



Genesys Quality Management 8.1

**GQM Suite Administration
Reference 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_ADMIN_4-2013_8.1.511.00



Table of Contents

Chapter 1	Introduction	18
	Document Purpose	19
	Audience	19
	Document Version	19
	Typographical Conventions	20
	Expected Knowledge	20
	Browser Recommendations and Technical Requirements	21
	Internet Explorer Security Settings:	22
	Technical Requirements for Playing Audio and Video Media	23
Chapter 2	Activating Call Recording, and Displaying Licensing and Versions ...	1
	Activating Call Recording	2
	Uploading the Un-Activated Call Recording License File	4
	Activating an Un-Activated Version of Genesys Call Recording	6
	Restarting Call Recording	8
	Displaying the Version for Call Recording	9
	Displaying the License Information for Call Recording	10
	Displaying the Call Recording Status Overview	12
Chapter 3	Changing the Language, Time Zone, and Column Settings	15
	Changing the Language	16
	Changing the Time Zone	17
	Changing Which Columns Display in the Recorded Calls Tab	18
Chapter 4	Administering Groups and Users in Call Recording	19
	Groups in Call Recording	20
	Creating a New Group	21
	Assigning Privileges	23
	Limiting Group Access by Phone Numbers	25
	Limiting Group Access by Boolean Filters	26
	Editing Groups	28

	Deleting Groups	29
	Administering Users	30
	Adding Users to Groups	31
	Limiting User Access by Phone Numbers	32
	Limiting User Access by Boolean Filters	33
	Editing Users	34
	Moving Users between Groups	35
	Adding Users from LDAP	36
	Deleting Users	37
	Deleting multiple users	38
Chapter 5	Creating Recording Rules	39
	Recording Rules Overview	40
	Types of Recording Rules	42
	Rule Order	43
	Using Wild Cards for Recording Rules	44
	Identifying SIP Calls	45
	Creating a New Recording Rule	46
	Creating a Recording Rule to Record All Calls	48
	Hierarchical Recording Rules	49
	Hierarchical Recording Rules Example	50
	Hierarchical Rule Administration Example	52
	Creating a Recording Rule with External Data	53
	Adding External Data to Recording Rules	56
	Editing recording rules	57
	Deleting Recording Rules	58
Chapter 6	Configuring Call Recording Core	59
	Adding New Servers	60
	Displaying Database Pools	61
	Adding a New Pool	63
	Configuring Call Recording Core Addresses and RMI	64
	Changing the SMTP Settings	65
	Changing the Admin Email Notifications "From" Address	66
Chapter 7	Configuring Protocol Adapters and Protocol Drivers	67

	Protocol Adapters and Protocol Drivers Overview	68
	Protocols Supported By Protocol Adapters and Protocol Drivers	69
	Configuring Drivers and Readers for JTAPI Adapters	70
	Adding a New Reader	71
	Configuring JTAPI adapter	72
	Downloading JTAPI Library from CUCM (JTAPI Signaling)	74
Chapter 8	Configuring Genesys Driver for Recording	77
	Setting up Genesys Driver	78
	Setting the Operation Mode in Genesys Driver	79
	Setting up Tenant Specific Parameters	81
	Adding Tenant Information	82
	Default Tenant Configuration	83
	DN Activity Detection	84
	Configuring DN Activity Detection	86
	Configuring Notification of Recording	87
	External Data Available from CIM	89
	Setting Genesys Driver Encoding for Attached Data	90
	Basic Call-related Data	91
	Call-related User Data	94
	User data configuration	95
	Agent Configuration Data	96
	Extension Data	99
	Other Genesys Driver Data	100
	Configuring Full Agent Name Assembly	101
Chapter 9	Configuring Avaya Driver for Recording	103
	Setting up Avaya Driver	104
	Viewing and Configuring the AES Server Settings	105
	Configuring the TSAPI Interface	107
	Configuring the DMCC Interface	108
	Adding and Configuring the Recorder Groups	109
	Configuring the Recorder Settings	111
	Settings for Multi Server Installations	112
	Configuring the Terminal Activity Detection	113
	Preparing for Avaya Communication Manager	115

	Creating a TSAPI CTI User	116
	Enabling the CTI User	118
	Configuring the DMCC Port	119
	Enabling the Security Database	120
	Finding out What the Alias for the Switch Is	121
	Setting the IP Address for the H.323 Gatekeeper	122
	Finding out the Tlink Name	123
Chapter 10	Configuring Recorders	125
	Configuring Standalone Recorders	126
	Adding and Configuring Recorder Groups	127
	The API Section Recorder of Server Communicator	129
	High Availability	130
Chapter 11	Configuring Decoders	131
	Configuring Decoder1	132
	Additional Parameters for Decoder1	133
	Adding a New Decoder Server	134
	Audio Quality settings	136
	MP3 Codex Quality Settings:	137
	Changing Audio Gain Settings for the Decoder	138
	Configuring Decoder Server Communicator	139
Chapter 12	Configuring the Web UI	140
	Configuring the User Interface	141
	Configuring Database and User Interface settings	142
	Application Communicator	144
	Media Restore	145
	Core server	146
	Filter factory	147
	Recording Rules that are not listed in the recording rules tab	148
	Configuring Passwords	149
	Enabling LDAP Authentication	151
	LDAP User Account	152
	Configuring the LDAP Server Settings	153
	Configuring Group Filtering	155

	Backup LDAP Server	156
	Adding LDAP users	157
	Importing LDAP users	158
	Setting up Advanced Searches	161
	Creating an Advanced Search with External Data	163
	Customizing Columns Setup	168
Chapter 13	Installing Screen Capture	170
	Screen Capture Server Components	171
	Screen Capture Client	172
	Service Slave Mode	173
	Capture Client Installation	174
	Standalone Mode	178
	Capture Client Security	179
	Capture Client Hostname Configuration	180
	Capture Client Logs	181
	Setting the Level of Logging	182
Chapter 14	Configuring Screen Capture in the Call Recording Settings	184
	Pre-requisites for Configuring Screen Capture in the Call Recording GUI ..	185
	Configuring MasterScreen Capture	186
	Configuring the Resolver	187
	Configuring the Registry address	188
	Configuring the Output File and Uploader Settings	189
	Configuring the Uploader Settings	191
	Configuring the Recording Specifications	192
	Recording Specifications (Advanced)	194
	Configuring the Uploader global settings	195
	Pairing Screen Capture Agents to Their Desktops	196
	Option 1 - XML Resolver	197
	Option 2 - Agent ID Resolver	198
	Option 3 – Property Resolver	199
	Option 4 – IP to IP Resolver	200
	Screen Capture Communicator Settings	201
	Configuring the Media Encoder	203
	Database Setting	204

	Application Communicator	205
	Mixer Task Settings	206
	Encoder Settings	207
	Configuring a Custom Temporary Directory for the Media Encoder	209
Chapter 15	Screen Capture High Availability Options	210
	Java Standalone Thin Client	212
	.NET Standalone Thin Client	213
	Screen Capture Port Usage Guide	214
Chapter 16	Configuring CUCM Prerecording	216
	Prerecording Overview	217
	Configuring Prerecording in CUCM 5 and higher	218
	Adding the Prerecording Service	219
	Making Prerecording Available for Users for CUCM 5 and Higher	221
	Configuring Prerecording in CUCM 4	224
	Adding the Prerecording Service in CUCM 4.3	225
	Making Prerecording Available for Users in CUCM 4.3	228
	Configuring Prerecording in Genesys Call Recording	230
	Setting the Call Wait Timeout	231
	Enabling the Send by Email Option for Record Status	232
	Enabling the Send by Email Option for Prerecording Status	233
	Configuring the Application Communicator	234
	Configuring the External Data Feature	235
Chapter 17	Recording CUCM in SRST Mode	236
Chapter 18	Connecting to two Independent CUCM Clusters	240
	Preventing Call Recording from Restarting New Installations	241
	Stopping Call Recording Existing Installations	242
	Creating an additional JTAPI Adaptor	243
Chapter 19	Integrating Genesys CIM with GQM Using GIM	248
	Genesys Passive Recording	249
	Installing the Genesys Integration Module	250
	External Data Available from Genesys CIM for GIM	251

	Setting GIM Encoding for Attached Data	252
	Configuring the Integration Module	253
	Configuring the Application Names and Address for GIM	254
	Configuring the T-Server and Configuration Server for GIM	255
	Configuring the DN Range for Attached Data	257
	Configuring Notification of Recording for GIM	259
Chapter 20	Setting up Media Lifecycle Maintenance	262
	Managing the Media Lifecycle	264
	Media Lifecycle Management Tools	265
	Activating Changes, and Enabling Tools	266
	Activating Tool Configuration Changes	267
	Enabling Tools	268
	Running Tasks	269
	Starting the Tools Manually One-shot	270
	Restarting a Tool to Run Continually	271
	Troubleshooting	272
	Configuring Application Communicator	273
	Archiving	274
	Configuring Media Archive	275
	Adding an Archive Task	277
	Selecting an Archive	279
	Starting the Archive Tool Manually One-shot	281
	Restarting the Archive to Run Continually	282
	Archiving and Deleting	283
	Activating Deletion	284
	Viewing Results	285
	Configuring Backup	286
	Creating a Backup Task	287
	Starting the Backup Tool Manually One-shot	288
	Starting the Backup Tool Manually Continually Using Cron	289
	Viewing Results	290
	Configuring Restore	291
	Configuring Requests	293
	Starting the RestoreTool Manually	294
	Viewing the archived files	295

Restored calls	296
Setting the Expiration Time	297
Notifying Admin of a Restore Request	298
Synchro	299
Configuring the Replay Server Synchro Settings	300
Adding a New Source	302
Setting up the Target	304
Target Parameters:	305
Restarting the Synchro Tool	306
Configuring Delete	307
Configuring Delete Calls, Delete Recorded Screens, Delete Screens in Recd Format, and Delete Index Files	308
Delete Database Records	309
Starting the Delete Tool Manually One-shot	311
Restarting the Delete Tool to Run Continually	312
Configuring Media Relocation	313
Restarting the Relocation Tool	315
Configuring the Disk Space Monitor	316
Viewing Disk Usage in the Disk Space Monitor	318
Custom Triggers	319
Alternative Source Paths	320
Alternative Target Paths	321
Time Specification	322

Chapter 21	PCI DSS Compliance	324
	PCI DSS Compliance Overview	325
	GQM PCI Compliance Checklist	327
	Vendor-supplied Default Passwords Are Not Used	330
	Pause/Resume Functionality Is Enabled	331
	Key Manager Is Active and Keys Are Valid for no Longer than 12 Months ..	332
	Self-Signed or Commercial Certificates	333
	Key Manager in Cluster Installations	334
	Activating Key Manager	335
	Enabling Encryption in Client Setup	336
	Installing Commercially Signed Certificates	337
	Installing Commercial Certificates for Key Manager	338

