Name**, configured in the Genesys Configuration Manager.
- An (optional) **User Name** and **Password** for a user account on the T-Lib servers.
- The **Config primary server** and **Config secondary server** IP addresses (or FQDN) of your Genesys Configuration Servers. Again, use a comma-separated list for more than one.
- The (required) **User Name** and **Password** of the Call Recording user set up in your Genesys Configuration Server.
- The **Config Reload interval** in minutes. This specifies how often the GIM will re-connect to the Configuration Manager to get the latest configuration data.
- Enter the **RTP info password** and **RTP info password** (pre-defined in the Genesys Configuration Manager. See the Genesys EPR Integration section in the Call Recording Administration Guide)

2. Select **Next**.

Important:

If no IP port is specified, the default ports are 3063 for T-Lib servers and 2020 for Configuration servers. For compatibility with earlier EPR releases, IP addresses can be prefixed with two slashes “//” and suffixed with the IP port. The backup servers are optional, although strongly recommended for a production installation.

Entering the Genesys MSR Settings

If you did not select the Genesys MSR service earlier, this will not appear during installation.

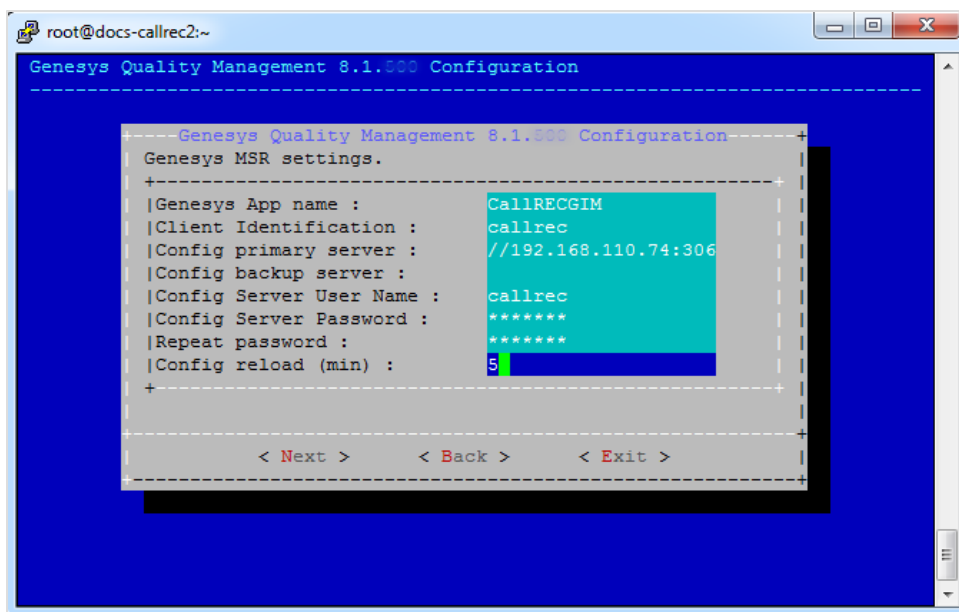


Figure 14: Configuring Genesys MSR

1. Type:

- Your Genesys **App Name**, configured in the Genesys Configuration Manager.
- An (optional) **User Name** and **Password** for a user account on the T-Lib servers.
- The **Config primary server** and **Config secondary server** IP addresses (or FQDN) of your Genesys Configuration Servers. Again, use a comma-separated list for more than one.
- The (required) **User Name** and **Password** of the Call Recording user set up in your Genesys Configuration Server.
- The **Config Reload interval** in minutes. This specifies how often the GIM will re-connect to the Configuration Manager to get the latest configuration data.

2. Select Next.

Important:

If no IP port is specified, the default ports are 3063 for T-Lib servers and 2020 for configuration servers. For compatibility with earlier EPR releases, IP addresses can be prefixed with two slashes “//” and suffixed with the IP port. The backup servers are optional, although strongly recommended for a production installation.

Entering the Avaya Settings

If the Avaya service was not selected earlier, it does not appear during installation.

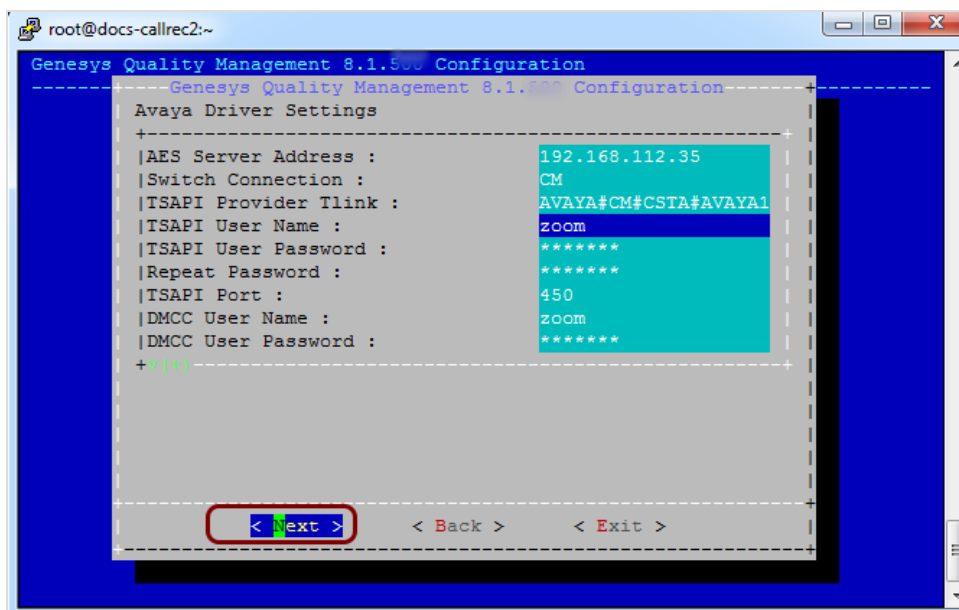


Figure 15: Avaya Setup

1. Type the **AES Server Address**: This is the IP address of the AES Server.
 Type the **Switch Connection**: This is an alias for the switch.
 Type the **TSAPI Provider Tlink**: This can be any non empty string separated by '#', for example, AVAYA#CM#CSTA#AVAYA1AES.
 Type the **TSAPI User Name**: This can be any non empty string.
 Type **TSAPI User Password**: This can be any non empty string.
 Type the **Repeat Password**: The same non empty string as the TSAPI User Password.
 Type the **TSAPI Port**: This is a number between 1 and 65535. The default value is 450.
DMCC User Name: Login needed to obtain the Avaya virtual recording service. This can be any non empty string.
DMCC User Password: Password needed to obtain the Avaya virtual recording service.
Repeat Password: Password needed to obtain the Avaya virtual recording service.
DMCC Port: This is a number between 1 and 65535. The default value is 4721.
Recording Device Range: Range of terminal extensions used as Avaya

virtual recording devices (must be configured on the Avaya server). This can be any number.

IP Station Security Code: This is needed to obtain the Avaya virtual recording service. This field must not be empty.

2. Click **Next**.

Packet Sniffing

User Datagram Protocol (UDP) uses a simple transmission model without implicit hand-shaking dialogues for guaranteeing reliability, ordering, or data integrity. Time-sensitive applications often use UDP because dropping packets is preferable to using delayed packets.

Important:

It's highly recommended that you select **Every UDP**.

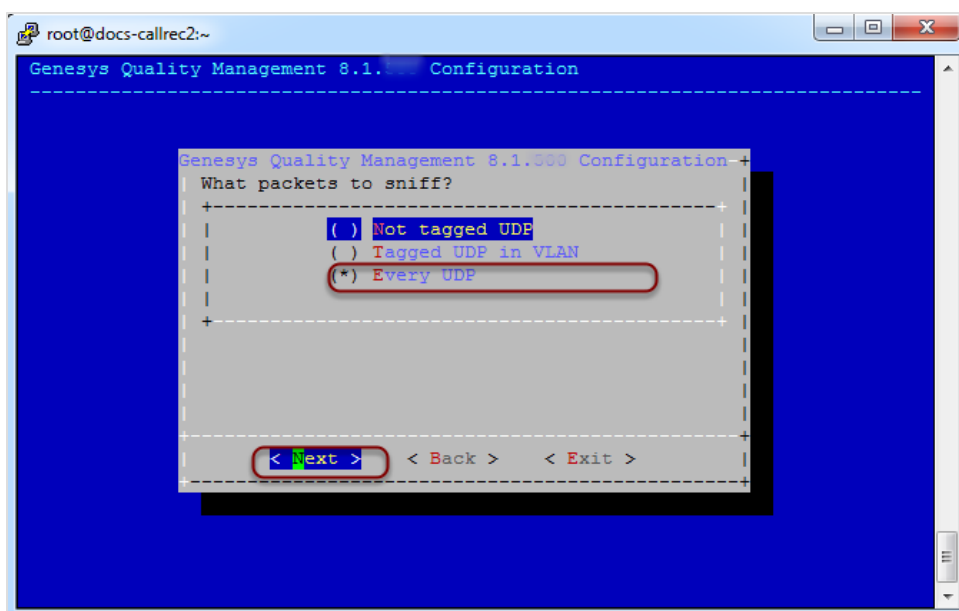


Figure 16: Packet Sniffing Configuration

1. Select your choice from the list.
2. Select **Next**.

PostgreSQL - Database Locale Settings

If you have selected the PostgreSQL database in GQM services, you will now be presented with this screen. For Oracle-based installations, skip the following two steps.

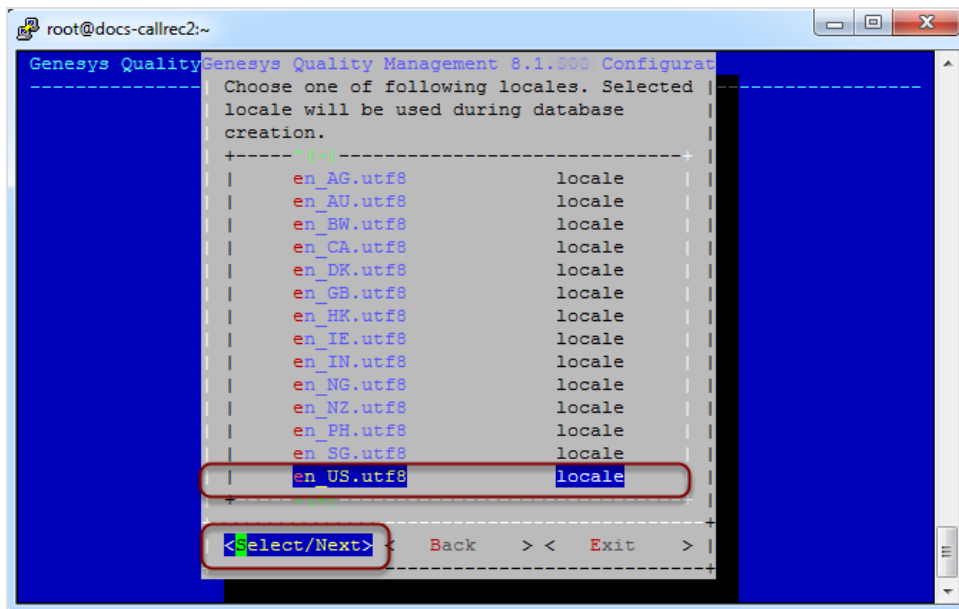


Figure 17: PostgreSQL Database Locale Selection

1. Select the appropriate database language locale settings for your installation.
2. Click **Select/Next**.

This will ensure that locale-specific features, such as alphabetic order, will work correctly in GQM. The default is `en_US.utf8` (UTF-8 US English locale).

Important:

The PostgreSQL database locale can only be specified when the database is being created (normally during the first setup after installation).

Changing the locale in an existing database entails creating a new database with the required locale and migrating (dumping and restoring)

the data from old to new databases. Please contact Genesys Support (<http://genesyslab.com/support/contact>) for more information.

PostgreSQL - Remote Database Connections

Depending on your installation, you must provide GQM with access to remote PostgreSQL database connections. If you are setting up a single standalone server, you do not need to configure remote database connections at this point.

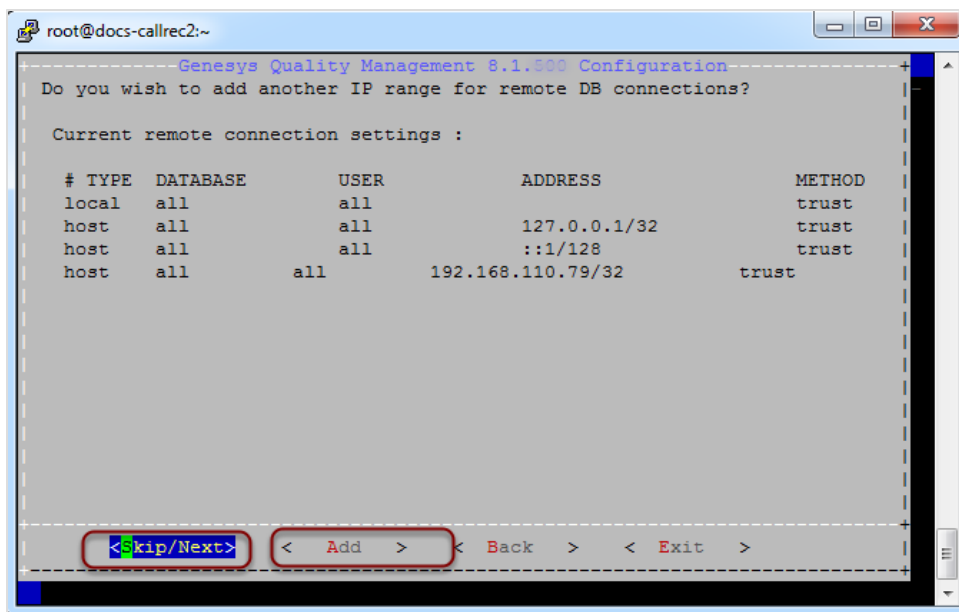


Figure 18: Remote Database Connections

1. If you have no remote databases connections, select **Skip/Next**.
2. To enter remote database connections, select **Add**.

The Remote Connection Settings screen appears.

Important:

If you are unsure about what settings are required, refer to the *PostgreSQL Administrator's Guide*, chapter "Client Authentication" for more details.

This screen controls which hosts are allowed to connect, how clients are authenticated, which PostgreSQL user names they can use, and which databases they can access.

Type can be one of the following values: `local` (a Unix-domain socket), `host` (either a plain or SSL-encrypted TCP/IP socket), `hostssl` (an SSL-encrypted TCP/IP socket), or `hostnossl` (a plain TCP/IP socket).

Database can be `all`, `sameuser`, `samerole`, a database name, or a comma-separated list.

User can be `all`, a user name, a group name prefixed with `+`, or a comma-separated list.

In both the **Database** and **User** fields you can also write a filename prefixed with `@` to include names from a separate file.

CIDR-Address specifies the set of hosts the record matches. It is made up of an IP address and a CIDR mask that is an integer (between 0 and 32 (IPv4) or 0 and 128 (IPv6) inclusive) that specifies the number of significant bits in the mask.

Method can be `trust`, `reject`, `md5`, `crypt`, `password`, `krb5`, `ident`, or `pam`. Note that `password` sends passwords in clear text. The setting `md5` is preferred since it sends encrypted passwords.

Database and user names containing spaces, commas, quotes and other special characters must be quoted. Quoting one of the keywords `all`, `sameuser` or `samerole` makes the name lose its special character, and just match a database or username with that name.

Important:

Configuring the system for `local trust` authentication allows any local user to connect as any PostgreSQL user, including the database super user. If you do not trust all your local users, use another authentication method.