	Create keys directory, private keys and certificate request files	338
	Obtain Signed Certificates	340
	Install signed certificates and create encryption/decryption certificates ..	341
	Troubleshooting Key Errors	343
	Configuring Key Manager	345
	Server Setup	345
	Client Setup	346
	Audio Files Are Encrypted	348
	Video Files Are Encrypted	349
	Web Access Is Encrypted	350
	Audit Logs Are Collected	351
	Password Management Is Enforced	352
	Brute-force protection is enforced	353
	Data Retention Policies Are Enforced	354
	Archive Tool	355
	Delete Tool	356
	Encrypt Tool	357
	Parameters	358
	Examples:	359
	Switching On Debug Logs	360
	Password Storage in GQM	361
Chapter 22	Secure Web Access for PCI-DSS Compliance	362
	Component Compatibility	363
	Configuration	364
	Creating the Key and Certificate	365
	Obtaining a Commercially Signed Certificate	366
	Creating a Self-signed Certificate	367
	Converting the Certificate	368
	Configuring Tomcat	369
	Restarting the Call Recording Web Service	370
	Adding the Localhost Certificate to the Java CA Certificates	371
	Adding the Port Redirect to the IP Tables	372
	Configuring the Quality Manager Stream URL Setting	373
	Secure LDAP	374
	Install SSL Certificates	375

	Enable LDAPs in the Call Recording Web GUI	376
	GQM Port Usage Guide	377
Chapter 23	Activating Quality Manager	380
	Activating Quality Manager	381
	Open Quality Manager in a Web Browser	382
	Log In as Administrator	383
	Uploading the Un-activated Quality Manager License File	384
	The Activation Key	385
	Uploading the Activated Quality Manager License File	386
	Log Out, Refresh Page, Log In as CC Manager	387
	Logged In as ccmanager	389
	Default Quality Manager Users	390
Chapter 24	Configuring Quality Manager	392
	Configuring Quality Manager in the Call Recording GUI	393
	Basic Settings	394
	Rounding Strategy	396
	Scheduled Actions	397
	Quality Manager Integrations	398
Chapter 25	Synchronizing Quality Manager with a Genesys Configuration	
Server		400
	Genesys Importer Features	401
	Preparation for Importing	402
	Importing Agent Groups and Related Users	405
	Importing Virtual Agent Groups	406
	Advanced Filtering by Annex Value	407
	Specify Agent Group Supervisors by specific Annex value	408
	Authentication against Genesys Configuration Manager	410
	Quality Manager Genesys Configuration	411
	User Synchronization Option	415
	Scheduling Genesys Synchronization	416
	Web-based Configuration	417
	Assigning the agent Identification for Genesys Importer Using the "Agent property to match the AgentID in recorded calls" Field	419

	Configuration at the Command Line	420
	Integration Data Definition	422
Chapter 26	Setting Up Data Export from Quality Manager	424
	Customizing the Report Template Spreadsheet	425
	Integrating the Quality Manager Database with Excel	428
	Setup Instructions	429
	Create a Read-only Database User	429
	Set up the ODBC Source	430
	Import the ODC Files	433
	Modifying ODC SQL Queries	436
Chapter 27	Live Monitor	438
	Configuring Live Monitor in Call Recording	439
	Adding External Data Fields	441
	Restricting Calls in Live Monitor	443
	NAT and Firewall Settings with Live Monitor	444
Chapter 28	Viewing and Sending Call Recording Logs	446
	Viewing Logs	447
	Important Log Files	448
	Sending Logs to Genesys	449
	Sending the Logs as an Email Attachment	450
	Sending the Logs with the bugreportScript :	451
	DEBUG Mode	452
	Switching Between log4j and Debug Modes	453
	Logs advanced modifications	454
	Changing the Log Page Size	455
	Adding Logs to the User Interface	456
	Log File Output Example	458
Chapter 29	Generating and Using Call Recording Reports	460
	Generating a Report	461
	Report Type	463
	Report Results Setting	464
	Setting Up Periodical Reports with Quick Filter	465

	Report Results	466
	Time Range Setup for Selected Parameters	469
	Bad Calls Report	470
	Not Decoded Calls Report	471
	Transfers	472
Chapter 30	SNMP	474
	Structure of the Call Recording SNMP MIB	475
	Configuring the SNMP Agent for Oracle	477
	Testing SNMP Functionality	480
	Backing Up Call Recording	482
	Compatible Backup Agents	483
	Target components	484
	Back up calls	484
	Back up the database	484
	Back up Call Recording configuration	484
	Genesys Backup Scripts	485
	Download	485
	Configuration	485
	Implementation	485
Chapter 32	Using Oracle	488
	Overview	489
	Supported Oracle Versions	490
	Pre-install Tasks	491
	Installation and Setup	493
	Run Standard Installer and Setup	494
	Set System Variables	497
	Install the Database Schema	498
	Update Oracle Schema	500
	Start Call Recording	501
	Troubleshooting Database Parameters	502
Chapter 33	Database Migration to Oracle	504
	Deployment and Migration Scenarios	505
	Call Recording Only (Existing version: 8.0.46x - 8.0.47x)	506

	Call Recording (8.0.46x – 8.1.5x) + Quality Manager	507
	Migration Requirements	508
	Migration Overview	509
	Call Recording Database Migration from PostgreSQL to Oracle	510
	Call Recording Database Migration from Oracle to PostgreSQL	511
	Quality Manager Database Migration from PostgreSQL to Oracle	512
	Quality Manager Database Migration from Oracle to PostgreSQL	513
	Call Recording Migration	514
	Source Database Pool	515
	Target Database Pool	516
	Source and Target Assignment	517
	Export Node	517
	Import Node	517
	Run the Migration Script	519
	Sample (minimal)	521
	Quality Manager Migration	522
	Source Database Pool	523
	Target Database Pool	524
	Source and Target Assignment	525
	Run the Migration Script	527
Chapter 34	Oracle Mapping and Maintenance	530
	Database Pool Mapping	531
	Call Recording Web GUI	532
	XML Configuration Files	533
	Removing the Database Schema	534
	Additional Reference	536
Chapter 35	Using GQM Virtual Appliances	538
	Virtual Appliance Overview	539
	Prerequisites	540
	Default configuration	541
	Installing VMWare Tools on a Virtual Server	542
	Starting the Installation Process	543
	Checking that the CD/DVD is Connected:	545
	Installing the VMware tools.	547

Importing the Virtual Appliance	548
Reading and Accepting the EULA	557
Restarting CallREC	558
Restarting the Server	560
Shutting down the Server	561
Configuring the Network	562
Configuring the Time Zone	564
Logging In	565
Mounting Storage for Calls for the VM Appliance	566
Mounting and formatting a partition in QM Suite Virtual Appliance	567
Converting a Virtual Appliance to VMware Workstation or VMware Server	573
Using More than One CPU in the VA	574

Chapter 36	Command Line Scripts	576
	Starting and stopping Call Recording	577
	Starting Call Recording	578
	Stopping Call Recording	579
	Restarting Call Recording	580
	Automatic running	581
	Reloading the Configuration manager	582
	Checking the Status of Call Recording	583
	Restarting and Shutting Down the Server	585
	Restarting the Decoder	586
	Restarting Call Recording Core	587
	Restarting the Call Recording System	588
	Restarting other Call Recording Components	589
	Restarting Clustered Servers	591
	Restarting Redundant Servers	592
	Restoring the Default Configuration	593
	Using Symlinks to the Call Recording PCAP Storage Directory	594
	Important Note on Synchronization	595
	Mounting Windows File Shares	597
	Troubleshooting Tips	599
	Advanced Configuration Parameters	600
	Active Recorder (SLR) Configuration Parameters	601
	Notes on Parameters	602

	Limit on the Maximum Number of Threads	603
Chapter 37	Additional Call Recording Scripts	604
	bugreport	605
	call2mp3	607
	callrec_status	608
	repaircalls	610
	selectivebackup	612
	status.pl	616
	tools	617
	gen_cfgtest	618
	Additional Scripts	619
Chapter 38	AMQP Implementation	620
	Resources Required for RabbitMQ	621
	AMQP Queues in Call Recording	622
	Listing All Available Queues	623
	The Decoding Process	624
	Repair Call Process	626
	Media Removal Process	627
	RabbitMQ configuration	628
	RabbitMQ As a Dedicated AMQP Server	629
	Changing the AMQP Server via the Call Recording UI	630
	Changing Where RabbitMQ Stores the Content of the Queues Clean installation	631
	Changing Where RabbitMQ Stores the Content of the Queues Running installation	632
	Changing the AMQP Server Settings via the configuration file	633
	Troubleshooting AMQP	634
	Typical Issues with Decoding performance	637
	Typical Issues with Available Disk Space	639
Chapter 39	Known Issues	640
	Incorrect Handling of Hunt Lists in CUCM versions older than 8.0	641
Chapter 40	Request Technical Support	642

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 administration, configuration, and maintenance of GQM.

Audience

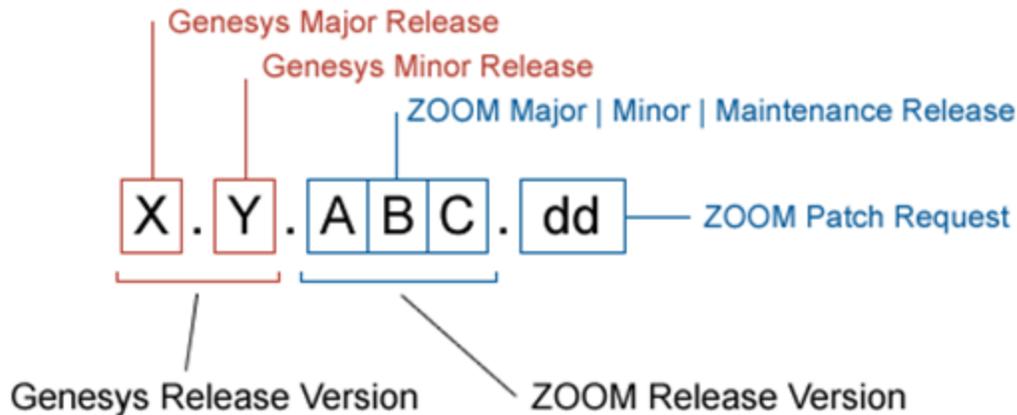
This document is intended for system engineers, programmers and administrators responsible for integration of the Genesys GQM with other existing third party applications.

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:

Genesys Quality Management Document Versioning 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 Genesys Call Recording system features and functionality
- 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

Activating Call Recording, and Displaying Licensing and Versions

This chapter describes how to activate Call Recording, and how to view the product license and version information.

This chapter contains the following sections:

[Activating Call Recording](#)

[Displaying the Version for Call Recording](#)

[Displaying the License Information for Call Recording](#)

[Displaying the Call Recording Status Overview](#)

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:

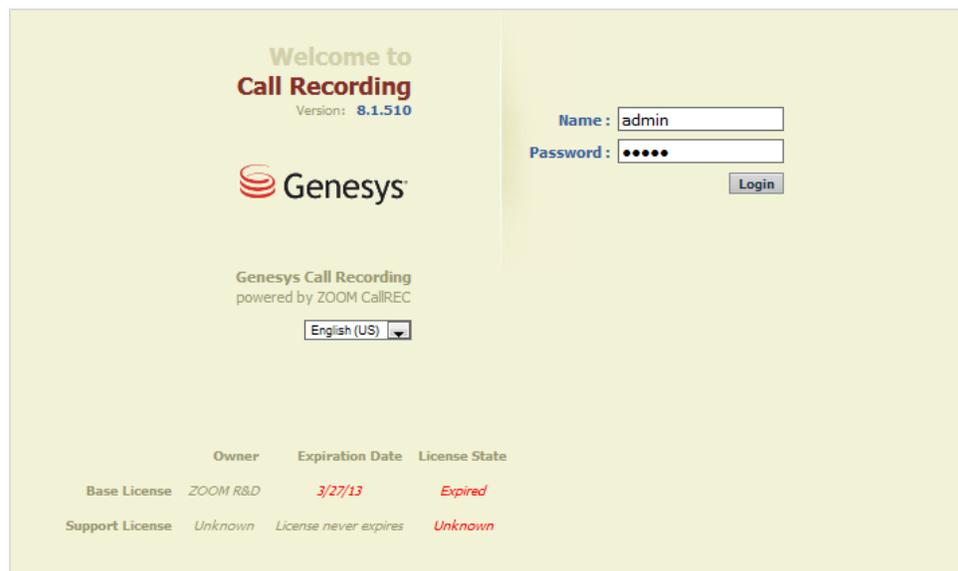


Figure 1: Log in for Activation

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 2: License Details

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

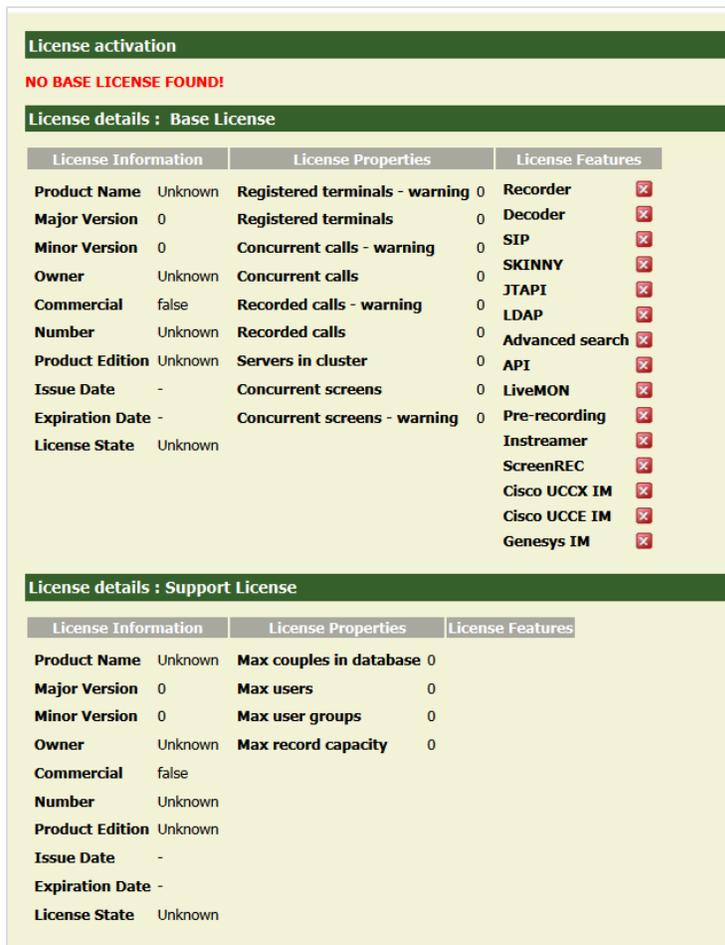


Figure 3: No Base License Found

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 4: 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**.

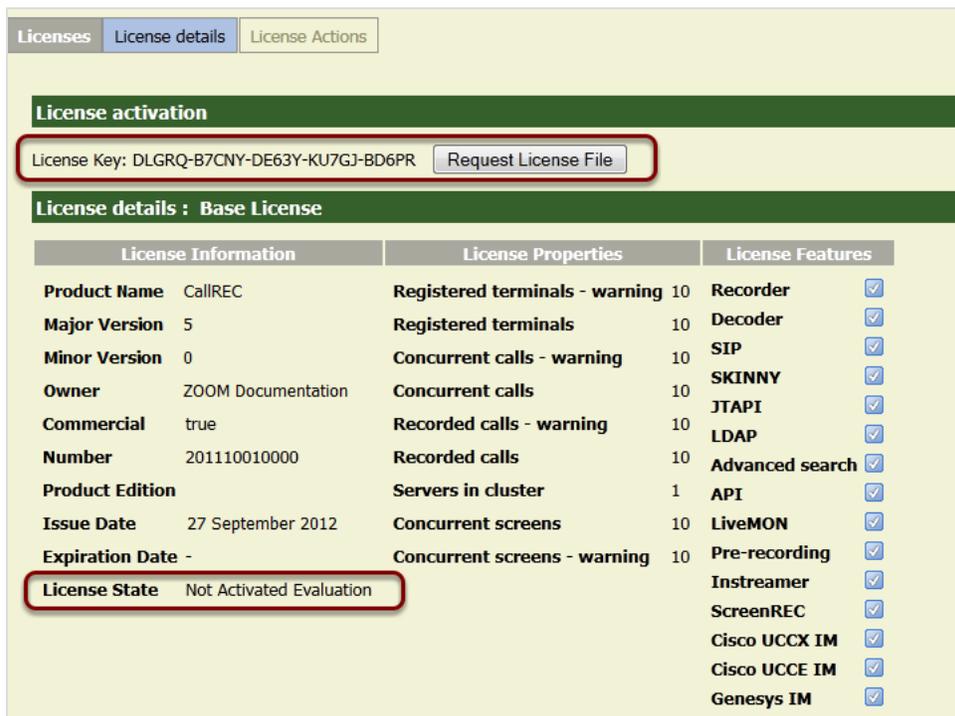


Figure 5: Un-Activated License

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.

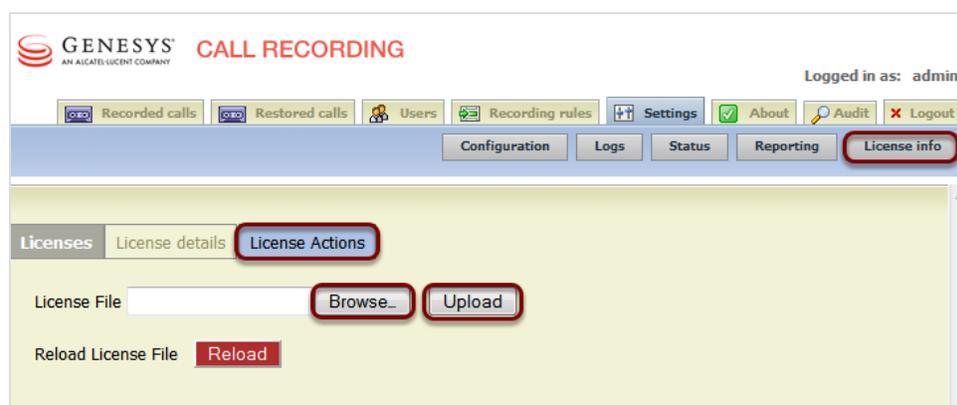


Figure 6: License Actions Dialog

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		Recorded calls	100	Advanced search	<input checked="" type="checkbox"/>
Issue Date	September 27, 2012	Servers in cluster	10	API	<input checked="" type="checkbox"/>
Expiration Date	December 31, 2013	Concurrent screens	100	LiveMON	<input checked="" type="checkbox"/>
		Concurrent screens - warning	100	Pre-recording	<input checked="" type="checkbox"/>
License State	OK			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 7: 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.

Displaying the Version for Call Recording

The Genesys Call Recording **About** tab displays the version of all the currently installed components that Call Recording needs to run.

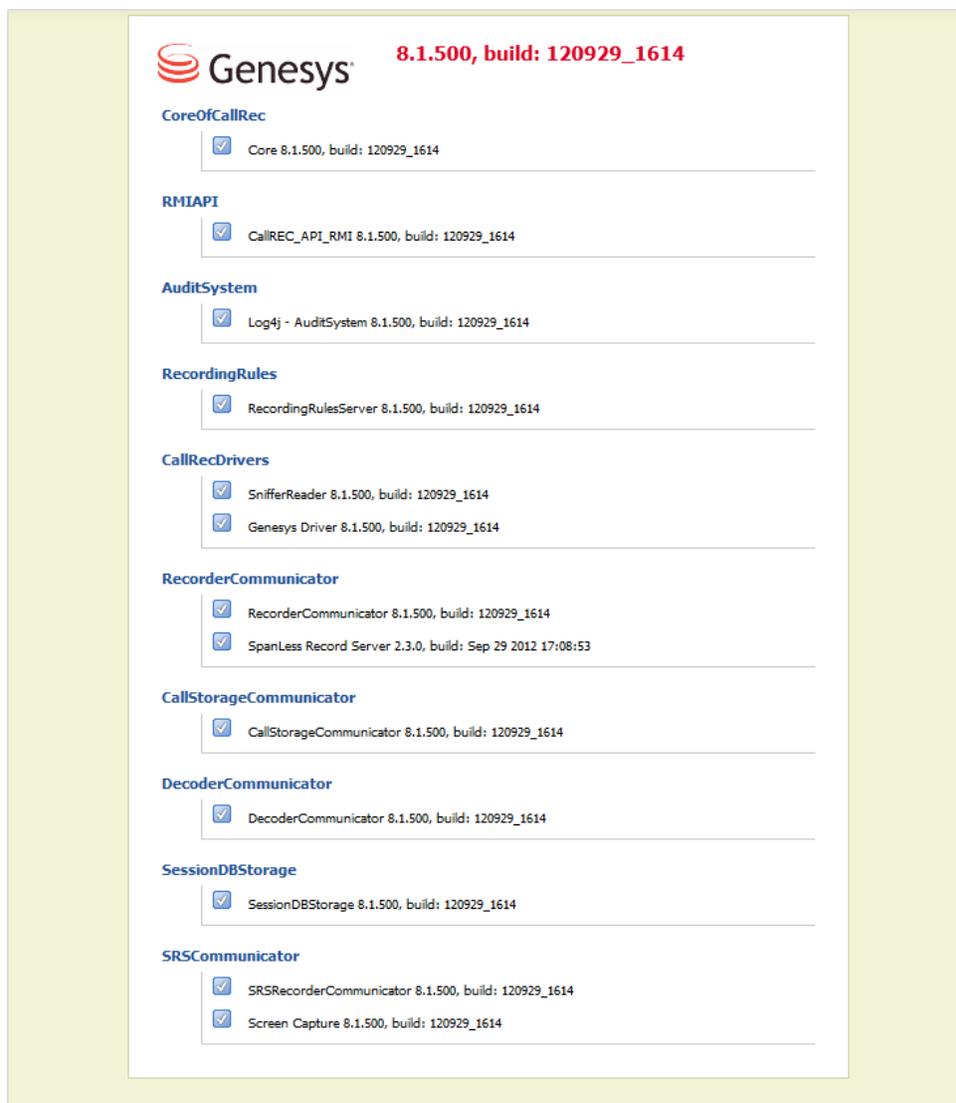


Figure 8: About Call Recording - Showing Current Call Recording Version and Version of Components

The information on the **About** tab is useful when contacting Genesys Support.