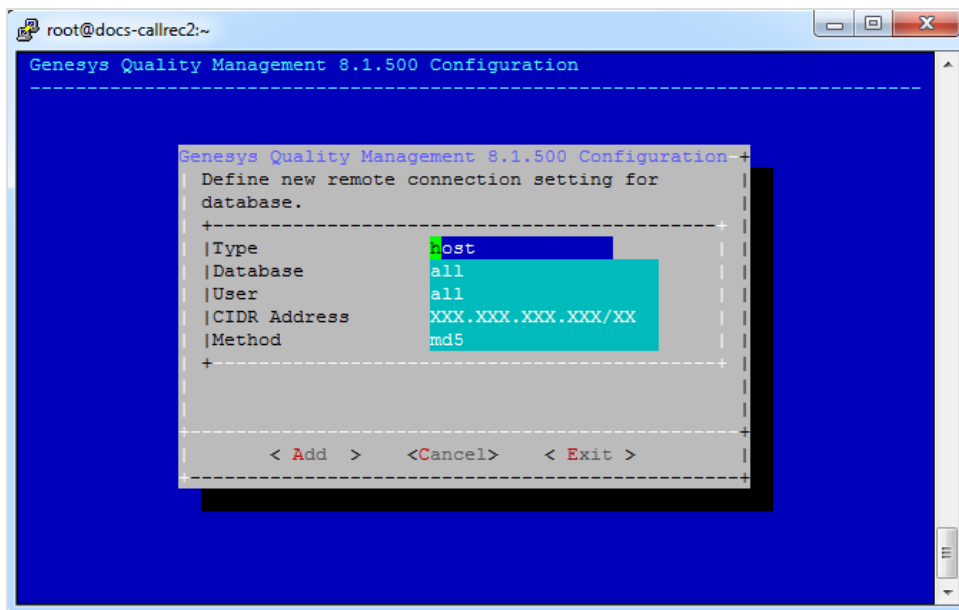


Figure 19: Identifying Remote Databases

1. Enter the connection **Type**.
2. Enter the **Database** access setting.
3. Enter the **User** setting.
4. Enter the IP address / CIDR mask for the **CIDR Address**.
5. Type the **Method** of accessing the database.
6. Select **Add**.

The Database now appears in the Current Remote Connections list.

Important:

In order to enter the CIDR Address you will need to delete the existing X characters first, using the Delete key.

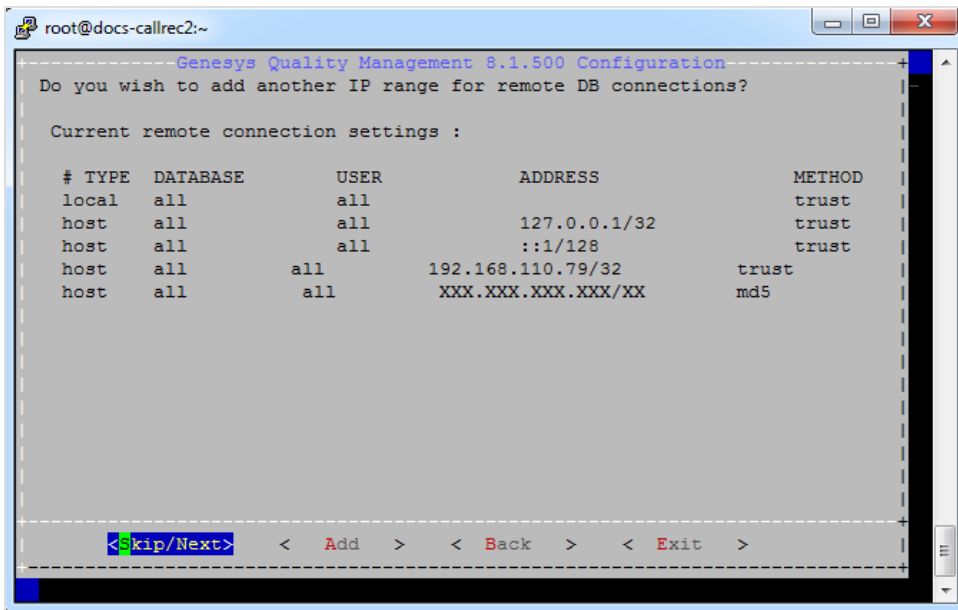


Figure 20: Updated Remote Connections List

- To add another database, select **Add**.
- When you are finished, select **Skip/Next**.

SMTP Server

GQM requires access to an SMTP server to provide status notifications via email.

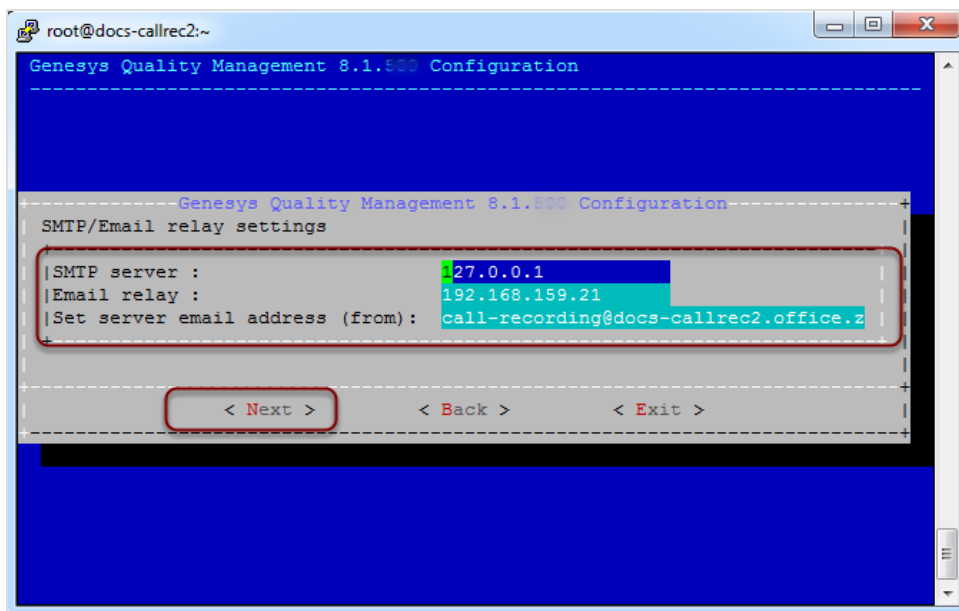


Figure 21: SMTP Server Configuration

1. Type:
 - Your **SMTP Server** IP address.
 - Type your **Email Relay** IP address (if any).
 - Specify the server 'from' email address.
2. Select **Next**.

Increase Tomcat Server Memory

Certain services (particularly Quality Manager) require the Tomcat web server to have more system memory allocated to its java virtual machine (JVM) than is provided as standard. This screen allows the installer to configure Tomcat according to your requirements.

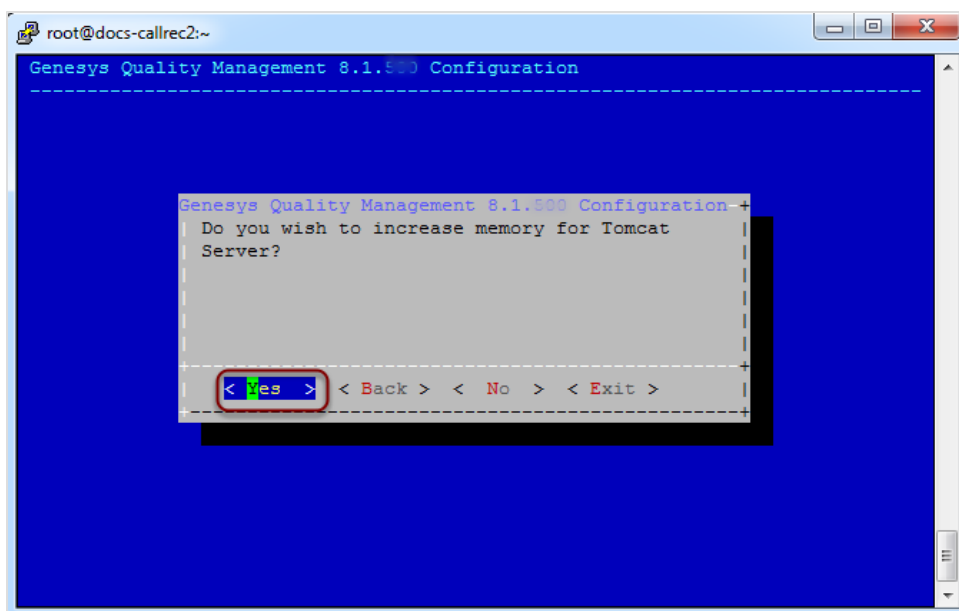


Figure 22: Increase Tomcat Server Memory

- If Quality Manager is enabled in this GQM installation, it is strongly recommended to answer **Yes** at this prompt, to avoid potential operational issues.

Call Recording Automatic Startup

It is recommended that Call Recording starts automatically after the server is booted up. If you choose **No** at this prompt, Call Recording must be started manually.

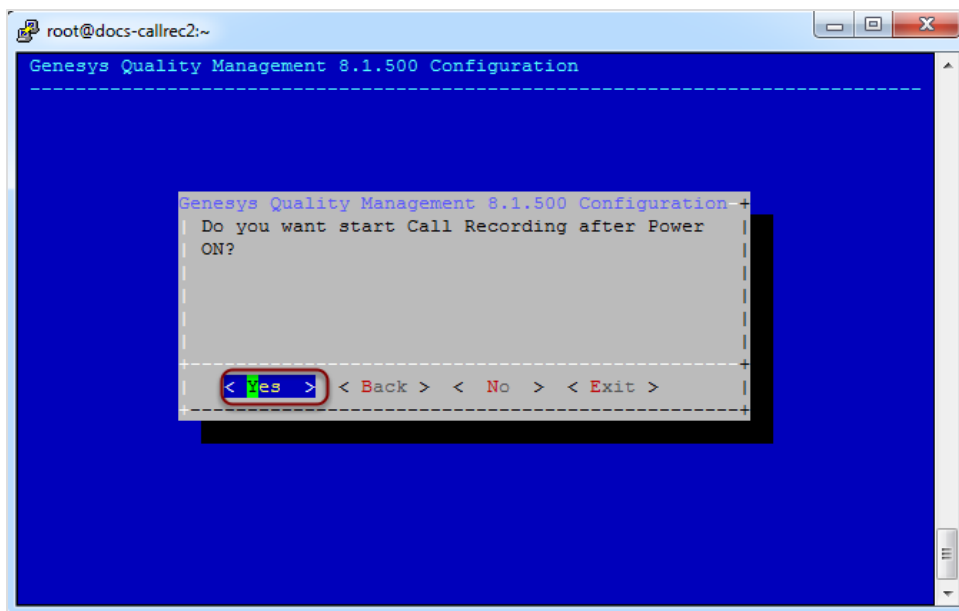


Figure 23: Starting Call Recording Automatically After Power On

- Select **Yes** to start Call Recording automatically.

Generate Self-signed Certificate and Keys

If the Key Manager service was enabled during the service selection step, you are prompted at this point to decide whether you wish to create a self-signed certificate and keys for Key Manager.

Using a self-signed certificate (as opposed to a commercial encryption certificate offered by companies such as Thawte and Verisign) enables you to encrypt client-server communications and audio/video calls immediately after setup, but can lead to issues with browsers and servers rejecting the certificates due to their lower security nature. It is most suited to testing purposes.

Please see the GQM Security Guide for more information about certificates, keys and PCI-DSS compliancy.

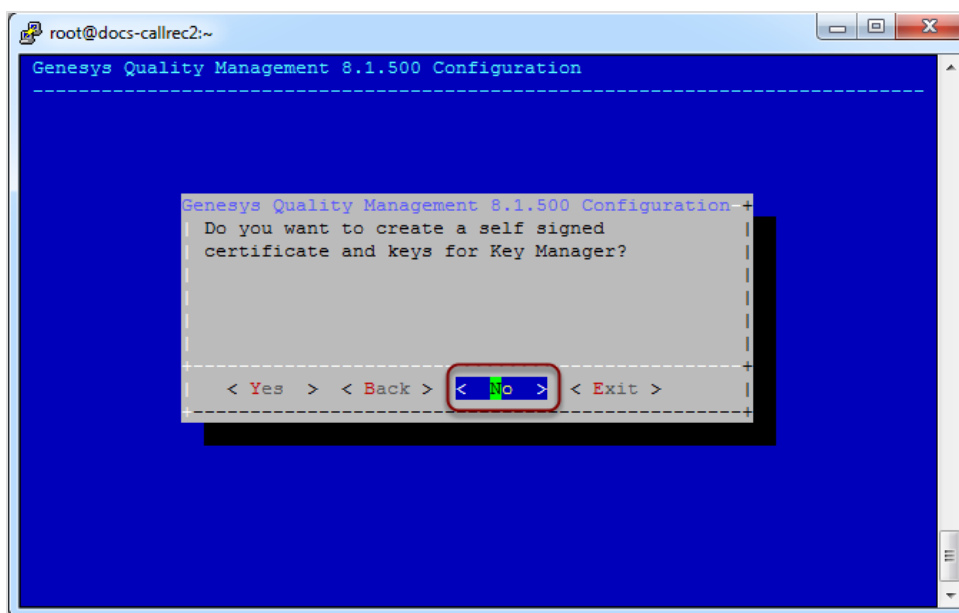


Figure 24: Create a self-signed certificate and keys for Key Manager

- Select **Yes** to create self-signed certificates (for testing purposes) or **No** to create no certificates for call encryption.

Restarting Call Recording

Setup can automatically start Call Recording (or restart it if already running) after the installation has completed.

If you choose No at this prompt, Call Recording must be (re)started manually. Sometimes this can be helpful, if you still need to perform some manual updates to the Call Recording configuration files before Call Recording can safely be started. The manual command to start Call Recording is shown later in this guide.

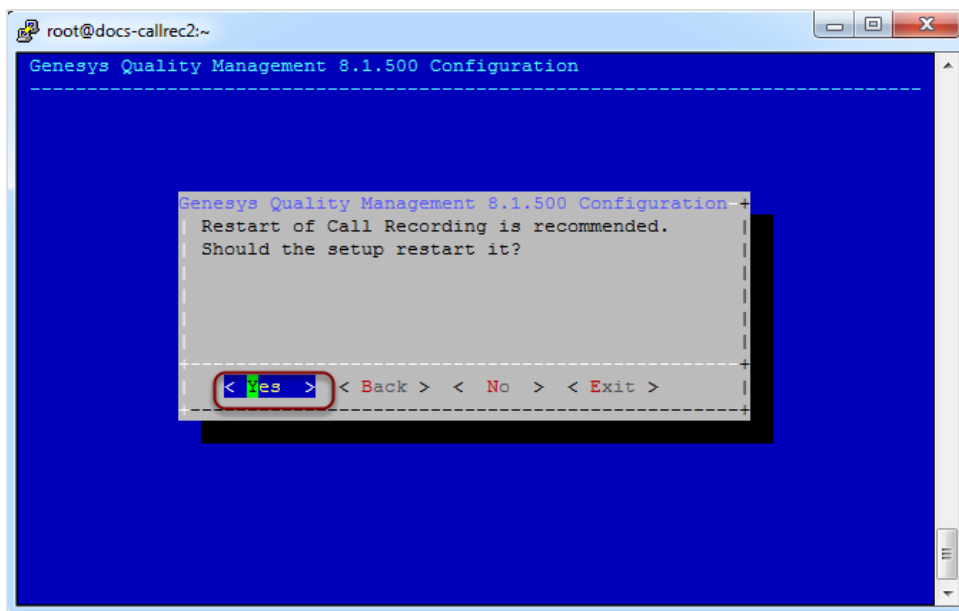
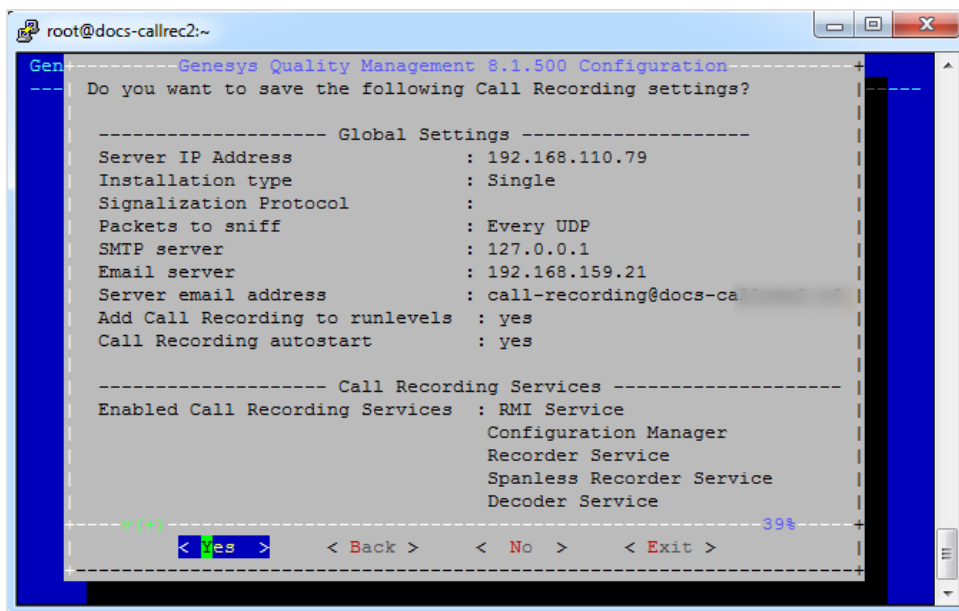


Figure 25: Enabling the Automatic Restart of Call Recording After Installation

Select **Yes** to restart Call Recording automatically after installation is complete.