Displaying the License Information for Call Recording

To access the license information, navigate to **Settings > License info.**

Licenses
License details
License Actions

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 1000	Recorder <input checked="" type="checkbox"/>
Major Version 5	Registered terminals 1000	Decoder <input checked="" type="checkbox"/>
Minor Version 1	Concurrent calls - warning 1000	SIP <input checked="" type="checkbox"/>
Owner ZOOM R&D	Concurrent calls 1000	SKINNY <input checked="" type="checkbox"/>
Commercial false	Recorded calls - warning 1000	JTAPI <input checked="" type="checkbox"/>
Number 20130103000	Recorded calls 1000	LDAP <input checked="" type="checkbox"/>
Product Edition	Servers in cluster 10	Advanced search <input checked="" type="checkbox"/>
Issue Date January 3, 2013	Concurrent screens 1000	API <input checked="" type="checkbox"/>
Expiration Date December 31, 2013	Concurrent screens - warning 1000	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"/>

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 -		

Figure 9: Example of License Info Screen from Fully Activated Call Recording 8.1.5x

To upgrade an existing license, contact Genesys Labs, Inc. at:
<http://genesyslab.com/support/contact>.

Displaying the Call Recording Status Overview

The **Status overview** page summarizes all SNMP information with records of current and historical values. Status reports are divided into groups according to the services that generate status reports.

Navigate to **Settings > Status**. The **Status overview** displays.

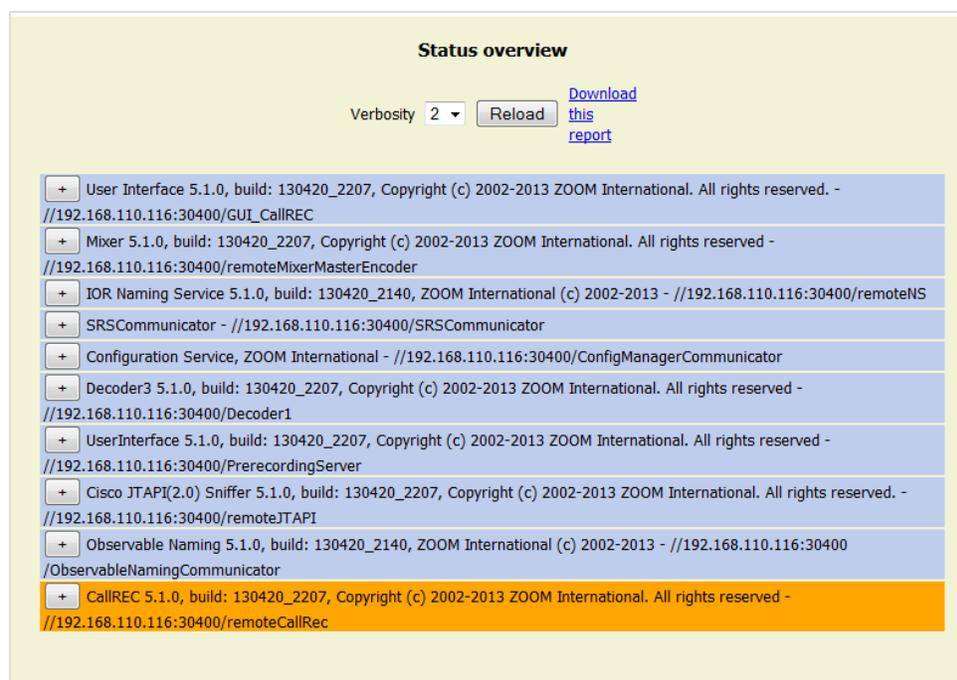


Figure 10: Example of Status Report

1. Select the required **Verbosity**, level of detail, from the drop-down list. Select a verbosity of 1 for the least amount of detail and select 5 for the most detail.
2. Click **Reload** to apply the **Verbosity** level.

The **Status overview** shows the current status of each module with color codes to warn about potential problems:

- a blue row indicates that the particular module functions within defined parameters.

- an orange row indicates a warning that the particular module is not operating within defined parameters, or there is an issue that requires attention. Call Recording continues to operate.
 - a red row indicates a failure. The system is NOT operating within defined parameters and at least one value has not returned or has returned with **FAILED** status. Correct this parameter, and adjust it or fix it as required.
3. Click + on that row to expand the view for that module and display the details. Click - to collapse the list.

Chapter

3

Changing the Language, Time Zone, and Column Settings

This chapter describes how to change the settings in the user interface.

This chapter contains the following sections:

[Changing the Language](#)

[Changing the Time Zone](#)

[Changing Which Columns Display in the Recorded Calls Tab](#)

Changing the Language

To change the default Call Recording language for the main application, log in to Call Recording.

Navigate to **Settings > Configuration > User Setup > Personal Setup**.

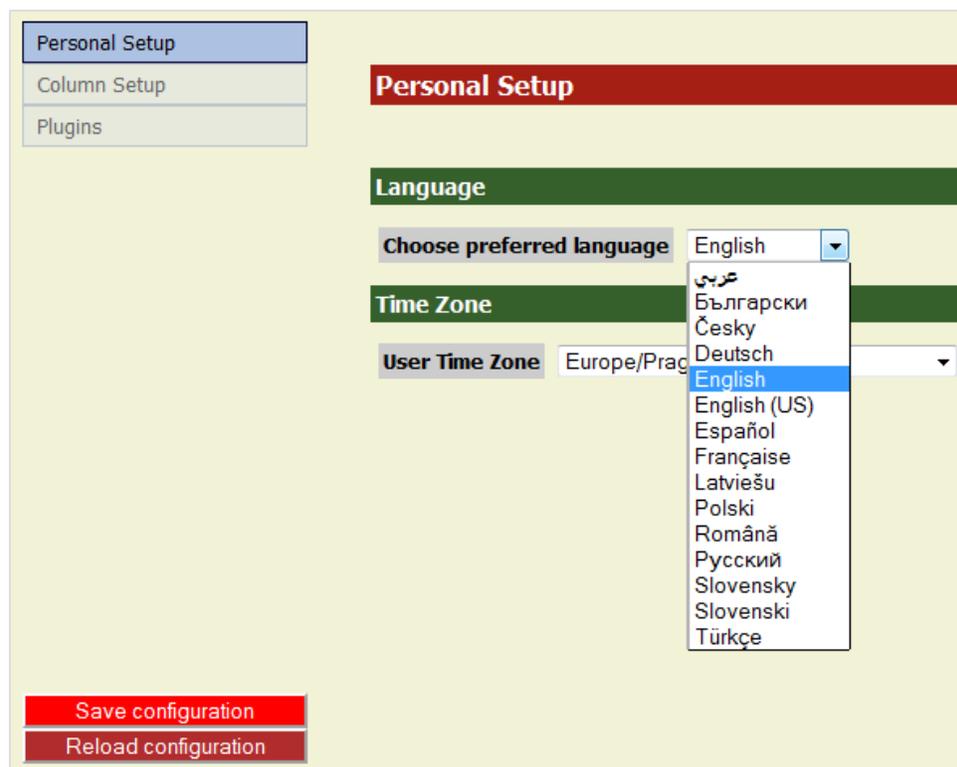


Figure 11: Changing the Default Language

1. Select the language from the **Choose preferred language** drop-down list.
2. Click **Save configuration**.

Click on another tab in Call Recording to refresh the web page, or click **Refresh** in the web browser.

The labels in Call Recording display in the language selected. Some user interface elements may not change language because of naming restrictions and integration with other systems

Login screen language selection is separate and only controls the login page.

Changing the Time Zone

The **Time Zone** setting affects all dates and times that display in the Call Recording Web UI when logged in with the user profile. The only exceptions are dates and times used for **Recording rules**, that are always set to the server time.

To change the default Call Recording Web UI time zone for the user profile:

Navigate to **Settings > Configuration > User Setup > Personal Setup**.

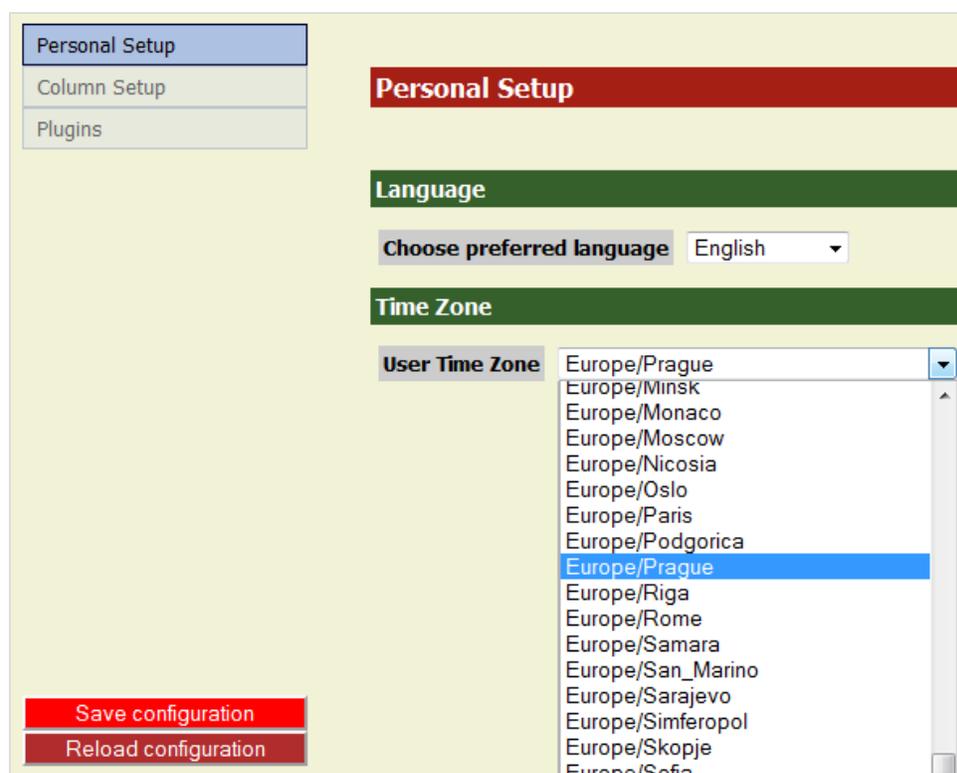


Figure 12: Changing the Default Time Zone

1. Select the time zone from the **User Time Zone** drop-down list.
2. Click **Save configuration**.

Click on another tab in Call Recording to refresh the web page, or click **Refresh** in the web browser.

Changing Which Columns Display in the Recorded Calls Tab

The **Recorded calls** tab contains call information to help the user select calls to play. Add or subtract columns to control how much information displays. These selections only affect the users own view of listed calls.

The number and type of columns available for selection depends on the system configuration, and is set by the system administrator.

Navigate to **Settings > Configuration > User Setup > Columns setup**.

Personal Setup
Column Setup
Plugins

Columns Global Setup

Setup rights

Settings below will affect column view if this checkbox is checked

Basic columns

Column name	Visible	Description
Date	<input checked="" type="checkbox"/>	
Call start time	<input checked="" type="checkbox"/>	
Call end time	<input type="checkbox"/>	
Length of call	<input type="checkbox"/>	
Calling number	<input checked="" type="checkbox"/>	
Called number	<input checked="" type="checkbox"/>	
Description	<input checked="" type="checkbox"/>	

LiveMON columns

Column name	Visible	Description
Duration	<input checked="" type="checkbox"/>	
Calling number	<input checked="" type="checkbox"/>	
Called number	<input checked="" type="checkbox"/>	

Save configuration
Reload configuration

Figure 13: User's Setup - Columns

1. Select the columns to display in the **Recorded calls** tab.
2. Click **Save configuration**.

The columns display in the **Recorded calls** tab.

Chapter

4

Administering Groups and Users in Call Recording

This chapter describes how to administer groups and users.

This chapter contains the following sections:

[Groups in Call Recording](#)

[Administering Users](#)

Groups in Call Recording

Call Recording uses groups to grant system access privileges, and determine recording and filtering rules. Individual users are assigned to a group, and inherit the group's access privileges and rules.

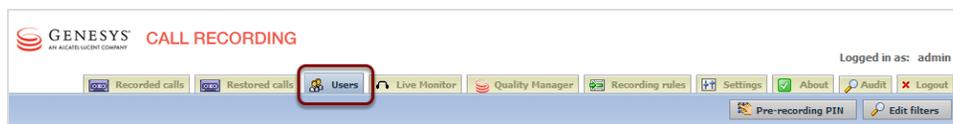


Figure 14: The Users Tab

To configure these privileges and rules click **Users**.

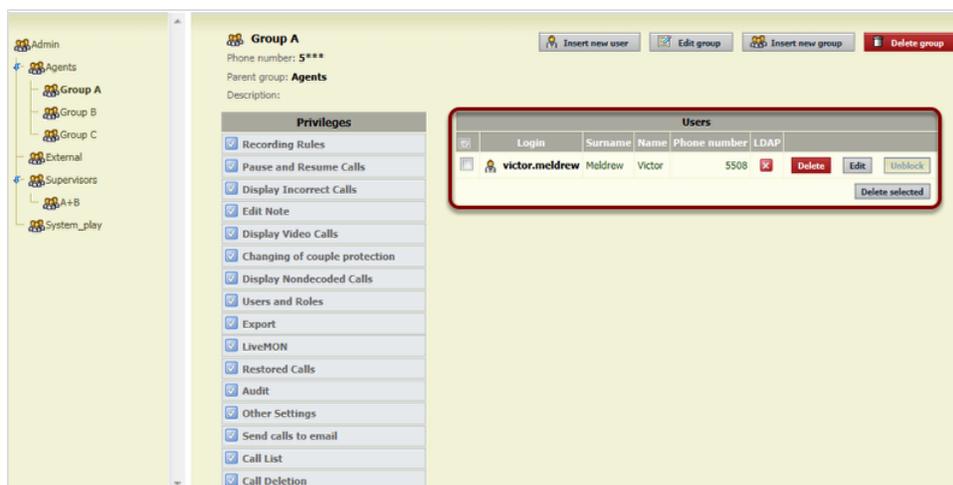


Figure 15: Tree View of Groups, Users, and Access Rights

The group with the most complete set of access rights is always called **Admin**. All the other groups are subordinate to **Admin**. Users in the **Admin** group inherit all access rights, including setting recording rules and filters.

1. The figure shows the full list of privileges. Any changes in a group's rights are reflected for all sub-groups and users assigned to that group. A subordinate group cannot have more **Privileges** than the parent group.
2. The tree view of groups. Set up unlimited groups and users, each using its own recording rules and filters. This controls which calls are recorded and who has access to those calls.
3. The figure shows that **Group A** only has one user presently with a full set of privileges.

Creating a New Group

To create a new group, navigate to **Users > Insert new group**.



Figure 16: Creating a New Group

The **Add new group** form displays.

Figure 17: Adding a New Group

1. Type the group **Name**:
2. Type the group **Phone number**: The phone number can be a mask that indicates a range of numbers. Wild cards are valid. To include all numbers beginning with 6, type **6***. GQM supports alphanumeric characters for extensions, DNs or terminals. To include all numbers in the system, that is, to use the settings of the parent group with no filter applied, use the wildcard ***** or leave the field blank.
3. Select the **Parent group**: from the drop-down list.
4. Type a **Description**: of the group.

5. Select **Privileges:** for the group. These privileges cannot be greater than the rights of the parent group.
6. Select multiple pre-existing filters, and combine the filters with Boolean operators to restrict how call recordings display for the group.
7. Click **Insert new group** to save the new group.

The new group displays in the tree list of groups. Add users to this group.

Assigning Privileges

Privileges are inherited by all members of the group and any subgroups.

Privilege	Definition
Recording Rules	Add, and Edit recording rules.
Pause and Resume calls	Pause and Resume calls.
Display Incorrect calls	Display calls that are not recorded correctly, for example, calls that contain signaling data for the call but no audio recording. Recommended only for system administrators.
Edit Note	Add, and Edit call notes with the ability to add comments to call data records.
Display Video Calls	Enables viewing of Screen Capture recordings.
Changing of couple protection	Ability to remove protection from, for example, couples that can not be deleted.
Display Nondecoded calls	Displays calls which are not yet decoded and calls waiting to be decoded from the original format , PCAP, to the final format. MP3 or WAV.
Users and Roles	Ability to administer groups, users and access rights.
Export	Ability to export recordings in selected audio format.
Live Monitor	Access to live call monitoring.
Restored calls	Access to restored recordings from backup and archive.
Audit	Access to audit information, for example, logs .
Other settings	Access to system and configuration

Privilege	Definition
	settings. Recommended only for system administrators.
Send calls to email	Ability for the user to send call recordings to specified email addresses.
Call list	Ability to play recordings. Disabling this option also disables Edit note, Export and Call deletion.
Call deletion	Ability to delete recordings.

Table 1: External Data for Recording Rules

Limiting Group Access by Phone Numbers

Users inherit access rights from their group. Specify a phone number filter for the group to restrict access rights further. This can be a single phone number, for example 2435, or a range of numbers, for example, 24??. Wild cards are valid.

These settings also apply to the calls that display in Live Monitor.

Limiting Group Access by Boolean Filters

Navigate to **Users**.

Boolean operators combine several pre-existing filters together and display only the results to the members of the group. The tree list contains groups, users, and access rights.

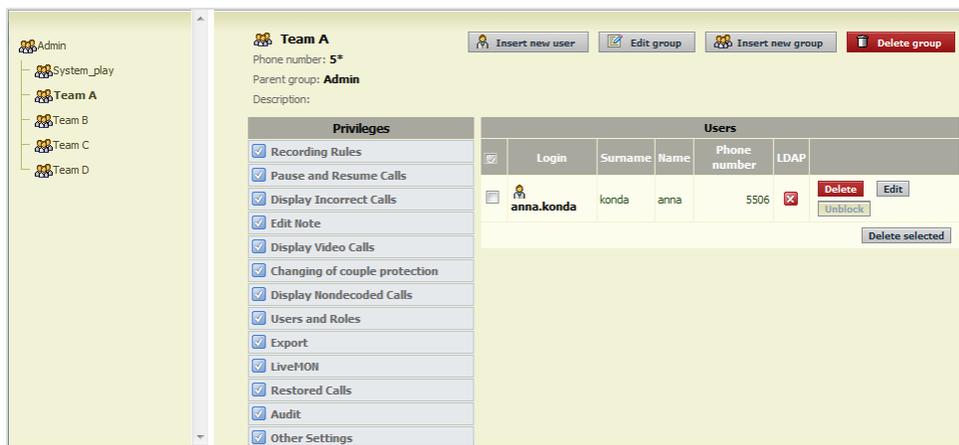


Figure 18: Edit Group

1. Select a group from the tree list of groups, on the left hand side of the screen.
2. Click **Edit group**. The **Edit group** form displays.

Figure 19: Edit Group Form

1. Choose a filter from the **Choose filter:** drop-down list.
2. If this is the only filter needed then select **END**. To use more than one filter, select a **AND** or **OR** to link the next filter. Using **AND** the group only views calls that satisfy both filters, using **OR** the group views all the calls from the first filter and all the calls from the second filter.
3. The **AND** or **OR** option displays an extra **Choose filter:** drop down . Choose additional filters, and connect them with operators to define the filter. The final Boolean operator must always be **END** to complete the filter definition.
4. Click **Save**.

The filter applies to all members of the group and its subgroups.

Users may also apply filters to their individual view of recorded calls. The group filters apply first, and then the user filters. The result is that the viewer views a restricted set of recorded calls.

To apply a filter using SIP, define the mask for the whole SIP number. For example, 12345@*.

These settings do not apply to the list of calls displayed in Live Monitor. It only affects the list of calls that display in the **Recorded calls** list.

Editing Groups

Navigate to **Users > Edit Group**.

The screenshot shows the 'Edit group' interface for 'Team A'. The form includes the following fields and sections:

- Name:** Team A
- Parent group:** Admin
- Phone number:** 5*
- Description:** (Empty text area)
- Privileges:** A list of 15 checked items: Recording Rules, Pause and Resume Calls, Display Incorrect Calls, Edit Note, Display Video Calls, Changing of couple protection, Display Nondecoded Calls, Users and Roles, Export, LiveMON, Restored Calls, Audit, Other Settings, Send calls to email, Call List, and Call Deletion.
- Choose filter:** DavidLuiz (admin) OR Filter115 (admin) END
- Buttons:** Save (highlighted with a red circle) and Cancel

Figure 20: Group Editing

1. Select or deselect **Privileges**.
2. Change the **Phone number**: range.
3. Click **Save**.

The changes are saved and inherited by all members of the group and any of its subgroups.

Deleting Groups

Navigate to **Users**.

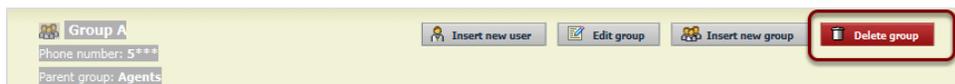


Figure 21: Group Deletion

Select a group from the tree list of groups on the left hand side of the screen.