Verifying the Configuration

Before GQM setup completes the configuration and setup, it displays the information you have entered so far. This allows you to verify the settings and change them if needed.



```
root@docs-callrec2:~  
Gen----- Genesys Quality Management 8.1.500 Configuration  
-----  
Do you want to save the following Call Recording settings?  
  
----- Global Settings -----  
Server IP Address      : 192.168.110.79  
Installation type     : Single  
Signalization Protocol :  
Packets to sniff      : Every UDP  
SMTP server           : 127.0.0.1  
Email server          : 192.168.159.21  
Server email address  : call-recording@docs-ca  
Add Call Recording to runlevels : yes  
Call Recording autostart : yes  
  
----- Call Recording Services -----  
Enabled Call Recording Services : RMI Service  
                                Configuration Manager  
                                Recorder Service  
                                Spanless Recorder Service  
                                Decoder Service  
  
v(+)  
-----  
< Yes > < Back > < No > < Exit >
```

Figure 26: Configuration Verification and Save

- Scroll to the bottom of the Configuration Verification screen using the up and down arrow keys.
- Verify your configuration and setup settings.
- Click **Yes** to complete configuration.
- Click **Back** to change configuration and setup settings.
- Click **Exit** to abort configuration and setup.

Completing Configuration

GQM setup requires up to several minutes to run the configuration and setup. A progress bar displays the current setup progress.

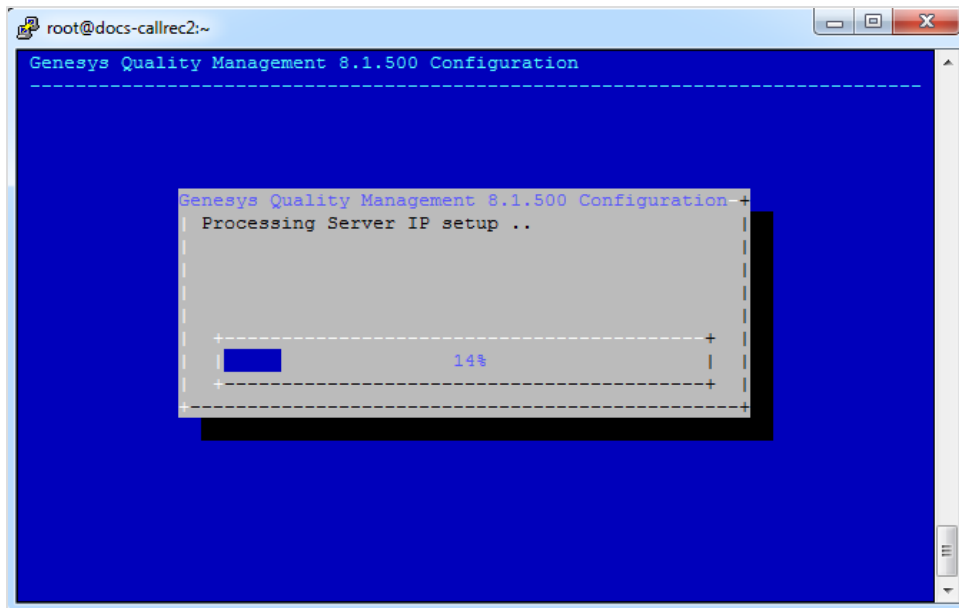


Figure 27: Configuration Status Display

If there is an error during configuration, GQM setup displays a warning and continues. For troubleshooting, refer to the *Planning Guide* and the *Call Recording Administration Guide*, or contact Genesys Support <http://genesyslab.com/support/contact>.

When setup and configuration is complete, GQM setup displays a notification message.

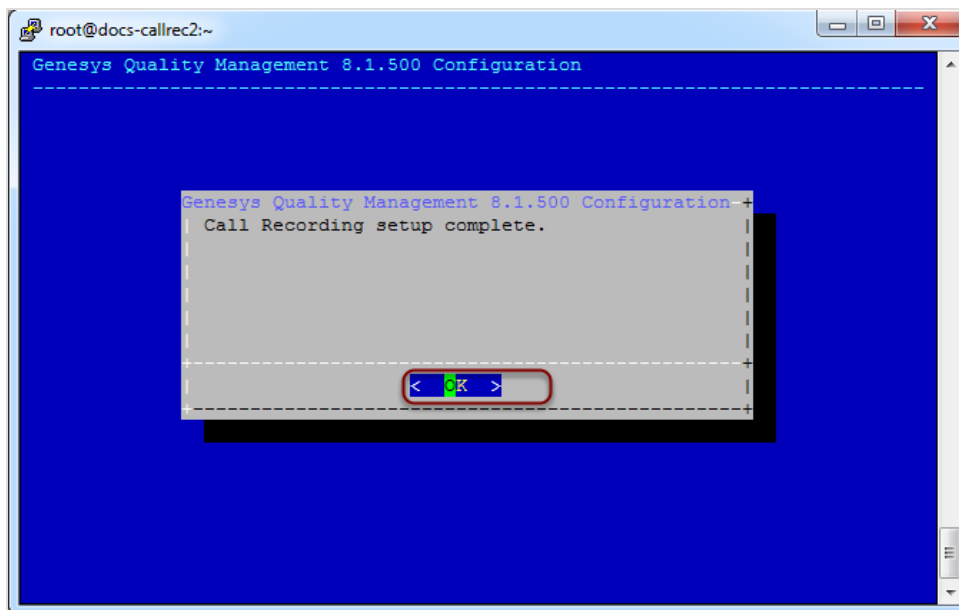


Figure 28: Configuration Complete

Select **OK**.

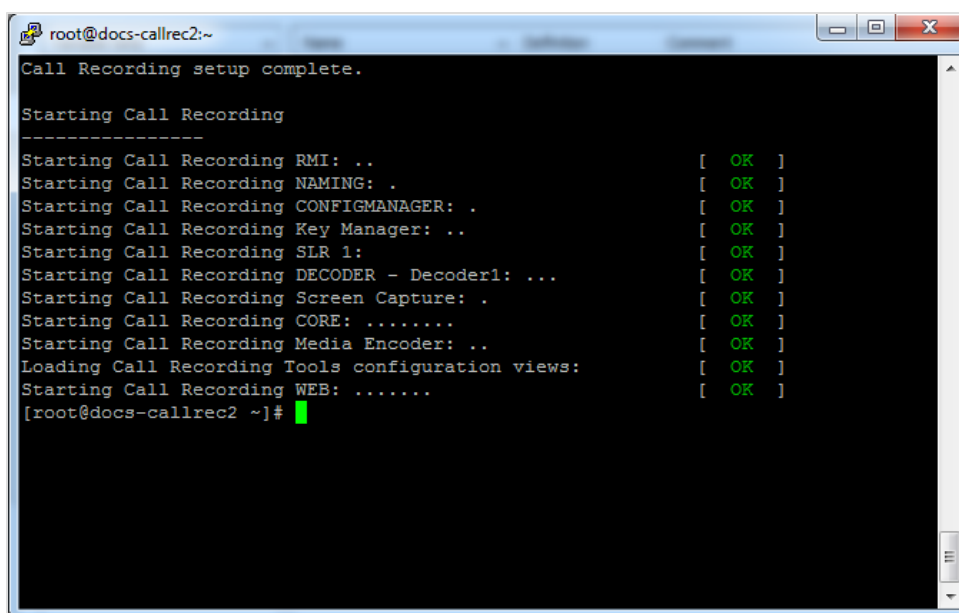
The **QM Suite** setup utility returns you to the command line prompt, and (re)starts Call Recording if configured to do so.

Starting Call Recording Services

If you did not select automatic (re)starting of Call Recording after configuration, type `service callrec start` at the command prompt. See the *Call Recording Administration Guide* for more details on Call Recording commands.

Call Recording now starts each service and displays a status message for each service. This can take several minutes.

The screenshot below is just illustrative (you may have different services enabled), but note the following:



```
root@docs-callrec2:~  
Call Recording setup complete.  
  
Starting Call Recording  
-----  
Starting Call Recording RMI: .. [ OK ]  
Starting Call Recording NAMING: . [ OK ]  
Starting Call Recording CONFIGMANAGER: . [ OK ]  
Starting Call Recording Key Manager: .. [ OK ]  
Starting Call Recording SLR 1: [ OK ]  
Starting Call Recording DECODER - Decoder1: ... [ OK ]  
Starting Call Recording Screen Capture: . [ OK ]  
Starting Call Recording CORE: ..... [ OK ]  
Starting Call Recording Media Encoder: .. [ OK ]  
Loading Call Recording Tools configuration views: [ OK ]  
Starting Call Recording WEB: ..... [ OK ]  
[root@docs-callrec2 ~]#
```

Figure 29: Starting Call Recording Services

- Some services may fail when first attempting to start. This may be because they require further independent configuration (for example, Synchro). Refer to the *Call Recording Administration Guide* for more information
- If you have enabled Key Manager and selected to generate self-signed certificates, the final stage of encryption certificate generation is performed after Call Recording has been fully started.

Important:

If the Call Recording restart is not successful (particularly if the 'Call Recording WEB' component fails to start), this can indicate that the server does not have enough memory available, which can be an issue particularly with virtual servers. Check the logs; for example the web server log (`less /opt/callrec/logs/web.log`) and check for the following lines, which indicate that the Java VM needs more RAM:

```
Error occurred during initialization of VM
Could not reserve enough space for object heap
```

Important Note on Synchronization

If the Call Recording installation is part of a multiple site cluster configuration, all the servers in the cluster should be time-synchronized, for example via [NTP](#), with the same server as the time source.

If the servers are not properly synchronized, some of the recordings may have issues with stream synchronization.

Setting a Custom Locale for the Web Server

The GQM web server (Apache Tomcat) uses the same locale as the server by default, for language- and culture-related environment settings, for example.

To set a custom locale for the web server (affecting both Quality Manager and Call Recording web interfaces), `user.language` and `user.country` properties need to be added to the `JAVA_OPTS_WEB` JVM parameter, included at the end of the `callrec.conf` configuration file. In a standard Call Recording installation, this file is located at `/opt/callrec/etc/callrec.conf`.

The following configuration sample shows the `JAVA_OPTS_WEB` JVM parameter containing `user.language` and `user.country` properties (prefixed with the `-D` flag) for an `en_GB` UK locale. Many servers are configured with a default `en_US` locale during setup.

```
JAVA_OPTS_WEB="-jvm server -XX:NewSize=256m -XX:SurvivorRatio=16 -
XX:MaxNewSize=256m -XX:MaxPermSize=256m
-XX:PermSize=256m -Xms512m -Xmx512m -XX:+DisableExplicitGC -
Duser.language=en -Duser.country=GB"
```

The range of values for these parameters can be found at the following URLs:

- `user.language`: ISO 639-1 / ISO-639-2 code list (http://www.loc.gov/standards/iso639-2/php/code_list.php).
- `user.country`: ISO 3166 code list (http://userpage.chemie.fu-berlin.de/diverse/doc/ISO_3166.html).

Chapter

4

Licensing and Activating GQM

This section briefly describes how to launch and activate GQM

This chapter contains the following sections:

[Launching the Call Recording Web GUI](#)

[Activating Call Recording](#)

[Activating Quality Manager](#)

[Configuring Quality Manager in the Call Recording GUI](#)

Launching the Call Recording Web GUI

The Call Recording login screen appears.

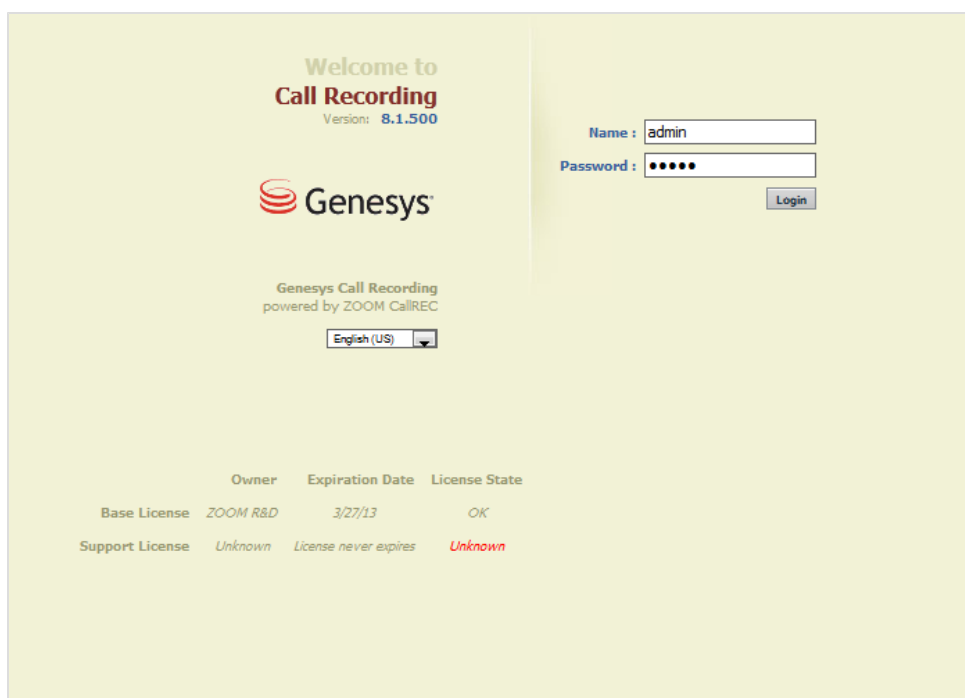


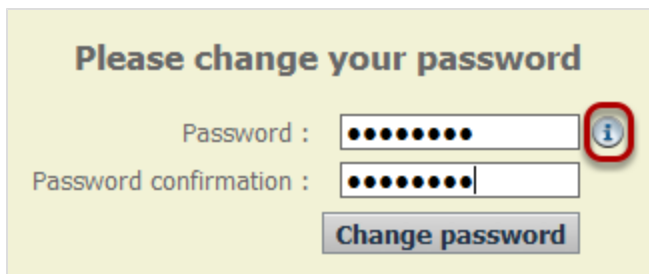
Figure 30: Call Recording Login Screen

Log in as `admin` and enter the password. If this is the first login after installation, enter the default password: `admin` and a dialog appears with a prompt to change the password.

The first time you log in to the Call Recording Web GUI with the default username and password you will be required to change the password (enter a new password twice) before continuing.

Important:

The default password `admin` can never be entered again as the password.



Please change your password

Password : ⓘ

Password confirmation :

Figure 31: Change Default Password

Click the information icon to view the password requirements

You are now ready to begin to configure Genesys Call Recording – see the *Call Recording Administration Guide* for more details.

Depending on the components that you have purchased, you may also wish to consult the following:

- *The Quality Manager Administration Guide*
- *The Screen Capture Administration Guide*
- *The Security Guide*

Activating Call Recording

This section gives a step-by-step guide to activate Call Recording.