1. Click **Delete group**.
2. Click **OK** to confirm deletion of the group.

The group and all its members are deleted from the system. If a user has created a filter that is in use, then the user who created the filter cannot be deleted.

Important:

If a group is deleted, then all its members and recording rules are also deleted and cannot be restored. Do not delete the group **System_play** because this group provides access for Quality Manager to play calls.

Administering Users

Agents do not need to be users to be recorded. Only create user profiles for staff that actively use Call Recording to listen to calls as a minimum. Users can only be created within groups and inherit the privileges and filters assigned to the group. Assign additional filters to the users, further restricting their access to recorded calls.

Users can be assigned to a different group, edited, or deleted. Users can change their own password. Administrators and supervisors can also edit user passwords.

Adding Users to Groups

Navigate to **Users**.

Open a group from the tree list of groups on the left hand side of the screen, and then create users to fill the group. Users inherit the rights of their group.

Click **Insert new user**. The **Add new user:** form displays.

Figure 22: Window for Adding a New User

1. Type the username in the **Login:** field.
2. Type the user's password in the **Password:** field. Confirm the user's password in the **Password confirmation:** field.
3. Type the user name, surname, email, and phone number in the **Name:**, **Surname:**, **E-mail:**, and **Phone Number:** fields. If the phone number field is blank, the user inherits the group phone number. GQM supports alphanumeric characters for extensions, DNs or terminals.
4. Choose filters assigned to this user. Add Boolean operators **AND**, **OR**, or **END** to connect multiple filters. The last operator must always be **END**.
5. If the user is found in the LDAP and Call Recording is configured to access the LDAP, then the LDAP user checkbox is selected. Otherwise, leave this blank.
6. Click **Insert new user** to add the user to the group.

The user is now a member of the group and inherits all its privileges, recording rules, and filters.

Limiting User Access by Phone Numbers

Users inherit access rights from their group. The user can further restrict access rights by specifying a phone number filter for the user. This can be a single phone number, or a range of numbers. Wild cards are valid. This affects the list of calls in **Recorded calls**.

These settings also apply to the calls that display in Live Monitor.

Limiting User Access by Boolean Filters

Navigate to **Users**.

Users inherit group access rights and filters. Add additional filters to a user, further limiting access. Set and save filters, and then apply the filters to individual users. Restrict user access to a very specific level, by combining these pre-existing filters with Boolean operators.

1. Choose a filter from the drop-down list.
2. Select a Boolean operator.
3. Choose additional filters, this connects them with operators to define the filter.
4. Click **Save**.

The user only has access to the calls enabled by the filters.

The group filters apply first, and then the user filters. The result is that the user sees only a highly restricted set of recorded calls.

To apply a filter using SIP numbers, define the mask for the whole SIP number. For example, 12345@*.

These settings do not apply to the list of calls that display in Live Monitor. It only affects the list of calls that display in the **Recorded calls** list.

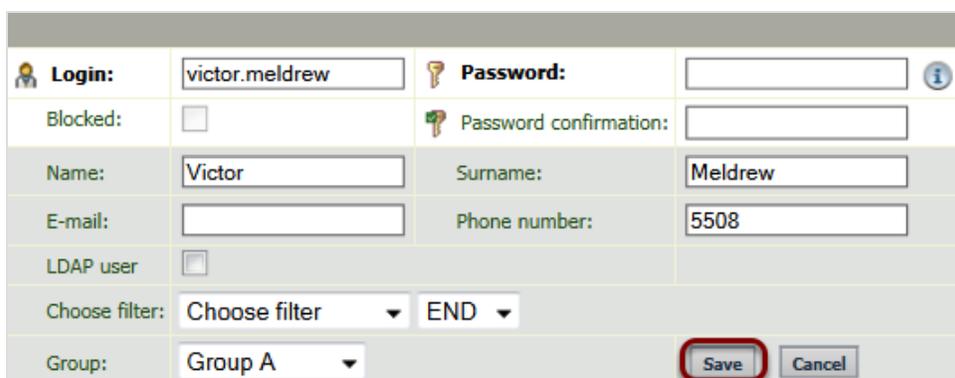
Editing Users

Navigate to **Users**.

Administrators, supervisors, and users can change user information, depending on access permissions.

Open the user's group from the tree list on the left hand side of the screen. A list of users displays.

Find the user in the list, and click **Edit**.



 Login:	<input type="text" value="victor.meldrew"/>	 Password:	<input type="password"/>	
Blocked:	<input type="checkbox"/>	 Password confirmation:	<input type="password"/>	
Name:	<input type="text" value="Victor"/>	Surname:	<input type="text" value="Meldrew"/>	
E-mail:	<input type="text"/>	Phone number:	<input type="text" value="5508"/>	
LDAP user	<input type="checkbox"/>			
Choose filter:	<input type="text" value="Choose filter"/>	<input type="text" value="END"/>		
Group:	<input type="text" value="Group A"/>	<input type="button" value="Save"/>	<input type="button" value="Cancel"/>	

Figure 23: Editing a user

1. Make changes as required.
2. Click **Save**. The changes apply to the user immediately.

Moving Users between Groups

Navigate to **Users**.

To move a user to another group:

1. Open the group that the user is a part of in the tree list on the left hand side of the screen.
2. Find the user in the list, and click **Edit**.
3. Choose a group from the **Group:** drop-down list.
4. Click **Save**.

The user is now a member of the new group and inherits all of that group's rights, recording rules, and filters.

Adding Users from LDAP

Navigate to **Users**.

To add users to Call Recording from LDAP, the system administrator must configure both Call Recording and the LDAP so they communicate together.

Using LDAP to add users to Call Recording imports information for several users simultaneously, and maintains user information in the LDAP so it is updated in Call Recording automatically.

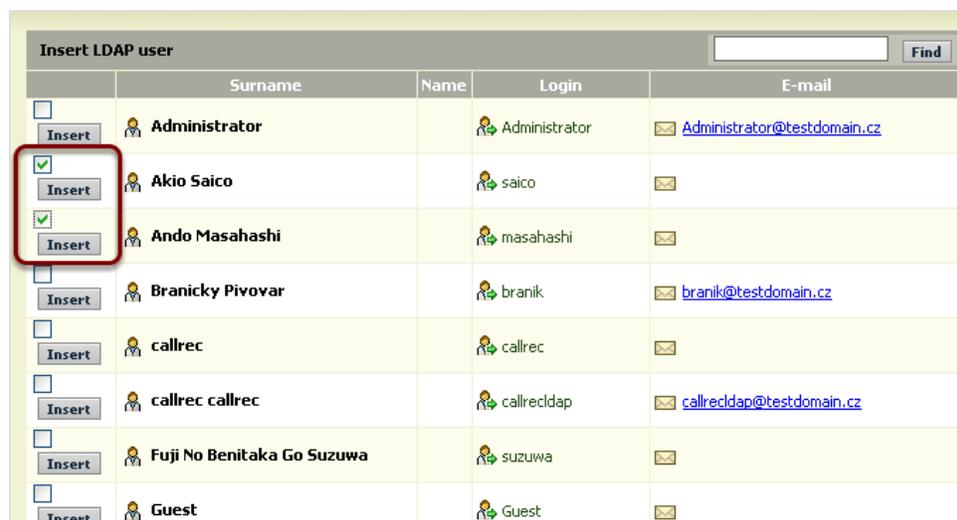


Figure 24: Inserting Users from LDAP

1. Open a group from the tree list on the left hand side of the screen.
2. Click **Insert new user**.
3. Click **Insert from LDAP**.

The **Insert LDAP user** form displays.

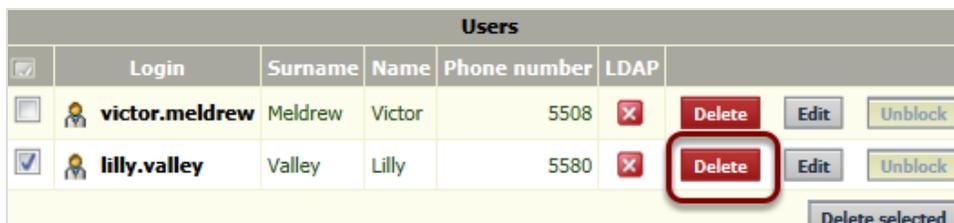
Select users to insert. Click **Insert**.

The LDAP information is imported into Call Recording, and the LDAP users are inserted into the group, inheriting the group's rights, recording rules, and filters.

Deleting Users

To delete a user, navigate to **Users**.

Open the **Users Group** in the tree list on the left hand side of the screen.



Users						
<input type="checkbox"/>	Login	Surname	Name	Phone number	LDAP	
<input type="checkbox"/>	 victor.meldrew	Meldrew	Victor	5508		<input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Unblock"/>
<input checked="" type="checkbox"/>	 lilly.valley	Valley	Lilly	5580		<input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Unblock"/>
						<input type="button" value="Delete selected"/>

Figure 25: Deleting a User

Find the user in the list, and click **Delete**.

The user is deleted and no longer has any access to the Call Recording system.

Important:

Deleting users cannot be undone. Do not delete the user **scorecard** in the group **System_play** because this user provides access for Quality Manager to play calls.

If a user has created a filter, and that filter is utilized by any other user of the system, the user who created the filter cannot be deleted.

Deleting multiple users

To delete multiple users, navigate to **Users**.

1. Open the **Users Group** from the tree list on the left hand side of the screen.
2. Find the users in the list.
3. Select the checkboxes for users to be deleted.
4. Click **Delete Selected**.

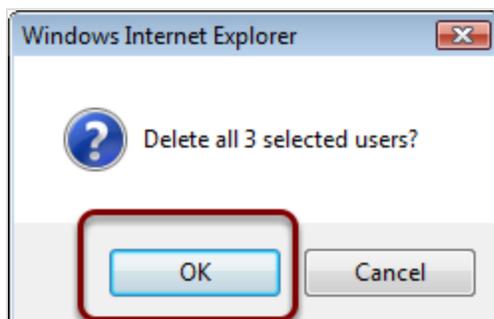


Figure 26: Deleting confirmation

5. Click **OK** to confirm the deletion.

All the users selected are deleted and no longer have access to the Call Recording system.

Important:

Deleting users cannot be undone. If a user has created a filter, and that filter is utilized by any other user of the system, the user who created the filter cannot be deleted.

Chapter

5

Creating Recording Rules

This chapter describes how to create and implement recording rules. Recording rules determine which calls are recorded by Call Recording. This manages the load on the Call Recording system and avoids wasting system resources on unwanted recordings.

This chapter contains the following sections:

[Recording Rules Overview](#)

[Types of Recording Rules](#)

[Rule Order](#)

[Using Wild Cards for Recording Rules](#)

[Identifying SIP Calls](#)

[Creating a New Recording Rule](#)

[Creating a Recording Rule to Record All Calls](#)

[Hierarchical Recording Rules](#)

[Creating a Recording Rule with External Data](#)

[Adding External Data to Recording Rules](#)

[Editing recording rules](#)

[Deleting Recording Rules](#)

Recording Rules Overview

Navigate to Recording rules.