Activating Call Recording is the first task to complete after installation of the system.

Important:

It is very important to activate the license file immediately. There is a 30 day grace period from the date of issue. At 00:00 hours on the 30th day, an un-activated license stops working.

To access the installation licensing information once Call Recording is installed and started:

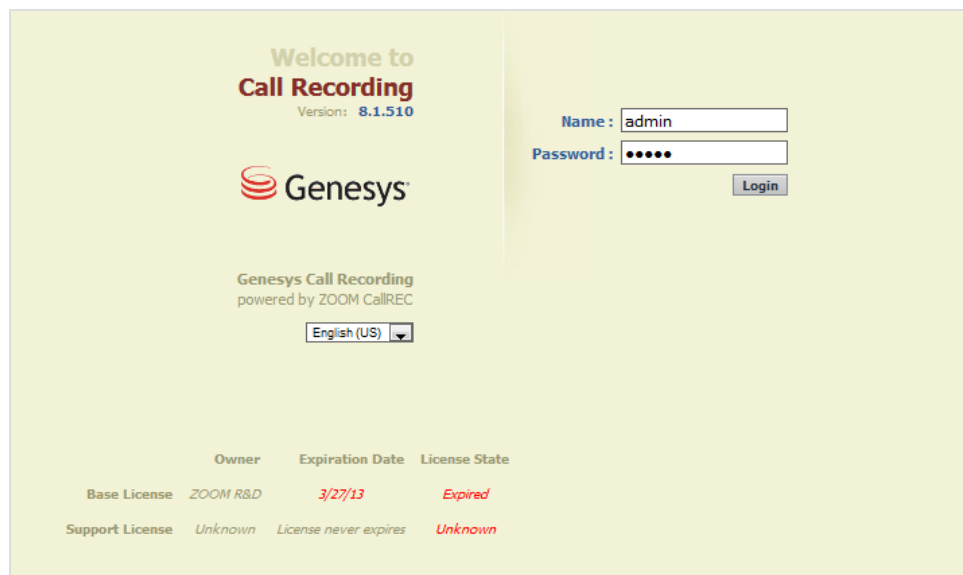


Figure 32: Log in for Activation

1. Open the Call Recording web interface.
2. Log in as `admin` and enter the password. If this is the first login after installation, enter the default password: `admin` and a dialog appears with a prompt to change the password.

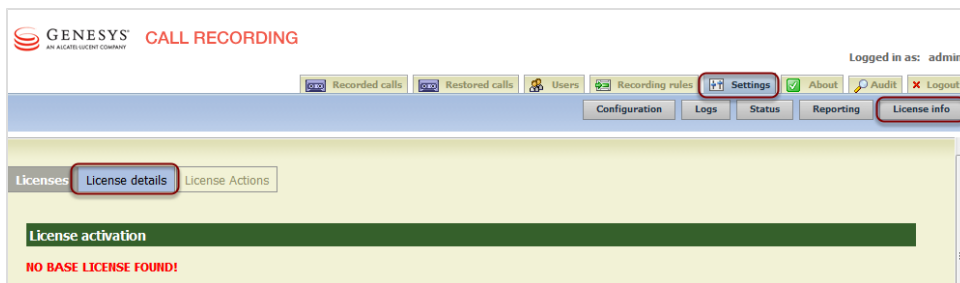


Figure 33: License Details

1. Open the **Settings** tab.
2. Click **License info**.
3. Click **License details**. The **License activation** form displays.

License activation

NO BASE LICENSE FOUND!

License details : Base License

License Information		License Properties		License Features	
Product Name	Unknown	Registered terminals - warning	0	Recorder	✖
Major Version	0	Registered terminals	0	Decoder	✖
Minor Version	0	Concurrent calls - warning	0	SIP	✖
Owner	Unknown	Concurrent calls	0	SKINNY	✖
Commercial	false	Recorded calls - warning	0	JTAPI	✖
Number	Unknown	Recorded calls	0	LDAP	✖
Product Edition	Unknown	Servers in cluster	0	Advanced search	✖
Issue Date	-	Concurrent screens	0	API	✖
Expiration Date	-	Concurrent screens - warning	0	LiveMON	✖
License State	Unknown			Pre-recording	✖
				Instreamer	✖
				ScreenREC	✖
				Cisco UCCX IM	✖
				Cisco UCCE IM	✖
				Genesys IM	✖

License details : Support License

License Information		License Properties		License Features	
Product Name	Unknown	Max couples in database	0		
Major Version	0	Max users	0		
Minor Version	0	Max user groups	0		
Owner	Unknown	Max record capacity	0		
Commercial	false				
Number	Unknown				
Product Edition	Unknown				
Issue Date	-				
Expiration Date	-				
License State	Unknown				

Figure 34: No Base License Found

Uploading the Un-Activated Call Recording License File

Genesys Support has sent an email containing an un-activated license file named `callrec.license`. Save the un-activated license file in a location that is easy to find. Do not rename this file.

Call Recording does not record without a valid license file.

Upload the un-activated license file. This generates the unique license key, based on information including the MAC addresses of the NICs in the server. If the MAC addresses change, then the installation requires a new license file. Contact Support at the email address listed at <http://genesyslab.com/support/contact>.

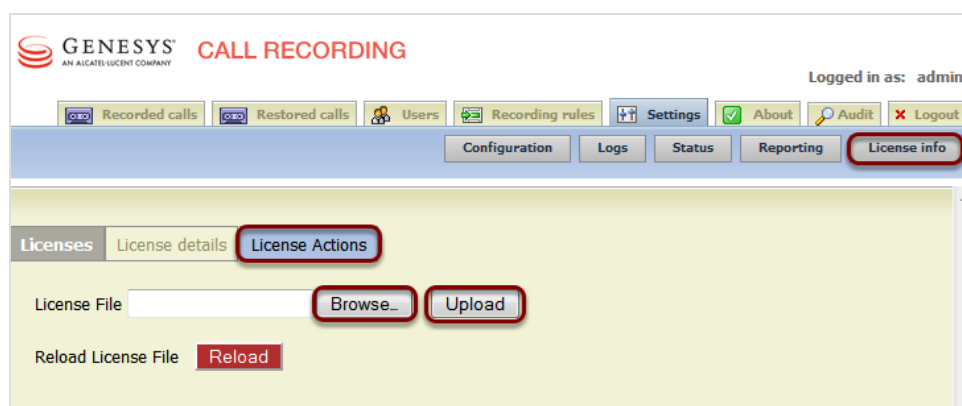


Figure 35: License actions dialog

To upload the License File:

1. Open the **Settings** tab and click **License info**.
2. Click **License Actions**. The license action dialog displays.
3. Click **Browse** for *Firefox* or *Internet Explorer* or **Choose File** in *Chrome* and browse to the un-activated license file in the location it was saved.
4. Click **Upload**.

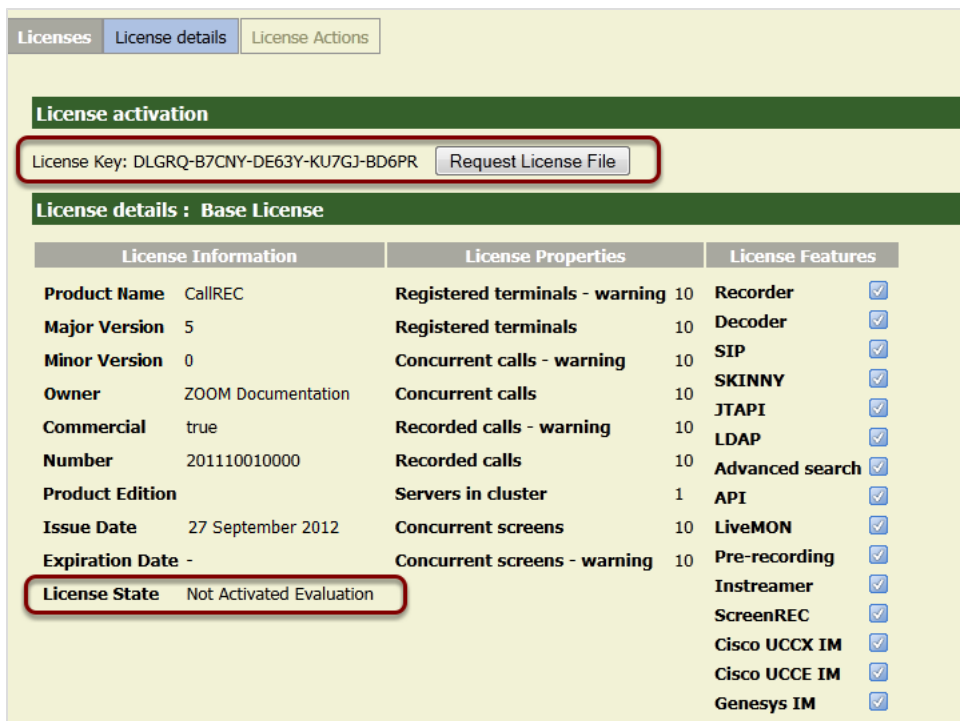


Figure 36: Un-Activated License

Once the license is successfully uploaded:

1. The license key is visible on the **License details: Base License** tab.
2. Note the **License State** is **Not Activated Evaluation**.

If the system prompts to reload the license file, follow the same procedure as above, and click **Reload**.

Activating an Un-Activated Version of Genesys Call Recording

To fully activate the system, upload a permanent activated license. There are two ways to get a permanent activated license file:

With SMTP Access: If the server that Call Recording is installed on has SMTP server access, on the **License details** page, click **Request License File**. This sends an email request to Genesys Labs, Inc. containing the license key.

Without SMTP Access: If the server that Call Recording is installed on has no SMTP server access or is installed behind a firewall, then send an email to Genesys Support at the email address listed at <http://genesyslab.com/support/contact> with the complete license key. The key is required to generate the license file.

Genesys Support sends a permanent activated license file that corresponds to the system and purchase details. Save the activated license file in a location that is easy to find. Do not rename this file. The license file contains the parameters of the license, ensuring that all permitted features are properly activated.

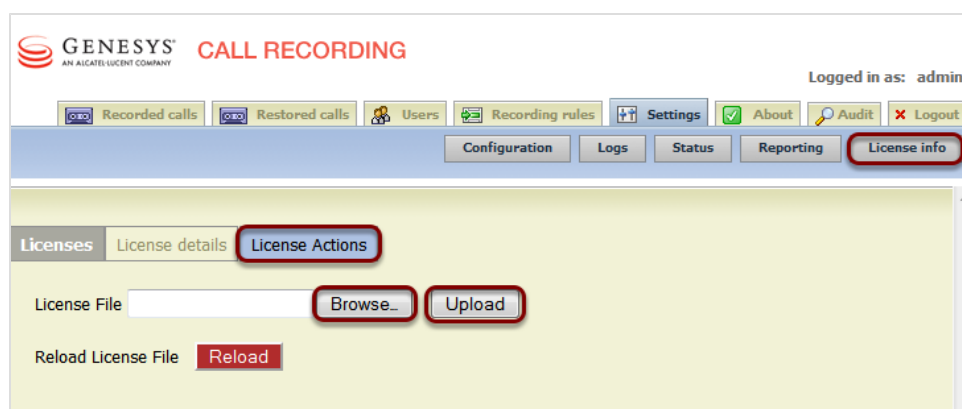


Figure 37: License Actions Dialog

The procedure for uploading the activated license is the same as for the un-activated license:

1. Open the **Settings** tab, and click **License info**.
2. Click **License Actions**. The license action dialog appears.
3. Click **Browse**, and navigate to the activated license file.
4. Click **Upload**.

If the system prompts to reload the license file, follow the same procedure as above, and click **Reload**.

Once the permanent license has been successfully uploaded, the license keys are visible on the **License details** tab.

Repeat the process for the support license if purchased. The license file is named `callrec-support.license`.

License activation

License already activated or license activation not required.

License details : Base License

License Information		License Properties		License Features	
Product Name	CallREC	Registered terminals - warning	100	Recorder	<input checked="" type="checkbox"/>
Major Version	5	Registered terminals	100	Decoder	<input checked="" type="checkbox"/>
Minor Version	1	Concurrent calls - warning	100	SIP	<input checked="" type="checkbox"/>
Owner	ZOOM Documentation	Concurrent calls	100	SKINNY	<input checked="" type="checkbox"/>
Commercial	false	Recorded calls - warning	100	JTAPI	<input checked="" type="checkbox"/>
Number	20120927001	Recorded calls	100	LDAP	<input checked="" type="checkbox"/>
Product Edition		Servers in cluster	10	Advanced search	<input checked="" type="checkbox"/>
Issue Date	September 27, 2012	Concurrent screens	100	API	<input checked="" type="checkbox"/>
Expiration Date	December 31, 2013	Concurrent screens - warning	100	LiveMON	<input checked="" type="checkbox"/>
License State	OK			Pre-recording	<input checked="" type="checkbox"/>
				Instreamer	<input checked="" type="checkbox"/>
				ScreenREC	<input checked="" type="checkbox"/>
				Cisco UCCX IM	<input checked="" type="checkbox"/>
				Cisco UCCE IM	<input checked="" type="checkbox"/>
				Genesys IM	<input checked="" type="checkbox"/>

Figure 38: Activated Licence

Restarting Call Recording

Access the Call Recording server via an SSH client, for example PuTTY.

Log in as `admin`. Enter `su -` to log in as the root user. Enter the password, the default is `zoomcallrec`.

Enter the following command:

```
service callrec restart
```

Call Recording restarts. This takes several minutes.

Activating Quality Manager

Important:

Only perform this step to use Quality Manager. If no Quality Manager license has been purchased, skip this step.

Before configuring Quality Manager, upload and install a valid license. The web URL to the Call Recording installation is required. Genesys Support sends an un-activated license file. Save this un-activated license file in a location where it can be accessed easily. Do not rename this file.

Open Quality Manager in a Web Browser

Open a web browser and enter the following URL:

```
http://<CallREC server>/scorecard-webui
```

Quality Manager opens in the browser window. It usually takes a few seconds for the application to load before the login window appears.

Log In as Administrator

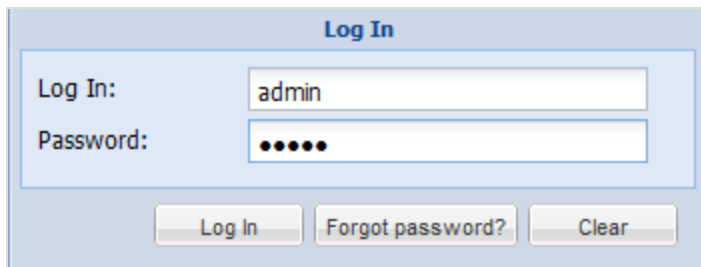


Figure 39: Log in as Administrator

Log in as `admin` and enter the password. The default is `admin`. The `admin` account is the only login that works without a valid license.

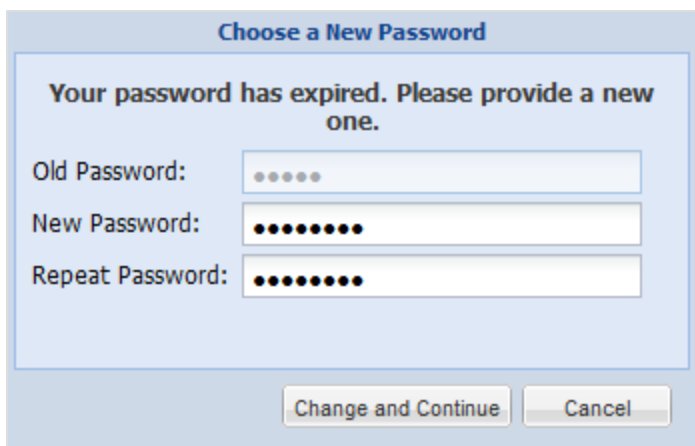


Figure 40: Choosing a New Password

When logging in for the first time, a password change is required. The default password `admin` can never be used again.

Important:

After two incorrect passwords, Quality Manager displays: "Warning: The next incorrect entry will lead to the account being locked." After the third attempt with the wrong password Quality Manager blocks the account for a configurable period and displays: "Please contact your administrator to unblock your account".

Uploading the Un-activated Quality Manager License File

Click **About** in the left hand menu. The tab below opens.

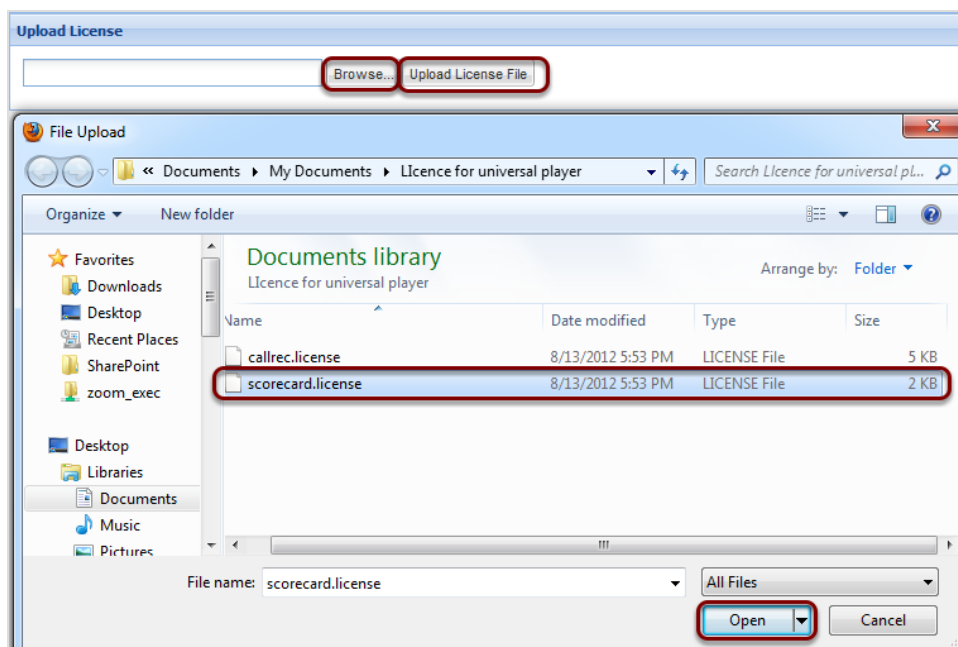


Figure 41: Browse to the License File

1. Click **Browse**, and navigate to the folder containing the licence file named `scorecard.license`.
2. Select the license file.
3. Click **Open**.
4. Click **Upload License File**.

The license file generates a unique **Activation key** based on information including the MAC addresses of the NICs in the server. If the MAC addresses need to be changed, a new license file is required. Please contact the email address listed at <http://genesyslab.com/support/contact> for assistance.

If the import browser is Chrome, the file path may display incorrectly. For example, `C:\fakepath\scorecard.license`. This is an issue with Chrome and does not affect the upload.

The Activation Key

About	
Product Info	
Version:	8.1.510
Build:	130301_2222
Product License	
Product Name	Quality Manager
Product Version	8.1.510
Owner	ZOOM Documentation
Issue Date	Thu Sep 27 00:01:00 GMT+200 2012
Expiry Date	Tue Dec 31 23:59:59 GMT+100 2013
License Type	EXTENDED_EVALUATION
State	OK
Activation Key	
Maximum Allowed Users	100
Maximum Allowed Users [warning]	100
Upload License	
scorecard.license	<input type="button" value="Browse..."/> <input type="button" value="Upload License File"/>

Figure 42: License is Now Uploaded

Once the un-activated license has been successfully uploaded, the **Activation Key** is visible on the **Product License** section of the **About** tab. Copy and paste the **Activation Key** into a new email and send it to the email address listed at <http://genesyslab.com/support/contact>. Genesys Support sends an activated license file. Save this file where it can be accessed easily. Do not rename the file.

Important:

If the license file is not accepted, ensure that it is named `scorecard.license`. Try uploading it in either Firefox or Internet Explorer if a different browser is used, or try again after restarting Call Recording.

If there is still an issue, contact Service and Support via the email address listed at <http://genesyslab.com/support/contact>.

Uploading the Activated Quality Manager License File

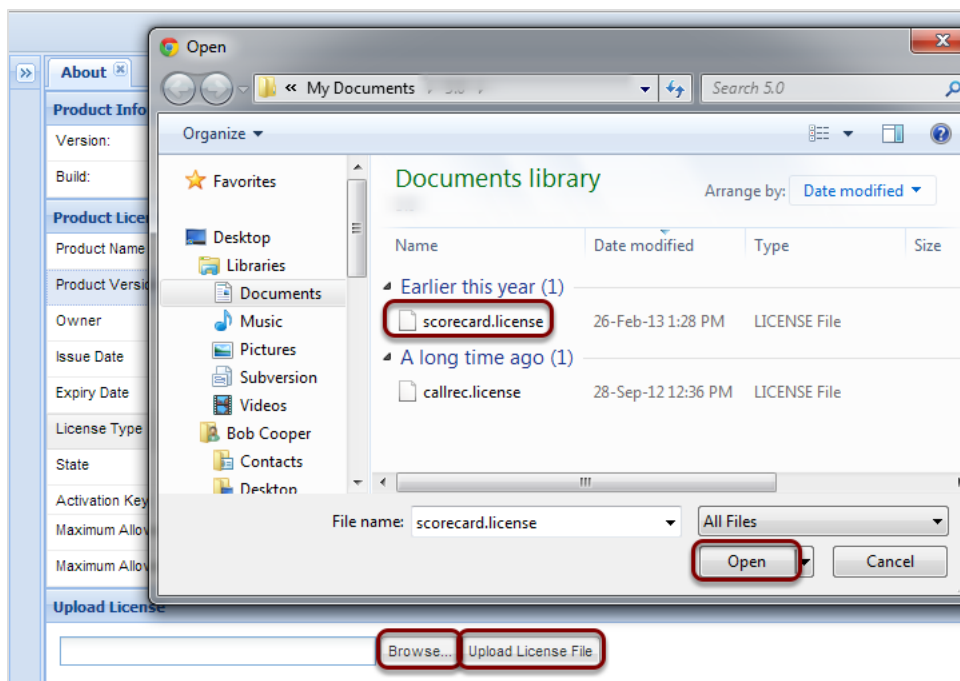


Figure 43: Browse to the License File

1. Click **Browse**, and navigate to the folder containing the activated licence file named `scorecard.license`.
2. Select the license file.
3. Click **Open**.
4. Click **Upload License File**.

Please check the information on the **About** tab.

Restart the GQM web server. Log in to the server using an ssh client. Log in as `admin`. Enter `su -` to log in as the root user. Enter the password, the default is `zoomcallrec`.

Restart the web UI using the following command:

```
/opt/callrec/bin/rc.callrec_web restart
```

Configuring Quality Manager in the Call Recording GUI

After Call Recording setup is complete and the Call Recording Web User Interface (UI) is available, view and edit the most important Call Recording configuration settings for Quality Manager by logging in to the Call Recording Web UI as an administrator.

Navigate to **Settings > Configuration > Quality Manager Setup**.

The tab opens.

Quality Manager Setup

Quality Manager Setup

Basic Setup

Quality Manager database	scorecard
Quality Manager Authentication Pool	scorecard
Call Recording database	callrec
Wrap up key	!! null !! This must be set in Advanced Search
Agent ID key	!! null !! This must be set in Advanced Search
URL to Call Recording stream	http://192.168.110.79:80
Login for Call Recording Media	scorecard
Password for Call Recording Media	!MF-Az~Z8RDERU1S,

SMTP Server

SMTP Server	192.168.159.21
-------------	----------------

Excel Reports Setup

Excel Template Path	././cz.zoom.scorecard.
Lower Grade Is Better	<input checked="" type="checkbox"/>

Save configuration
Reload configuration

Figure 44: Quality Manager Configuration - Basic Setup

Basic Settings

1. The **Basic Setup** section contains the following settings:
 - **Quality Manager database:** the database pool to use for Quality Manager data, that includes saved evaluations, user data, and media location (link) data. Database Pools are defined in **Settings > Call Recording Core > Database**.
 - **Quality Manager Authentication Pool:** the default database pool to use for Quality Manager authentication. This is usually set to the same value as for **Quality Manager database**.
 - **Wrap up key:** the external data key that identifies the agent wrapup data, obtained via a Call Recording integration module. This enables Quality Manager to use this value when searching for evaluations, for example. The value for this key should be GEN_TEV_CallID for Genesys taken from a custom advanced search **Item key**, specified in the **Advanced Search** column setup in the Web GUI: **Settings > Web UI > Search > Advanced Search**.
 - **Agent ID Key:** the external data key that identifies the agent ID in the Contact Center, obtained via a Call Recording integration module. This is essential because Quality Manager uses this value to access specific agent's calls in Call Recording, for example when the calls need to be evaluated. For more information about user setup in Quality Manager, please see the User Management section in the Quality Manager User Guide CC Manager document.

Important:

The **Agent ID Key** value must be GEN_TEV_ThisDN or GEN_TEV_AgentID for Genesys and must be the same as the **Item key** value for an Advanced Search column for external integration data, specified in the Web GUI: **Settings > Web UI > Search > Advanced Search**.

If these keys are not the same, Quality Manager reports such as the Interaction Volume chart does not function correctly.

For some integration scenarios, recorded call data is required before external data keys become available for selection in the Web GUI.

- **URL to Call Recording stream:** The base URL for access to media files for streaming. Updated only for custom installations and https secure communication.
- **Login for Call Recording Media:** The user account login for Quality Manager to access Call Recording media files.

- **Password for Call Recording Media:** The user account password for Quality Manager.

Important:

If the **Password for Call Recording Media** value is changed, users of Quality Manager are not be able to play evaluation media from Call Recording until the web server is restarted, using the following command (run with `root` user permissions):

```
/opt/callrec/bin/rc.callrec_web restart
```

It is therefore recommended that the default randomly generated password is not updated often.

2. The **SMTP Server** section enables a change of the sending email server, from the server set by default, to any another server.
3. **Excel Reports Setup** contains the following settings for exporting reports in spreadsheet format:
 - **Excel Template Path:** this points to the following location on a default Call Recording server installation:

```
/opt/callrec/web/webapps/scorecard-webui/cz.zoom.scorecard.webui.Scorecard/
```

This directory location contains the `styles.xlsx` template file.
 - **Lower Grade is Better** checkbox determines which order the grades are sorted in the exported spreadsheet. With the checkbox selected the lower scores are best and are sorted first; the higher numbers are worst and therefore appear last. With the checkbox unselected the reverse is true.

Rounding Strategy

The **Rounding Strategy** section sets the number of decimal places used for the weight value of answers in Quality Manager questionnaires.

Navigate to **Settings > Configuration > Quality Manager Setup**.



Rounding Strategy	
Default Scale	2
Points Scale	0
Percentage Scale	1
Grades Scale	3

Figure 45: Rounding Strategy

It is possible to set separate settings for:

- **Points Scale**
- **Percentage Scale**
- **Grades Scale**

Chapter

5

Configuring Genesys Driver for Recording

This section describes how to configure the Genesys Driver for and Genesys Active Recording and EPR .

This chapter contains the following sections:

[Setting up Genesys Driver](#)

[DN Activity Detection](#)

[Configuring DN Activity Detection](#)

[Configuring Notification of Recording](#)

[External Data Available from CIM](#)

[Configuring Full Agent Name Assembly](#)

[External Data](#)

Setting up Genesys Driver

The most important configuration is the address of the Configuration Manager. Configuration Manager provides Call Recording with a list of available T-Servers and their addresses.

Navigate to **Settings > Configuration > Protocol Drivers > Genesys Driver**.

The screenshot displays the 'Genesys Driver Configuration' web interface. On the left, a sidebar shows 'Genesys Driver' selected. The main content area has a red header 'Genesys Driver Configuration' and a green sub-header 'General Configuration'. Below this, several configuration fields are visible: 'Application Name' with the value 'CallREC_GIM', 'Primary Configuration Server Address', 'Secondary Configuration Server Address', 'Configuration Server User Name', and 'Configuration Server User Password'. The 'Operation Mode' dropdown menu is open, showing options: 'Active Recording', 'Enhanced Passive Recording', and 'Active Recording Replay Server'. At the bottom left, there are two red buttons: 'Save configuration' and 'Reload configuration'.

Figure 46: MSR Configuration

1. Enter the **Application Name** that has been created in Genesys Configuration Manager. For example, `CallREC_GIM`. See the section *Adding the Call Recording Application to the Configuration Manager* in the Pre-implementation Guide.
2. Type the **Primary Configuration Server Address**. This may be the hostname or IP Address of the Primary Configuration Server, or Configuration Server Proxy, or Single Configuration Server.
3. Type the **Secondary Configuration Server Address**. This may be the hostname or IP address of the Secondary Configuration Server, or leave empty if there is no Secondary Configuration Server.
4. Type the **Configuration Server User Name**.
5. Type the **Configuration Server User Password**.

Setting the Operation Mode in Genesys Driver

Navigate to **Settings > Configuration > Protocol Drivers > Genesys Driver**.

The screenshot shows the MSR Configuration interface with the following settings:

- Operation Mode:** Active Recording (dropdown menu)
- Geo-location Selection:** Do not send (dropdown menu)
- Send AttrExtensions "dest=":** (text input field)
- Send AttrExtensions "dest2=":** (text input field)
- Reconnect Enabled:**
- Reconnect Time (sec):** 30 (text input field)
- Update Period for Tenants and Agents (min):** 30 (text input field)
- Only Connect to Tenants Listed Below:**

At the bottom left, there are two buttons: **Save configuration** and **Reload configuration**.

Figure 47: MSR Configuration

1. Select the **Operation Mode: Active Recording, Enhanced Passive Recording, or Active Recording Replay Server**. The default is **Active Recording**.
2. Ensure that the **Reconnect Enabled** checkbox is checked (default).
3. Set the **Reconnect Time (sec)** in seconds (default 30 seconds).
4. Set the **Update Period for Tenants and Agents (min)** in minutes (default 30 minutes).

Click **Save Configuration** to save the configuration.

In addition for Active Recording mode only:

1. Select the **Geo-location Selection** option, which sets the `RequestPrivateService record` attribute. In a Dynamic Recording scenario, this enables Call Recording to specify where the recording leg is pinned to the Media Server:
 - **Do not send** (default): do not send a geo-location preference in this attribute.
 - **Source (thisDN)**: specify `record=source`. This is normally the extension (agent) DN and is the SIP Server default if the extension is not defined.
 - **Destination (otherDN)**: specify `record=destination`. This is normally the trunk (customer) DN.
2. Enter an optional value for **Send AttrExtensions "dest="**: Set the `RequestPrivateService dest` attribute; `dest` is the address

specifying the first server group for media duplication. If empty, the attribute is not sent.

3. Enter an optional value for **Send AttrExtensions: "dest2="**: Set the `RequestPrivateService dest2` attribute; `dest2` is the address specifying the second server group for media duplication. If empty, the attribute is not sent.

Click **Save configuration** to save the configuration.

Setting up Tenant Specific Parameters

If some tenants do not require recording then select to only record specific listed tenants. To do so, select the **Only connect to tenants listed below** checkbox. If there is only one tenant then do not select the **Only connect to tenants listed below** checkbox.

Navigate to **Settings > Protocol Drivers > Genesys Driver**.

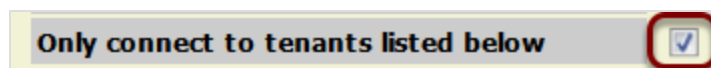


Figure 48: Only Connect to Tenants Listed below

At the bottom of the page, provide a list of tenants to be recorded.

Navigate to **Settings > Configuration > Protocol Drivers > Genesys Driver**. Scroll down.