Recording rules																
Rule	Rule type	Mask	Usage (%)	Days of week							From (hh:mm)	Till (hh:mm)	Priority	ScreenREC	ScreenREC Usage (%)	
				Mo	Tu	We	Th	Fr	Sa	Su						
Do not record	Phone number	685?	100%	<input checked="" type="checkbox"/>	00:00	24:00	▼	<input checked="" type="checkbox"/>	100%	Delete Edit						
Record	Phone number	6*	100%	<input checked="" type="checkbox"/>	00:00	24:00	▲ ▼	<input checked="" type="checkbox"/>	100%	Delete Edit						
Record	Phone number	5+	100%	<input checked="" type="checkbox"/>	00:00	24:00	▲	<input checked="" type="checkbox"/>	100%	Delete Edit						

Figure 27: Recording Rules Overview

Recording rules are always associated with groups of users, and identify which calls to record or not to record for those users. The recording rules in each group are processed in sequence in the order that they appear in the list from the top to the bottom. If there is no rule for the call or the condition is not met for the call, the processing is passed on to all subgroups. Processing takes place in all branches of the hierarchy in parallel.

Sequential processing of each group can be prevented by applying a mask filter, which limits the telephone numbers, and therefore processing, assigned to a group that would normally be always included in sequential rule processing. Additionally, the special Ignore rule is used for immediate switching of processing to remaining subgroups.

If a call doesn't match any rule in any of the groups or subgroups then it is not recorded.

Recording rules can be set for a range of phone numbers as well as a single phone number. Wild cards are valid when creating recording rules, and are described later in this section of the document.

Important:

Dates and times entered or displayed in recording rules always use the server time zone. All other dates and times in the Call Recording Web UI use the time zone specified in **Settings > User Setup > Personal Setup**.

Types of Recording Rules

There are four main types of recording rules that can be defined:

- **Record:** the system records incoming and outgoing calls from the specified number, or range of phone numbers.
- **Pre-record:** the system records the calls, but does not save the recording unless the user sends a request.
- **Do not record:** the system does not record any calls from or to the specified number, or range of phone numbers.
- **Ignore:** a rule that stops the process of rule evaluation in the current group and passes the processing to subgroups. This is only used if there is a complicated hierarchy of rules.

If no recording rules are set, no calls are recorded.

Rule Order

Navigate to **Recording rules**.

Recording rules																
Rule	Rule type	Mask	Usage (%)	Days of week							From (hh:mm)	Till (hh:mm)	Priority	ScreenREC	ScreenREC Usage (%)	
				Su	Mo	Tu	We	Th	Fr	Sa						
Do not record	Phone number	665?	100%	<input checked="" type="checkbox"/>	00:00	24:00	▼	<input checked="" type="checkbox"/>	100%	Delete Edit						
Record	Phone number	6*	100%	<input checked="" type="checkbox"/>	00:00	24:00	▲▼	<input checked="" type="checkbox"/>	100%	Delete Edit						
Record	Phone number	5*	100%	<input checked="" type="checkbox"/>	00:00	24:00	▲	<input checked="" type="checkbox"/>	100%	Delete Edit						

Figure 28: Recording Rules Order

Recording rules are applied from top to bottom. The rule that appears at the top of the rules list is processed first, and then the second and so on. It is important to be aware that rules are applied in the following hierarchy:

1. **Record.**
2. **Prerecord.**
3. **Do not record.**

To move rules up or down, use the up and down arrow buttons.

Order **Do not record** rules above the **Record** rules.

If there is a rule to **Record** all calls above a rule to **Record** a specific range of numbers, then all calls are still recorded.

If there is a rule to **Record** a specific range of numbers above the rule to **Record** all calls, then all calls are recorded from the range of numbers.

Add global rules to the admin group and group-specific rules to the appropriate subgroup.

Using Wild Cards for Recording Rules

Navigate to Recording rules.

Recording rules																	
Rule	Rule type	Mask	Usage (%)	Days of week							From (hh:mm)	Till (hh:mm)	Priority	ScreenREC	ScreenREC Usage (%)		
				Su	Mo	Tu	We	Th	Fr	Sa						Delete	Edit
Do not record	Phone number	665?	100%	<input checked="" type="checkbox"/>	00:00	24:00	▼	<input checked="" type="checkbox"/>	100%	Delete	Edit						
Prerecord	Phone number	445?	100%	<input checked="" type="checkbox"/>	00:00	24:00	▲ ▼	<input checked="" type="checkbox"/>	100%	Delete	Edit						
Record	Phone number	6*	100%	<input checked="" type="checkbox"/>	00:00	24:00	▲ ▼	<input checked="" type="checkbox"/>	100%	Delete	Edit						
Record	Phone number	5*	100%	<input checked="" type="checkbox"/>	00:00	24:00	▲	<input checked="" type="checkbox"/>	100%	Delete	Edit						

Figure 29: Recording Rules Example

Setting the range: 200? selects the numbers from 2000 to 2009; 20?? selects the numbers from 2000 to 2099.

Setting all numbers: entering 2* selects all phone numbers which start with the number 2. Entering *2 selects all phone numbers which end with the number 2.

Incoming and outgoing: the special character > sets the range for specifying incoming or outgoing phone calls. For example: 2005> selects all calls made from the number 2005 and >2005 selects all calls that were made to the number 2005.

From To: the special character = specifies calls made between two phone numbers. For example 2005=3000 selects calls made between 2005 and 3000.

Wild cards can be combined. For example 20??> selects all outgoing calls from numbers 2000 to 2099.

Identifying SIP Calls

SIP (Session Initiation Protocol) requires the use of the @ symbol when identifying telephone numbers to create recording rules. For example:

- 1224@*
- 123*@*
- ?????@*

Creating a New Recording Rule

Recording rules are always assigned to groups. Select a group in the **Recording rules** tab before adding or editing recording rules.

Navigate to **Recording rules**. Select a group from the tree list on the left hand side of the screen.

Click **Insert new rule**. The **Insert new rule** form displays.

All time fields on this page are in following timezone: Europe/Prague

Insert new rule

Rule: Record Rule type: Phone number

Mask: 42* Usage (%): 100

Days of week

Su	Mo	Tu	We	Th	Fr	Sa
<input checked="" type="checkbox"/>						

From (hh:mm): 00:00

Till (hh:mm): 24:00

ScreenREC: ScreenREC Usage (%): 100

Priority: High priority

Insert new rule Cancel

Figure 30: Insert a New Rule

1. Select a rule from the **Rule:** drop-down list:
 - Record
 - Do Not Record
 - Prerecord
 - Ignore.
2. Select a rule type from the **Rule type:** drop-down list:
 - Phone number
 - IP address
 - External Data.
3. Type the **Mask:**, a phone number or range of numbers using wildcards. GQM supports alphanumeric characters for extensions, DNSs, or terminals.
Type the **Usage (%)**:, for randomly recording only a percentage of all calls.

4. Select the **Days of week**.
5. Type the **From (hh:mm):** and **Till (hh:mm):** values to identify the daily time range to record calls.
Type the **Screen Capture Usage (%)** value, for randomly recording the screen of only a percentage of all calls.
6. Select the Screen Capture checkbox to also record agent desktops.
7. Click **Insert new rule**.



Figure 31: Apply Changes

Click **Apply changes**. The new recording rule is now active in Call Recording.

Creating a Recording Rule to Record All Calls

At least one recording rule must be defined otherwise calls are not recorded. The simplest rule mask to record all calls is an asterisk *, as shown in the following screenshot.

Navigate to **Recording rules**.

Click **Insert new rule**.

All time fields on this page are in following timezone: Europe/Prague

Insert new rule

Rule: Record Rule type: Phone number

Mask: * Usage (%): 100

Days of week

Su	Mo	Tu	We	Th	Fr	Sa
<input checked="" type="checkbox"/>						

From (hh:mm): 00:00

Till (hh:mm): 24:00

ScreenREC: ScreenREC Usage (%): 100

Priority: High priority

Insert new rule Cancel

Figure 32: Record all Calls Example

1. Type a phone number or asterisk * in the **Mask:** field.
2. Click **Insert new rule**.
3. Click **Apply changes**.

Hierarchical Recording Rules

Recording rules can be defined in every Call Recording group, and groups are arranged in a hierarchy. Higher group recording rules are processed prior to subordinate groups, therefore the more restrictive rules should be at the top of the rule hierarchy.

Hierarchical Recording Rules Example

Navigate to **Recording rules**.

In Call Recording groups are defined in a hierarchical order.

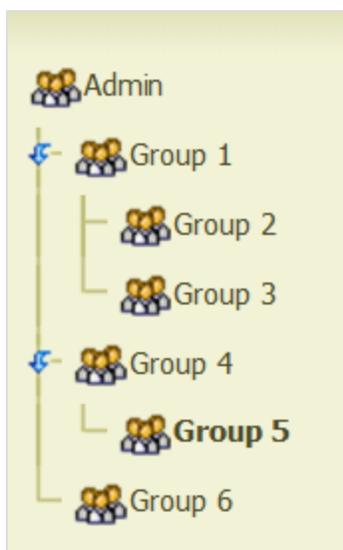


Figure 33: Group Hierarchy Tree Structure

1. The rules defined in the group at the top, for example **Admin**, have the highest priority.
2. The rules defined in groups 1,4, and 6 are processed next in parallel.
3. The rules defined in groups 2,3, and 5 are processed last in parallel because they have the lowest priority.

The **Admin** group has highest priority and any recording rule defined for **Admin** always overrides any recording rule from subordinate groups, first match rule. If a recording rule is defined within a group, then the recording rule is passed on to all subordinate groups. If there is no recording rule from the group above then the rules from the subgroups are processed directly.

Groups must be prevented from creating recording rules that can affect groups on the same level

This sequential processing can be prevented by applying a subgroup (mask) filter. In this case the type of recording for this subgroup branch remains undetermined. This is better illustrated in the following examples:

Example 1:

- There is a rule in Group 4 "do not record calls from 42???"
- Group 5 has a rule "record calls from 4????".

The Group 4 rule has priority over the Group 5 rule so the rule in Group 4 is applied first. Group 5 does not record calls from 4200 to 4299. The result is that Group 5 only records calls from 4000 – 4199 and from 4300 – 4999.

Example 2:

- The rule in Group 2 is to "record calls from 4????".
- The rule in Group 3 is to "pre-record calls from 4????".
- The rule in Group 5 is "do not record calls from 4????".

The Group 2 rule has priority over Group 3 and Group 5 rules. A record rule has priority over a do not record rule. The result is that Calls from 4???? are recorded.

Example 3:

- The rule in Group 2 is to "record calls from 4????",
- The rule in Group 3 is to "pre-record calls from 4????"
- The rule in Group 5 is "do not record calls from 4????".