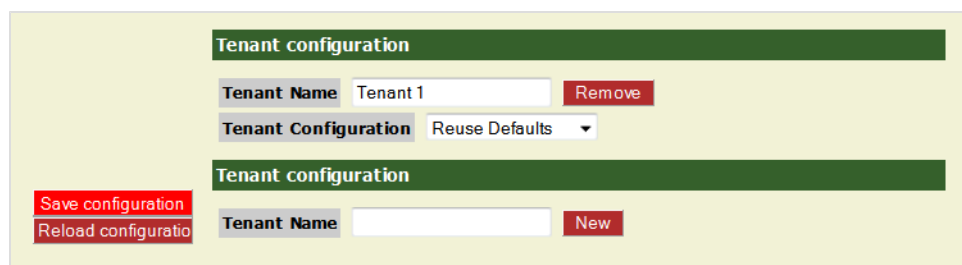


Figure 49: Tenant Configuration

For each tenant choose whether to:

1. Use the default the configuration options by selecting **Reuse Defaults**.
Configure each tenant separately by selecting **Override Defaults**:
2. If the default configuration is reused, the default configuration must include settings that cover all DNSs to be recorded for all tenants. Click **New** to provide space for the next **Tenant Name**.

Adding Tenant Information

Navigate to **Settings > Configuration > Protocol Drivers > Genesys Driver**.
Scroll down.

The screenshot displays the configuration interface for a tenant in the Genesys Driver. It is organized into several sections:

- Tenant Configuration:** Includes fields for Tenant Name (Tenant 1), Tenant Configuration Mode (Override Defaults), Client Identification (callrec), Tenant Password, and RTP Info Password. A 'Remove' button is next to the Tenant Name field.
- DN Activity Detection:** Includes fields for Include DN Range and Exclude DN Range, each with a 'New' button.
- Notification of Recording:** Includes sections for Audio and Video recording. Each section has an 'Enable' dropdown (set to 'Yes'), a 'Mandatory Part' field (e.g., RECORDING_STATU), and an 'Optional Part' field. Below these are 'User Data Value' fields for various states: State Recording (RECORDING_YES), State Not Recording (RECORDING_NO), State No Longer Recording (RECORDING_NO_LOI), State Prerecording (RECORDING_PPRE), and State Undefined (RECORDING_UNDEF).
- User Data Configuration:** Includes fields for User Data Key and User Data Name, with a 'New' button.
- Full Agent Name Assembly:** Includes an 'Enabled' checkbox (checked), a 'Names Order' dropdown (FirstName LastName), and a 'Delimiter' dropdown (Space (Example: "John Doe")).

At the bottom, there is a 'Tenant Configuration' section with a 'Tenant Name' field and a 'New' button. On the left side of the form, there are 'Save configuration' and 'Reload configuration' buttons.

Figure 50: Override Defaults

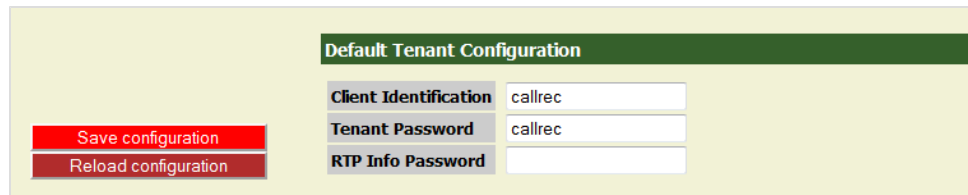
Configure the setting for each tenant in its **Tenant Configuration** section starting with the **Tenant Name**. If the tenant has more than one T-Server the T-Servers must use the same parameters for **Include DN Range**, **Exclude DN Range** and login.

The fields are the same as those in the **Default Tenant Configuration** and following sections.

Click **New** to provide space for the next tenant.

Default Tenant Configuration

Navigate to **Settings > Configuration > Protocol Drivers > Genesys Driver**.
Scroll down.



The screenshot shows a configuration form titled "Default Tenant Configuration". On the left side, there are two buttons: "Save configuration" (red) and "Reload configuration" (dark red). On the right side, there are three input fields with labels: "Client Identification" (containing "callrec"), "Tenant Password" (containing "callrec"), and "RTP Info Password" (empty).

Figure 51: Default Tenant Configuration

1. Type the **Client Identification**.
2. Type the **Tenant Password**.
3. Type the **RTP Info Password** if required. The RTP password is ignored in MSR mode.
4. Click **Save configuration**.

DN Activity Detection

Call Recording must monitor the activity of all Directory Numbers (DNs) to be recorded, including:

- DNs to be recorded by third parties.
- DNs configured to record all calls in the GVP Configuration Manager.
- DNs to be recorded because of a recording rule in Call Recording.

To monitor these DNs, Call Recording must subscribe to receive information from the SIP Server. Call Recording detects the activity of agent DNs, captures all relevant information, and determines whether the DNs should be recorded. If a DN is not monitored, then it is not recorded.

It is important that Call Recording does not subscribe to receive unnecessary information from DNs that is never recorded. This reduces the load on both the SIP server and the Call Recording server.

The **DN Activity Detection** configures which DNs Call Recording subscribes to for monitoring.

Specify a range of Agent DNs (for example 3000-3999) or an individual Agent DN (for example, 3556). Specify as many ranges as required.

Important:

If there is no number range stated in **Include DN range** and no DNs excluded in the **Exclude DN range** then all DNs are monitored.

GQM supports extensions, DNs, and terminals that include alphanumeric characters. The following characters are supported:

Character Type	Valid Characters
Letters	A-Z, a-z
Numbers	0-9
Symbols	@ & + \$ % ' . , : ; ! ~ () [] # - _

Table 2: Valid Alphanumeric Characters for Extensions, DNs and Terminals

Ranges can only use numeric characters, for example: 1234-5678, or a regular expression. Multiple ranges must be separated by commas (,) with no additional spaces, for example: 1000-1900, 2000-2700, 3200-3500.

For High Availability (HA) and load sharing where there are several instances of Call Recording Core, use **Include DN range** to configure each Call Recording Core to monitor a range of DNs. Then configure other Call Recording Cores to monitor the other ranges until all DNs are monitored by at least one Core.

Configuring DN Activity Detection

Navigate to **Settings > Configuration > Protocol Drivers > Genesys Driver**.

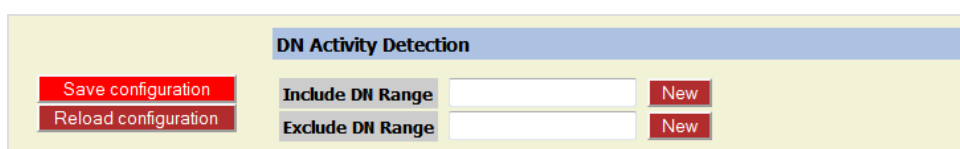


Figure 52: DN Activity Detection Configuration

1. Type a range of agent Directory Numbers in the **Include DN range** field to be monitored. If necessary, click **New** to create a new field for an additional **Include DN range**.
Repeat this for additional agents or ranges.
2. Optionally, enter a DN or range of DNs that do not require activity detection in the **Exclude DN range** field. If necessary, click **New** to create a new field for an additional **Exclude DN range**.
Repeat this for additional agents or ranges.
3. Click **Save configuration** to save changes.

Important:

Be careful which DNs are excluded. If a DN or range of DNs is excluded, recording is not processed, even if an external or third party application requests the recording.

Configuring Notification of Recording

Notification of recording	
Notification of audio recording enabled	YES ▾
User data key for audio notification - mandatory part	RECORDING_STATU
User data key for audio notification - optional part	GIM
Notification of video recording enabled	YES ▾
User data key for video notification - mandatory part	RECORDING_VIDEO_
User data key for video notification - optional part	GIM
User data value - state recording	RECORDING_YES
User data value - state not recording	RECORDING_NO
User data value - state no longer recording	RECORDING_NO_LOI
User data value - state prerecording	RECORDING_PRERE
User data value - state undefined	RECORDING_UNDEF

Figure 53: Notification of Recording

Call Recording can send a notification confirming whether a monitored DN call or screen capture is being recorded. This notification is in the form of attached data where the key consists of a mandatory and optional part linked by underscores, for example `RECORDING_STATUS_GIM`, the value part can be `YES` or `NO` as follows:

- **Notification of audio recording enabled:** select from the drop-down list. The default value is `YES`.
Notification of recording enables third party systems to display an icon on the agent desktop to indicate whether the call and screen are being recorded. This is useful, for example in the financial sector where certain transactions must be recorded and certain transactions must not be recorded, for instance credit card details.
- **User data key for audio notification - mandatory part:** select from the drop-down list. The default value is `RECORDING_STATUS`.
- **User data key for audio notification - optional part:** select from the drop-down list. The default value is `GIM`.
- **Notification of video recording enabled:** select from the drop-down list. The default value is `YES`.
- **User data key for video notification - mandatory part:** select from the drop-down list. The default value is `RECORDING_VIDEO_STATUS`.
- **User data value - state recording:** select from the drop-down list. The default value is `RECORDING_YES`.

- **User data value - state not recording:** select from the drop-down list. The default value is `RECORDING_NO`.
- **User data value - state no longer recording:** select from the drop-down list. The default value is `RECORDING_NO_LONGER`.
- **User data value - state prerecording:** select from the drop-down list. The default value is `RECORDING_PRERECORD`.
- **User data value - state undefined:** select from the drop-down list. The default value is `RECORDING_UNDEFINED`.

Click **Save configuration** to save the changes.

Important:

All of the values in **Notification of recording** are pre-defined defaults and should not change unless there is a specific need.

External Data Available from CIM

The data saved in the Call Recording external data table comes from various sources. The following information is available:

- basic call-related data.
- call-related user data (attached data).
- agent configuration data.
- extension Data.
- notification of recording.
- other GAD Data (only for Genesys Driver)
- other Call Recording Data (used internally by Call Recording)

The presence of specific data depends on the system configuration, routing design, network topology and on other conditions. Particular properties that must be stored in the Call Recording external data table must be configured during integration library implementation.

Setting Genesys Driver Encoding for Attached Data

The Genesys Driver assumes that any Attached Data received from the T-Server is in Unicode (UTF-8) format. However, the Genesys Platform SDK encodes this XML data according to the OS it is installed on.

Therefore if, for example, the Genesys software is installed on an OS with Czech encoding ('cp1250'), GIM does not store this correctly in the Call Recording database.

To avoid this encoding issue, an encoding parameter needs to be set manually in the Call Recording configuration file as follows:

1. Edit the Call Recording configuration file at:

```
/opt/callrec/etc/callrec.conf
```

2. Using a text editor add the parameter '-

Dfile.encoding=<encoding>' to the JAVA_OPTS_GENESYS environment variable found near the end of the file, for example, as follows:

```
JAVA_OPTS_CORE="-server -XX:+DisableExplicitGC -Xmx96m  
-Dcom.sun.CORBA.transport.ORBUseNIOSelectToWait=false -  
Dfile.encoding=cp1250"
```

3. Save the file and restart Call Recording:

```
/etc/init.d/callrec restart
```

Basic Call-related Data

Basic call-related data is available from real-time events generated when the T-Server notifies a client of call-based activity. These events arise when an observed phone performs actions like answering, transferring or hanging up the call. These events are a source of essential information about the agent activity.

The data is stored using the following naming convention:

External data key: `GEN_TEV_<TEvent.key>`

Example: `GEN_TEV_AgentID = "AG_3017"`

Default stored data keys are shown in bold text:

Key	Description
GEN_TEV_AgentID	Available by default. The agent identifier specified by the PBX or ACD.
GEN_TEV_ANI	Available by default. Automatic Number Identification. Specifies which number the current inbound call originates from.
GEN_TEV_CallID	Available by default. The call identifier provided by the switch (as opposed to connection identifier, or <code>ConnID</code> , which is assigned by T-Server).
GEN_TEV_CallUuid	Available by default. The UUID of the call; a unique call identifier provided by the Genesys platform
GEN_TEV_CallType	Available by default. Type of the call; one of the following values: Inbound, Outbound, Internal, Consult, Unknown
<code>GEN_TEV_CollectedDigits</code>	The digits that have been collected from the caller.
GEN_TEV_ConnID	Available by default. Connection identifier of the current call handled by the DN.
<code>GEN_TEV_CustomerID</code>	The string containing the customer identifier through which processing of the call was initiated.
GEN_TEV_DNIS	Available by default. The Directory Number Information Service. Specifies to which DN the current inbound call was made.
<code>GEN_TEV_NetworkCallID</code>	In the case of network routing, the call identifier assigned by the switch where the call initially arrived.

Key	Description
GEN_TEV_NetworkNodeID	In the case of network routing, the identifier of the switch where the call initially arrived.
GEN_TEV_NodeID	The unique identifier of a switch within a network.
GEN_TEV_OtherDN	Available by default. The other main Directory Number (which your application did not register) involved in this request or event. For instance, the DN of the main party of the call.
GEN_TEV_ThisDN	Available by default. The Directory Number (which the application registered) involved in this request or event.
GEN_TEV_ThisQueue	The queue related to <code>ThisDN</code> .

Table 3: Basic Call-related Data

Important:

If the value is empty then that key is not stored in the Call Recording database.

This list can be changed manually in the driver configuration in the xml in the equal group `messageDataKeys` with values `msgDataKey` and `coupleMsgDataKey`, which define the call event's attribute name and key that should be used for external data in Call Recording. If at least one basic call-related data attribute is set, no default is used and all required attributes must be configured. The following code shows how to store `CallID` and `ThisDN` where `ThisDN` is renamed to `SomeDN` for storage in Call Recording.

```
<SpecifiedConfiguration name="genesysDriver">
...
<EqualGroup name="messageDataKeys">
<Value name="msgDataKey">CallID</Value>
<Value name="coupleMsgDataKey">CallID</Value>
</EqualGroup>
<EqualGroup name="messageDataKeys">
<Value name="msgDataKey">ThisDN</Value>
<Value name="coupleMsgDataKey">ThisDN</Value>
</EqualGroup>
...
```

For Legacy GIM integration the `SpecifiedConfiguration` name is "genesys".


```
<SpecifiedConfiguration name="genesys">
```

The rest of the listing is the same as the example above.

Call-related User Data

User data or attached data is a set of call-related information predefined by agent or application handling the call. A user data object is structured as a list of data items described as key-value pairs.

User data can arrive at a client application with any event, at any time even after the call is cleared, for example, when the agent fills in wrap-up information.

Any value extracted from user data is attached using the following naming convention:

External data key: `GEN_USR_<UserData.key>`

Example: `GEN_USR_RStrategyName = "default"`

Important:

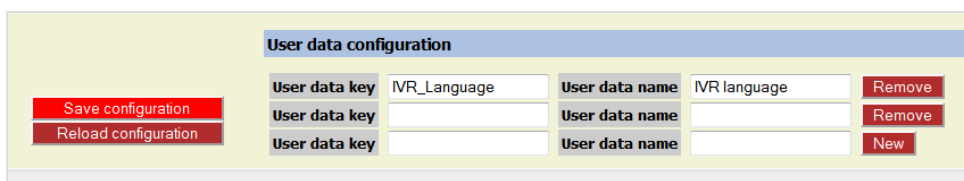
The list of the user data to attach must be defined in the configuration. By default no user data gets attached.

User data configuration

The **User data configuration** option enables the definition of Genesys User Attached Data.

Navigate to **Settings > Configuration > Protocol Drivers > Genesys Driver** and scroll down to **User Data Configuration**.

Only the user data in the column **User Defined Parameters** can be added in the GIM configuration section of the Call Recording GUI. Other non-default, pre-defined keys can be specified in the integration configuration file (`/opt/callrec/etc/integration.xml`) in XML format. These values should not be modified unless there is a very good reason to do so.



The screenshot shows a web interface titled "User data configuration". On the left, there are two red buttons: "Save configuration" and "Reload configuration". The main area contains a table with two columns: "User data key" and "User data name". The first row has "IVR_Language" in the key field and "IVR language" in the name field, with a "Remove" button to its right. The second row has empty fields and a "Remove" button. The third row has empty fields and a "New" button.

User data key	User data name	
IVR_Language	IVR language	Remove
		Remove
		New

Figure 54: Adding a User Data Definition Key

To add a **User data key** definition to GIM configuration:

1. Type the **User data key** and **User data name**(value).
2. Click **New** to add another key value pair if necessary.
3. Click **Save Configuration** to save the changes.

Agent Configuration Data

Configuration data objects enable the client to get any information about the user, agent, server or other object configuration stored in the Genesys configuration database in addition to information about the current state of the specific object.

Any value available from the configuration library should be attached using the following naming convention:

Externaldata key: `GEN_CFG_<CfgData.key>`

Example: `GEN_CFG_UserName = "jsmith"`

The following information is available from the Configuration Platform SDK:

Default stored agent data keys are shown in bold text:

Key	Description
GEN_CFG_EmployeeID	Available by default. The code identifying the person within the tenant staff.
GEN_CFG_FirstName	Available by default. The person's first name.
GEN_CFG_LastName	Available by default. The person's last name
GEN_CFG_UserName	Available by default. The name the person uses to log into a CTI system
GEN_CFG_AdminType	Specifies whether the person is configured as '=Admin'. Yes=1, No=0
GEN_CFG_AgentType	Specifies whether the person is configured as '=Agent'. Yes=1, No=0
GEN_CFG_PlaceDbid	A unique identifier of the Place assigned to this agent by default.
GEN_CFG_State	The current state of the person object.

Table 4: Agent Configuration Data

Some of the properties, namely LoginInfo and SkillInfo contain more items as agent can have more logins or more skills. In that case Call Recording saves them as indexed fields:

Key	Description
GEN_CFG_AgentLoginInfo_:_LoginDbid	agent-LoginDBID — A unique identifier of the Agent Login identifier
GEN_CFG_AgentLoginInfo_:_WrapupTime	wrapupTime — Wrap-up time in seconds associated with this login identifier. Cannot be a negative value
GEN_CFG_AgentSkillLevels_:_SkillDbid	skillDBID — A unique identifier of the skill the level relates to.
GEN_CFG_AgentSkillLevels_:_Level	level — Level of the skill. Cannot be a negative value.

Table 5: Agent Configuration Data

Important:

If the value is empty then thatkey is not stored in the Call Recording database.

This list can be changed in driver configuration manually in xml in equal group `agentDataKeys` with values `agentDataKey` and `coupleAgentDataKey`, which define event Telephonic attribute name and key which should be used for external data in Call Recording. If at least one Agent Data attribute is set, no default is used and all required attributes must be configured. Following listing shows configuration of storing only `EmployeeID`.

```
<SpecifiedConfiguration name="genesysDriver">
...
<EqualGroup name="agentDataKeys">
<Value name="agentDataKey">EmployeeID</Value>
<Value name="coupleAgentDataKey">EmployeeID</Value>
```

```
</EqualGroup>  
...
```

For Passive GIM integration the SpecifiedConfiguration name is "genesys".

```
<SpecifiedConfiguration name="genesys">
```

The rest of the listing is the same as the example above.

Extension Data

Extension data is stored with `GEN_EXT_` prefix. This data is taken from the Extensions section of Genesys voice events. None of this data is stored by default.

The required data can be configured in driver configuration manually in the xml in the equal group `extensionDataKeys` with values `extDataKey` and `coupleExtDataKey`, which define event Extension attribute name and key which should be used for external data in CallREC. Following listing shows configuration of storing `BusinessID`.

```
<SpecifiedConfiguration name="genesysDriver">
...
<EqualGroup name="extensionDataKeys">
<Value name="extDataKey">BusinessID</Value>
<Value name="coupleExtDataKey">BusinessID</Value>
</EqualGroup>
...
```

For Passive GIM integration the SpecifiedConfiguration name is "genesys".

```
<SpecifiedConfiguration name="genesys">
```

The rest of the listing is the same as the example above.

Other Genesys Driver Data

Genesys Driver and GIM also store some other Genesys related data. The following are not configurable.

`GEN_REC_` - external data with the signaling of recording state for audio and video .

`GEN_CONFERENCE_MEMBERS` - list of parties participating in conference Couple. Only available from Genesys Driver not GIM.

`GEN_CFG_FULLNAME` - full name of agent created according to configuration.

`GEN_CFG_Tenant` - call Tenant. Only available from Genesys Driver in Active recording mode not GIM.

`GEN_CFG_Switch` - call Switch. Only available from Genesys Driver in Active recording mode not GIM.

`GEN_TEV_CSUP_MODE` - call supervision mode: with the value `Monitoring` or `Coaching`. Only available from Genesys Driver in EPR or Active Recording mode not GIM.

`GEN_TEV_CSUP_SCOPE` - call supervision scope: with the value `Call` or `Agent`. Only available from Genesys Driver in EPR or Active Recording mode not GIM.

`GEN_TEV_CSUP_SUPID` - the agent ID of the monitoring Supervisor. Only available from Genesys Driver in EPR or Active Recording mode not GIM.

`GEN_TEV_CSUP_SUPDN` - the DN of the Monitoring Supervisor. Only available from Genesys Driver in EPR or Active Recording mode not GIM.

Configuring Full Agent Name Assembly

The **Full agent name assembly** decides how names from the integration are treated to make them easier to read in Call Recording reports.

Figure 55: Full Agent Name Assembly

The display of Genesys agent names can be defined in the **Full agent name assembly** section of Genesys driver configuration using a combination of the **Names order** and **Delimiter** options (including a custom delimiter). The following variations can be achieved, assuming a sample agent name of John Smith:

Sample	Name Order Setting	Delimiter Setting	Custom Delimiter Value [5 char limit]
John Smith	"Firstname Lastname"	"Space"	(not visible)
Smith, John	"Firstname Lastname"	"Comma + space"	(not visible)
Smith - John	"Firstname Lastname"	"Custom"	- (space dash space)

Table 6: Agent Name Configuration

External Data

The following T-Server External data is collected (see the earlier tables for definitions):

GEN_TEV_ANI
GEN_TEV_CallID
GEN_TEV_CallType
GEN_TEV_CallUuid
GEN_TEV_ConnID
GEN_TEV_DNIS
GEN_TEV_OtherDN
GEN_TEV_ThisDN

The following Agent External data is collected:

GEN_CFG_DEST_EmployeeID
GEN_CFG_DEST_FirstName
GEN_CFG_DEST_FULLNAME
GEN_CFG_DEST_LastName
GEN_CFG_DEST_UserName
GEN_TEV_AgentID

All other user-defined data must be configured in the Call Recording GUI web interface using key/name pairs syntax, for instance: GENESYS_KEYNAME : QM_KEYNAME.

Single Agent Call

If there is one agent in the call, then we have the following T-Server and Config Server messages (related to the calling party):

GEN_TEV_AgentId
GEN_CFG_EmployeeID

```
GEN_CFG_FirstName  
GEN_CFG_FULLNAME  
GEN_CFG_LastName  
GEN_CFG_UserName
```

Two Agent Call

If there are two agents in the call we get the following in addition to the single agent call messages above if using MSR or EPR (note the `_OTHER_` suffix):

```
GEN_TEV_OTHER_AgentId  
GEN_CFG_OTHER_EmployeeID  
GEN_CFG_OTHER_FirstName  
GEN_CFG_OTHER_FULLNAME  
GEN_CFG_OTHER_LastName  
GEN_CFG_OTHER_UserName
```

This additional information identifies the called party, so both the agents and their call roles can easily be identified.

Chapter

6

Integrating Genesys CIM with GQM Using GIM

The Genesys Integration Module (GIM) is a basic Genesys CIM integration module that provides information about agents and other attached data from CIM T-Server to Call Recording. This attached data can then be used in searches for call recording and so on.

This chapter contains the following sections:

[Genesys Passive Recording](#)

[Installing the Genesys Integration Module](#)

[External Data Available from Genesys CIM for GIM](#)

[Configuring the Integration Module](#)

[Configuring the Application Names and Address for GIM](#)

[Configuring the T-Server and Configuration Server for GIM](#)

[Configuring the DN Range for Attached Data](#)

[Configuring Notification of Recording for GIM](#)

Genesys Passive Recording

Genesys Passive recording uses the following services:

- the GIM service provides the attached data from the CIM T-server.
- the SIP service captures signaling from the SPAN port.
- the RS service captures the voice data of the calls from the SPAN port.

To implement Genesys Passive recording, select the GIM service, the RS service, and the SIP service.

Where possible, it is recommended to use the Genesys Driver service that offers deeper, more complete CIM integration with Genesys Call Recording.

Installing the Genesys Integration Module

The Genesys Integration Module is installed if selected during Call Recording setup. It can also be installed manually later.

To install the Genesys Integration Module manually:

1. Upload the standard RPM package (for example: `callrec-genesys-5.0.r-b.rpm`, where 5.0 is the major version of GQM, r stands for the release number and b stands for the build number of the Genesys Integration Module)
2. Install it with the following command:

```
rpm -i callrec-genesys-5.0.r-b.rpm
```

External Data Available from Genesys CIM for GIM

The data saved in the Call Recording external data table comes from various sources. The following information is available using GIM:

- basic call-related data.
- call-related user data or attached data.
- agent configuration data.
- extension data.
- notification of recording.

For the external available data see [External Data Available from CIM](#).

Setting GIM Encoding for Attached Data

The Genesys Integration Module assumes that any Attached Data received from the T-Server is in Unicode (UTF-8) format. However, the Genesys Platform SDK encodes this XML data according to the OS it is installed on.

Therefore if, for example, the Genesys software is installed on an OS with Czech encoding ('cp1250'), GIM does not store this correctly in the Call Recording database.

To avoid this encoding issue, an encoding parameter needs to be set manually in the Call Recording configuration file as follows:

1. Edit the Call Recording configuration file at:

```
/opt/callrec/etc/callrec.conf
```

2. Using a text editor add the parameter '-

`Dfile.encoding=<encoding>' to the JAVA_OPTS_GENESYS environment variable found near the end of the file, for example, as follows:`

```
JAVA_OPTS_GENESYS="-server -XX:NewSize=24m -XX:SurvivorRatio=16 -  
XX:MaxNewSize=24m -Xms32m -Xmx32m -Dfile.encoding=cp1250"
```

3. Save the file and restart Call Recording:

```
/etc/init.d/callrec restart
```

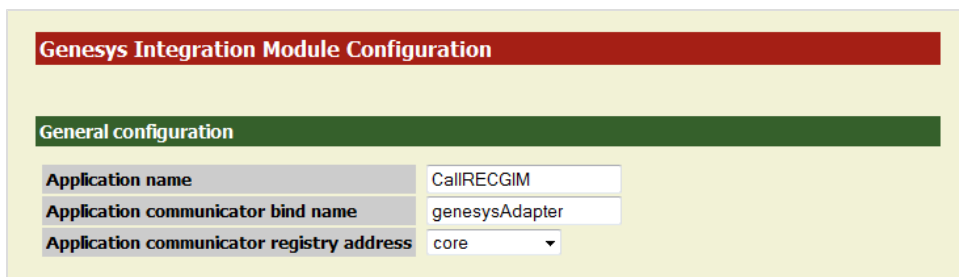
Configuring the Integration Module

Once the Genesys Integration Module is installed in Call Recording, log in as admin privileges and navigate to **Settings > Configuration > Integration > Genesys**.

The Integration tab does not appear unless an integration module is installed.

Configuring the Application Names and Address for GIM

Navigate to **Settings > Configuration > Integration > Genesys**.



The screenshot shows a web interface for configuring the Genesys Integration Module. At the top, there is a red header bar with the text "Genesys Integration Module Configuration". Below this is a green header bar with the text "General configuration". Underneath, there are three configuration fields:

Application name	CallRECGIM
Application communicator bind name	genesysAdapter
Application communicator registry address	core

Figure 56: Genesys Integration Module Configuration

The **Application name** for Genesys integration is set during Call Recording installation. The default value **CallRECGIM** can be used for most installations.

1. Type the name of the integration module to register on RMI in the **Application communicator bind name** field, for example, **genesysAdapter**.
2. Select the **Application communicator registry address** server, for example, **core**, this is the server with the RMI service running as defined in the servers part of the configuration.

Configuring the T-Server and Configuration Server for GIM

Navigate to **Settings > Configuration > Integration > Genesys**.

Specify the connection details for communication with **T-Server** and **Configuration Server**. The Integration Module is also capable of automatic reconnection in case the connection fails; this can be configured as part of the connection details.

Module specific configuration		
T-Server address	//192.168.110.74:3063	Remove
T-Server address	//192.168.110.75:3063	Remove
T-Server address	//ipAddress:3000	New
T-Server user name	callrec	
T-Server user password	callrec	
Configuration server address	//192.168.110.74:2020	Remove
Configuration server address	//192.168.110.75:2020	Remove
Configuration server address	//ipAddress:2200	New
Configuration server user name	callrec	
Configuration server user password	callrec	
Agent list update period (min)	5	
DN update period (min)	30	
Save configuration		
Reload configuration		
Reconnect enabled	YES	▼
Reconnect time (sec)	30	

Figure 57: Module Specific Configuration

Set up connection properties for the T-Servers, IP address, port, and login credentials:

1. Type the IP address and port of a T-Server in the **T-Server address** field in the format `//server:port`.
2. Click **New**.
Add as many T-Servers as required.
3. Type the T-Server user name in the **T-Server user name** field.
4. Type the T-Server user password in the **T-Server user password** field.
The user name and password are for a user that was recently created for GIM authorization.

Set up the connection properties for the Configuration Servers, IP address, port, and login credentials:

1. Type the IP address and port of the Configuration Server in the **Configuration Server address field** in the format `//server:port`.
2. Click **New**.
Add as many Configuration Servers as required.
3. Type the Configuration Server user name in the **Configuration Server user name field**.
4. Type the Configuration Server password in the **Configuration Server password field**.
The username and password are for a user that was recently created for GIM authorization.
5. Select the **Agent list update interval**, in minutes, for how often Call Recording requests data from the Configuration Server. The default value is 5 minutes.
6. Select the **DN update period**, in minutes, the default is 30. This sets the interval between synchronization updates with the Configuration Server. During synchronization, the list of DNs is checked, and any changes made on the T-Server (DN added/removed/enabled/disabled) are reflected in Call Recording.
7. To set up an automatic reconnection option, choose **YES** in the **Reconnect enabled** drop-down list and select a **Reconnect time** value.
The default value is 30 seconds.
8. To save the changes, click **Save configuration**.

After configuring the Genesys Integration Module, two additional operations must be performed for the module to operate correctly:

1. **Activate the module:** The GIM module is licensed, so a Call Recording license must be purchased and installed that also includes licensing for Genesys CIM integration.
2. **At least one recording rule must be present** (for example the “record all calls” rule using an asterisk “*”): See the **Creating Recording Rules** chapter in the *Call Recording User Guide*.

Configuring the DN Range for Attached Data

The **Agents Configuration** enables the user to select Agent DNs (Directory numbers) to be monitored by Call Recording to supply attached data. Specify a range of Agent DNs (for example 3000-3999) or an individual Agent DN (for example, 3556). Specify as many ranges as required.

Navigate to **Settings > Configuration > Integration > Genesys**.

Figure 58: Agents Configuration

1. Type a range of Agent Directory Numbers in the **Agent DN range** field.
2. Click **New** if you require an additional range.
Repeat for additional ranges.
3. Enter a range of Directory Numbers in the **Disabled DN range** field.

GQM supports extensions, DNs, and terminals that include alphanumeric characters. The following characters are supported:

Character Type	Valid Characters
Letters	A-Z, a-z
Numbers	0-9
Symbols	@ & + \$ % ' . , : ; ! ~ () [] # - _

Table 7: Valid Alphanumeric Characters for Extensions, DNs and Terminals

Ranges can only use numeric characters, for example: 1234-5678, or a regular expression. Multiple ranges must be separated by commas (,) with no additional spaces, for example: 1000-1900, 2000-2700, 3200-3500.

4. Click **New** if an additional range is required.
Repeat for additional ranges.
5. To save click **Save configuration**.

If no numbers or ranges are specified, Call Recording processes all Genesys calls.

Configuring Notification of Recording for GIM

Navigate to **Settings > Configuration > Integration > Genesys**.

Notification of recording	
Notification of audio recording enabled	YES ▾
User data key for audio notification - mandatory part	RECORDING_STATUS
User data key for audio notification - optional part	GIM_1
Notification of video recording enabled	NO ▾
User data key for video notification - mandatory part	RECORDING_VIDEO_S
User data key for video notification - optional part	GIM
User data value - state recording	RECORDING_YES
User data value - state not recording	RECORDING_NO
User data value - state no longer recording	RECORDING_NO_LON
User data value - state prerecording	RECORDING_PRERECD
User data value - state undefined	RECORDING_UNDEFIN

Save configuration
Reload configuration

Figure 59: Notification of Recording for GIM

Call Recording can send a notification confirming whether a monitored DN call or screen capture is being recorded. This notification is in the form of attached data where the key consists of a mandatory and optional part linked by underscores, for example `RECORDING_STATUS_GIM`, the value part can be YES or NO as follows:

Do not change the default values in **Notification of recording**.

- **Notification of audio recording enabled:** select from the drop-down list. The default value is YES. **Notification of recording** enables third party systems to display an icon on the agent desktop to indicate if the call and screen are being recorded. This is useful, for example in the financial sector where certain transactions must be recorded and certain transactions must not be recorded, for instance credit card details.
- **User data key for audio notification - mandatory part:** select from the drop-down list. The default value is `RECORDING_STATUS`.
- **User data key for audio notification - optional part:** select from the drop-down list. The default value is `GIM`.
- **Notification of video recording enabled:** select from the drop-down list. The default value is YES.

- **User data key for video notification - mandatory part:** select from the drop-down list. The default value is `RECORDING_VIDEO_STATUS`.
- **User data value - state recording:** select from the drop-down list. The default value is `RECORDING_YES`.
- **User data value - state not recording:** select from the drop-down list. The default value is `RECORDING_NO`.
- **User data value - state no longer recording:** select from the drop-down list. The default value is `RECORDING_NO_LONGER`.
- **User data value - state prerecording:** select from the drop-down list. The default value is `RECORDING_PRERECORD`.
- **User data value - state undefined:** select from the drop-down list. The default value is `RECORDING_UNDEFINED`.

Click **Save Configuration** to save the changes.

Chapter

7

Configuring Avaya Driver for Recording

This section describes how to configure the Avaya Driver in Call Recording and AES Management Console.

This chapter contains the following sections:

[Setting up Avaya Driver](#)

[Viewing and Configuring the AES Server Settings](#)

[Configuring the TSAPI Interface](#)

[Configuring the DMCC Interface](#)

[Adding and Configuring the Recorder Groups](#)

[Configuring the Recorder Settings](#)

[Settings for Multi Server Installations](#)

Setting up Avaya Driver

Navigate to **Settings > Configuration > Protocol Drivers > Avaya Driver**.

Avaya Driver Configuration	
AES Server Configuration	
Hostname or IP Address	192.168.112.35
Server Name	AVAYA1AES
Switch Connection	CM
Cleanup Timeout (sec)	60
Duration Timeout (sec)	180
TSAPI Interface Configuration	
Provider Tlink	AVAYA#CMSIM#CSTA
User Name	zoom
Password	Avaya@dimn1
TSAPI Port	450
DMCC Interface Configuration	
User Name	zoom
Password	Avaya@dimn1
DMCC Port	4721
Recorder Settings	
Recording Device Range	6030-6033
RTP Port Range	9000-9099
IP Station Security Code	1234
Recorder Group	Recorders Group 1

Save configuration
Reload configuration

Figure 60: Avaya Configuration

Many of the settings are configured during Call Recording setup. View and if necessary modify these settings in the Avaya **Driver Configuration**.

Viewing and Configuring the AES Server Settings

Navigate to **Settings > Configuration > Protocol Drivers > Avaya Driver** and scroll down.

AES Server Configuration	
Hostname or IP Address	192.168.112.35
Server Name	AVAYA1AES
Switch Connection	CM
Cleanup timeout (sec)	60
Duration timeout (sec)	180

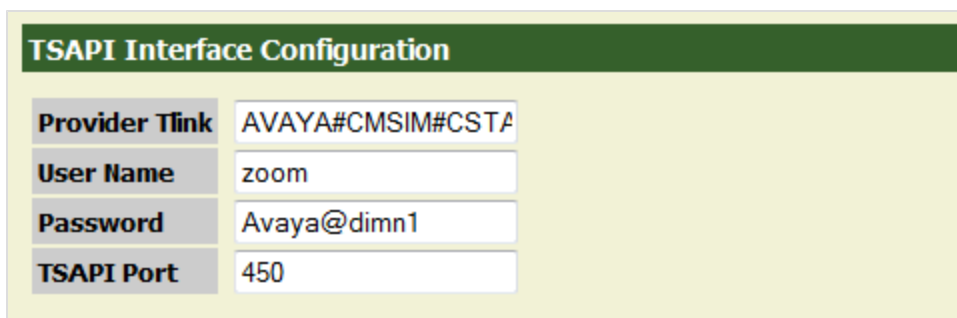
Figure 61: AES Server Settings

1. View the preconfigured **Hostname or IP Address** for the AES server. This is the IP address or hostname of the Application Enablement Services API connector server. This field must not be empty.
2. Type the **Server Name**. This may be any string.
3. View the preconfigured **Switch Connection** Switch alias. This may be any non empty string.
4. Set the **Cleanup timeout** timer value in seconds. This timer defaults to 0 for backwards compatibility purposes, but it should be set to a higher value, such as 60. After the loss of the connection to the client machine is detected, the session is not terminated until this timer expires. It is possible to resume the session with `reconnect()` if the session has not terminated.
5. Set the **Duration timeout** timer value in seconds. This is a timer to maintain active heart beat between the client application and the server. If the heart beat is not received within this timer value, then the server assumes the client application is terminated. This timer defaults to 60 seconds and the allowed range is between 30 seconds and two hours. However, if this value is set to a big number, then the server takes a long time to detect that the client application is terminated.

Click **Save configuration** and restart Call Recording at the end of the process to activate the new settings.

Configuring the TSAPI Interface

Navigate to **Settings > Configuration > Protocol Drivers > Avaya Driver** and scroll down.



TSAPI Interface Configuration	
Provider Tlink	AVAYA#CMSIM#CSTA
User Name	zoom
Password	Avaya@dimn1
TSAPI Port	450

Figure 62: TSAPI Interface Configuration

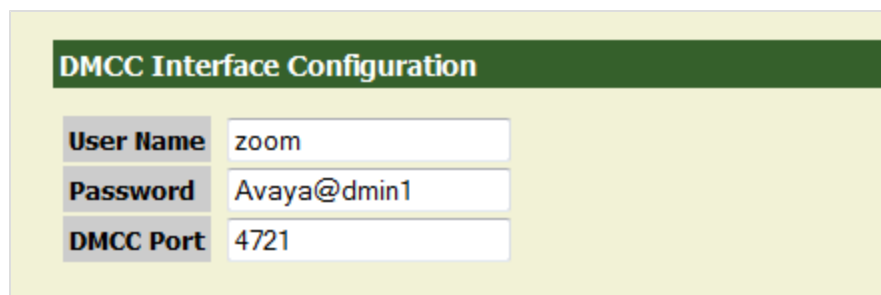
1. View the preconfigured **Provider Tlink**. The Service name or 'provider string' obtained from the Avaya administrator. This may be any non empty string separated using '#', for example, AVAYA#CM#CSTA#AVAYA1AES.
2. View the preconfigured TSAPI **User Name**. This may be any non empty string.
3. View the preconfigured TSAPI **Password**. This may be any non empty string.
4. View the preconfigured **TSAPI Port**.

Click **Save configuration** to activate the new settings. Do not need to restart Call Recording.

Configuring the DMCC Interface

Recorder settings contains Avaya virtual recording devices settings and Call Recording recorders and ports settings.

Navigate to **Settings > Protocol Drivers > Avaya Driver** and scroll down.



DMCC Interface Configuration	
User Name	zoom
Password	Avaya@dmin1
DMCC Port	4721

Figure 63: CM Server Configuration

1. View the preconfigured **DMCC User Name** for the Communication Manager API connector server, obtained from the Avaya administrator. The field must not be empty.
2. View the preconfigured **Password** obtained from Avaya administrator. This can be any non empty string.
3. View the preconfigured **Port number** of the connector server (obtained from the Avaya administrator). This must be between 1025 and 65535. The default port for DMCC is 4721.

Click **Save configuration** and restart Call Recording at the end of the process to activate the new settings.

Adding and Configuring the Recorder Groups

Navigate to **Settings > Configuration > Recorders > Recorder Groups**.

The screenshot shows the 'Recorder Groups' section of a web interface. At the top, there is a green header with the text 'Recorder Groups'. Below this, there is a form with two main fields: 'Group name' with the value 'Recorders Group 1' and 'Group load balancing method' with a dropdown menu set to 'Broadcast'. To the right of these fields is a red 'New' button.

Figure 64: Adding a Recorder Group

To add a **Recorder Group**:

1. Type a name for the new recording group in **Group name**. This may be any non empty string.
2. Click **New**.

A **Recorder Groups** section opens up with the name of the new recorder group.

The screenshot shows the 'Recorder Groups' section of a web interface. At the top, there is a green header with the text 'Recorder Groups'. Below this, there is a section titled 'Recorders Group 1' in a blue box. This section contains several fields: 'Group name' (Recorders Group 1), 'Group load balancing method' (Broadcast), and a 'Remove' button. Below these are four fields for a recorder: 'Recorder name' (Recorder 1), 'Naming service URL' (core), 'Bind name' (recordManager_eth0), and 'Recorder weight' (empty). A 'Remove' button is next to the 'Recorder name' field. Below this is another set of fields for a new recorder: 'Recorder name' (New recorder name), 'Naming service URL' (core), 'Bind name' (Recorder_bind_name), and 'Recorder weight' (1). A 'New' button is next to the 'Recorder weight' field. At the bottom, there are fields for a new group: 'Group name' (New group name) and 'Group load balancing method' (Broadcast), with a 'New' button.

Figure 65: Recorder Groups

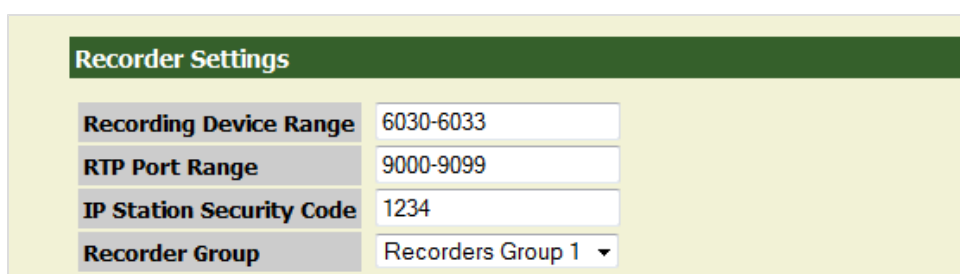
1. Type a name for the new recorder in **Recorder name**. This may be any non empty string.

2. Select the **Naming service URL** from the drop-down list.
3. Type the RMI **Bind name**. This may be a non empty string.
4. Type a name for the new recording group in **Group name**.
5. Click **New** to create an extra section for another recorder.

Click **Save configuration** and restart Call Recording at the end of the process to activate the new settings.

Configuring the Recorder Settings

Navigate to **Settings > Configuration > Protocol Drivers > Avaya Driver**.



Recorder Settings	
Recording Device Range	6030-6033
RTP Port Range	9000-9099
IP Station Security Code	1234
Recorder Group	Recorders Group 1 ▼

Figure 66: Recorder Settings

1. View the preconfigured **Recording Device Range**. This is the range of terminal extensions used as an Avaya virtual recording device (this must be configured on the Avaya server). The range consists of two numbers joined by -. This can be any number.
2. View the preconfigured **RTP Port Range**. This is the port range used by Call Recording recorders. The range consists of two numbers joined by -. The default is 9000-9099.
3. View the preconfigured the **IP Station Security Code**.
4. Select the **Recorder Group** from the drop-down list predefined in **Recorders Configuration**.

Click **Save configuration** and restart Call Recording before these settings take effect. There are further tasks to configure in Avaya Driver that require the steps to click **Save configuration** and restart Call Recording, wait until these have been completed before doing so.

Settings for Multi Server Installations

For cluster installations of RS servers the packet pool settings must be increased from the default of 400 to 600. Administrators must check and setup parameter `-s 600` manually on all recording servers.

To increase the packet pool settings:

1. Locate and open the file `/opt/callrec/etc/callrec.derived`
2. Locate the `RS_PARAMS` variable and add the `-s 600` parameter there

```
#  
# Record server  
#  
RS_IORFILE="$TMP/rs"  
RS_PARAMS="-s 600 -t 120 -m 40 -A 0 -A 8 -A 9 -A 18 -A 13 -A 19"
```

Configuring the Terminal Activity Detection

Navigate to **Settings > Configuration > Protocol Drivers > Avaya Driver** and scroll down.

Terminal Activity Detection		
Include Terminal Range	6021-6023	Remove
Include Terminal Range	6101	Remove
Include Terminal Range		New
Exclude Terminal Range		New

Figure 67: Terminal Activity Detection

QGM supports extensions, DNs, and terminals that include alphanumeric characters. The following characters are supported:

Character Type	Valid Characters
Letters	A-Z, a-z
Numbers	0-9
Symbols	@ & + \$ % ' . , : ; ! ~ () [] # - _

Table 8: Valid Alphanumeric Characters for Extensions, DNs and Terminals

Ranges can only use numeric characters, for example: 1234-5678, or a regular expression. Multiple ranges must be separated by commas (,) with no additional spaces, for example: 1000-1900, 2000-2700, 3200-3500.

1. Specify a range or list of terminals to monitor in the **Include Terminal Range** field. Only monitored terminals can be recorded.
2. Specify a range or list of terminals to exclude from monitoring in the **Exclude Terminal Range** field. These terminals are not monitored and not recorded.
3. Click **New** to create a new field for an extra range.
4. Click **Remove** to remove an unwanted range.

Click **Save configuration** and restart Call Recording before these settings take effect.

Important:

Remember every terminal monitored requires an extra TSAPI license so it is expensive to monitor terminals unnecessarily.

Fixpayloads

The Fixpayloads tool is a java application. In a SIP negotiated telephony session, each stream of the conversation may be encoded in a different codec. The decoder process in Call Recording is only designed to support the same codec in both streams. If the codecs are different, then the calls must be repaired before you can listen to them.

The Fixpayloads tool, periodically scans the database and repairs the affected calls. The tool re-encodes each call channel separately (using the Call Recording service) and then mixes the two mp3 files into one file using the command line utility `SoX(1)`.

The Fixpayloads tool is not connected to the configuration service. Configure the Fixpayloads tool by editing a startup script located in `/opt/callrec/bin/rc.callrec_fixpayload`. The configuration is done in the startup script variable `FIXPAYLOAD_PARAMS`:

For example:

```
FIXPAYLOAD_PARAMS="-c 0 -s 120 -l 100 -d localhost -p 5432 -u callrec -w  
callrec -n callrec"
```

List of tool parameters:

`-c, --count <arg>` Where `<arg>` is the repetition count (use 0 for daemon-like behavior).

`-s, --sleep <arg>` Where `<arg>` is the sleep time in seconds (between batch count).

`-l, --limit <arg>` Where `<arg>` is the maximum number of results retrieved during one batch processing.

`-d, --dbhost <arg>`: Where `<arg>` is the database host.

`-p, --dbport <arg>` Where `<arg>` is the database port.

`-u, --dbusername <arg>` Where `<arg>` is the database user.

`-w, --dbpassword <arg>` Where `<arg>` is the database password.

`-n, --dbname <arg>` Where `<arg>` is the database name.

`-i, --interval <arg>` Where `<arg>` is how long to search in the past (default 3 month, see interval SQL datatype for more information).

`-t, --dbtype <arg>` Where `<arg>` is the database type: ORACLE or PSQL.

Chapter

8

Request Technical Support

Technical Support from VARs

If you have purchased support from a value-added reseller (VAR), contact the VAR for technical support.

Technical Support from Genesys

If you have purchased support directly from Genesys, please contact <http://genesyslab.com/support/contact> Genesys Technical Support.