- We set the phone number for Group 1 to "42???" this restricts the influence of any rules created by any subordinate groups 2-6 to within the number range of 4200-4299.
- We set the number for Group 2 to "420?" this restricts the influence of group 2 to within the number range 4200-4209 even though the rule set is "record calls from 4????".

The result is calls that from 4200-4209 are recorded by the rule from Group 2, calls from 4210-4299 are pre-recorded from the rule in Group 3 and calls from 4000-4199 and 4300-4399 are not recorded.

Hierarchical Rule Administration Example

Navigate to **Recording Rules**.



Figure 34: Agent Group

The system administrator wants to delegate rule administration for each main group, groups 1, 2, 3 in the above diagram, to the respective agent group leader. This is accomplished as follows:

Each group is given the appropriate range of extension numbers as its phone number;.

For example:

- Group 1: 42?? covering extensions 4200-4299
- Group 2: 43?? covering extensions 4300-4399
- Group 3: 44?? covering extensions 4400-4499

Three ignore rules are created by the system administrator in the top-level **Admin** group.

- Ignore 42??
- Ignore 43??
- Ignore 44??

Each group leader creates additional rules for his or her group at the group level (that is, Group 1 leader creates rules when Group 1 is selected on the Recording Rules screen).

When a call is made to or from a group extension, all top-level Admin rules are ignored and only rules within that group are processed.

Creating a Recording Rule with External Data

Navigate to Recorded calls.

From	To		Description
5508 (Dev 5508 SLR)	5507 (Dev 5507 SLR)	   	
5508 (Dev 5508 SLR)	5507 (Dev 5507 SLR)	   	
5508 (Dev 5508 SLR)	5507 (Dev 5507 SLR)	   	
5508 (Dev 5508 SLR)	5507 (Dev 5507 SLR)	   	

Figure 35: The information Button

Select a record from a number that contains the desired data key and click the information icon . The **Call description** dialog opens and displays the available call data keys and values.

Call description

Couple Information

Call ID	69
Couple ID	69
Call Status	No stream recorded.
Synchro Tool	
Delete Tool	
Mixer Tool	
Restore Tool	
Archive Tool	
ScoreCARD Usage	
Synchronization ID	17521303192.168.7.8:24244192.168.7.7:19814_1
Protected Against Deletion	No

External Data

Key	Value
CALLED_STREAM_PAYLOAD	G.711 ulaw 64k (1104)
CALLED_URL	192.168.7.7:19814(1104)
CALLING_STREAM_PAYLOAD	G.711 ulaw 64k (1104)
CALLING_URL	192.168.7.8:24244(1104)
COUPLE_END_REASON	NORMAL
COUPLE_START_REASON	NORMAL
GROUP_ID	17521303
JTAPI_CALLED_TERMINAL_SEP	SEP000011120003
JTAPI_CISCO_CALLMANAGER_ID	1
JTAPI_CISCO_GLOBAL_CALL_ID	744087
JTAPI_CISCO_ID	17521303

Figure 36: Call Description

Copy the **External Data Key** required from the list, in this example, **GROUP_ID**. The **Call description** window is in a separate pop up, so it can be kept open for the following step.

Return to the top of the main window, navigate to **Recording rules** and select the group that the rule applies to, from the groups on the left hand side, in this example, Group A.

Create new rule for the group:  **Group A**

All time fields on this page are in the following time zone: Europe/Prague

Insert new rule

	Rule: Record ▼	Rule type: External Data ▼																						
	Mask: GROUP_ID 1752130?	Usage (%): 100																						
<table border="1" style="width: 100%; border-collapse: collapse; background-color: #a6a6a6;"> <thead> <tr> <th colspan="7">Days of week</th> </tr> <tr> <th>Su</th> <th>Mo</th> <th>Tu</th> <th>We</th> <th>Th</th> <th>Fr</th> <th>Sa</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">☑</td> </tr> </tbody> </table>		Days of week							Su	Mo	Tu	We	Th	Fr	Sa	☑	☑	☑	☑	☑	☑	☑	From (hh:mm): 00:00	Till (hh:mm): 24:00
Days of week																								
Su	Mo	Tu	We	Th	Fr	Sa																		
☑	☑	☑	☑	☑	☑	☑																		
ScreenREC: <input type="checkbox"/>		ScreenREC Usage (%): 100																						
Priority: High priority ▼	<input type="button" value="Insert new rule"/> <input type="button" value="Cancel"/>																							

Figure 37: Recording Rule Based on External Data

1. Select **External Data** in the **Rule type**: drop-down list.
2. In the **Mask**: field:
 - Paste the key into the mask then type a blank space after the key, to separate the **Key** and **Value**.
 - Go back to the **Call details** pop up and copy the **External Data Value**, then paste it after the blank space in the **Mask**: field, or type a value, wild cards are valid. GQM supports alphanumeric characters for extensions, DNs or terminals.
3. Click **Insert new rule**.
4. Click **Apply changes**.

The new recording rule using external data is now active in Call Recording.

To test the rule, make a call from a group that should contain the data, and check the **Recorded calls** tab for the recorded call.

Adding External Data to Recording Rules

Recording rules can be based on external data sources integrated with Call Recording. The following table contains an example of Genesys external data used for defining recording rules:

External Data Key	Sample Value
GEN_CFG_EMPLOYEE_ID	Employee_ID_20
GEN_CFG_FirstName	Jeremy
GEN_CFG_FULLNAME *	Jeremy Johns
GEN_CFG_LastName	Johns
GEN_TEV_AgentID	jjohns
GEN_TEV_CallType	Internal
GEN_TEV_DNIS	7600
GEN_TEV_OtherDN	7600
GEN_TEV_ThisDN	7620

Table 2: Sample external data keys and values

* customizable field created by integration module

Editing recording rules

Navigate to **Recording rules**.

The user must have sufficient access rights to change recording rules. Do not change recording rules without considering the effect on the performance of the system.

All time fields on this page are in following timezone: Europe/Prague	
Rule: Record	Rule type: Phone number
Mask: 5*	Usage (%): 100
Days of week: Su Mo Tu We Th Fr Sa <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	From (hh:mm): 00:00 Till (hh:mm): 24:00
Active <input checked="" type="checkbox"/>	
ScreenREC <input type="checkbox"/>	ScreenREC Usage (%): 100
Save Cancel	

Figure 38: Recording Rule Editing

In the **Recording rules** tab, navigate to a group that has a recording rule.

Click **Edit**. The **Edit the recording rule** form displays.

Edit the rule as required. Click **Save**.

Click **Apply changes**.

The changes to the recording rule apply immediately.

Turn a recording rule on and off with the **Active** checkbox that is only visible in the **Edit the recording rule** form.

Deleting Recording Rules

Navigate to **Recording rules**.

The user must have the rights to delete recording rules. Do not delete recording rules without considering the effect on the performance of the system.



Figure 39: Deleting Recording Rules

In the **Recording rules** tab, navigate to a group that has a recording rule.

1. Click **Delete**.
2. Click **Apply changes**.

The recording rule is deleted and calls within the deleted recording rule are no longer recorded, unless a new recording rule is created.

Click **Edit** and select the **Active** checkbox to activate a rule.

Chapter

6

Configuring Call Recording Core

This chapter describes the settings available in the **Call Recording Core** tab. The main configuration of Call Recording core is set during the installation process and is essential for Call Recording functionality. Changing any of these settings may dramatically change system performance.

Only skilled administrators should attempt to change the configuration of Call Recording Core. The default parameters are correct for a single server installation.

This chapter contains the following sections:

[Adding New Servers](#)

[Displaying Database Pools](#)

[Adding a New Pool](#)

[Configuring Call Recording Core Addresses and RMI](#)

[Changing the SMTP Settings](#)

[Changing the Admin Email Notifications "From" Address](#)

Adding New Servers

Log in as admin. Navigate to **Settings > Configuration > Call Recording Core > Servers** and scroll down.

The **Servers** screen displays all installed servers and ports, including the Core and Key Manager servers. Define aliases at the bottom of the list to use in other configuration dialogs.



The screenshot shows a web interface for adding a new server. At the top, there is a green header bar with the text "Add new server". Below this, on the left side, there are two red buttons: "Save configuration" and "Reload configuration". To the right of these buttons, there are three input fields: "Server name" (with a placeholder "Server name"), "Server IP address", and "Port" (with a placeholder "0"). A red button labeled "New" is positioned to the right of the "Port" field.

Figure 40: Servers Tab

To add a new server:

1. Type the **Server name**, **Server IP address** and **Port**. Each server name must be unique.
2. Click **New**.
3. Click **Save configuration**.

Displaying Database Pools

Log in as admin. Navigate to **Settings > Configuration > Call Recording Core > Database**.

The **Database** tab displays all database pools used by Call Recording, including aliases.

Database	
callrec	
Pool name (for CallREC set "callrec")	callrec
Pool type	ibatis pool
SQL map	Callstorage (PostgreSQL)
Host	192.168.110.78
Port	5432
Database	callrec
Login name	callrec
Password	callrec
Maximum connections	20
Connections on init	1
Timeout	5
Remove	

Figure 41: Database Tab

There can be multiple pools. The main pool must be named **callrec**. Settings for database pools use the following parameters:

1. **Pool name:** name of pool for Call Recording, this must always be **callrec**, other pools may be configured as described in the documentation.
 2. **Pool type:** select the type according to the Call Recording settings, in most cases this is set as **ibatis pool**.
The Genesys Connection pool type is only used for special purposes. If selected, the **Database driver** selection appears instead of **SQL map**.
- **SQL map:** select an XML description of the database structure. This setting is determined by the type of database required. For the Call Recording main database select **Callstorage (PSQL)**, for Maintenance tools, use

Maintenance (PSQL).

- **Host:** IP address of the database server.
- **Port:** port number of the database server.
- **Database:** the name of the database.
- **Login name:** the login name for user with administrator rights.
- **Password:** the user password.
- **Maximum connections:** maximum simultaneous connections to the database.
- **Connections on init:** the number of initial connections. It is recommended to set this value to 1.
- **Timeout:** registered in seconds.

If the User define option is selected in **SQL map**, then the option **SQL map path** appears. Define a path to a custom XML map. For example:

```
/cz/zoom/callrec/core/callstorage/pojo/sqlMap-config.xml
```

Adding a New Pool

Navigate to **Settings > Configuration > Call Recording Core > Database** and scroll to the bottom.

Below the display of existing Database pools, add new pools from the Database screen.



The screenshot shows a form titled "Add New Pool" with a green header. Below the header, there is a label "Pool name (for CallREC set 'callrec')", a text input field containing "pool name", and a red "New" button.

Figure 42: Database Add New Pool

To add a new pool:

1. Type the **Pool name (for CallREC set "callrec")**.
2. Click **New**. The new pool is added.
3. Define all fields.
4. Click **Save configuration**.

Configuring Call Recording Core Addresses and RMI

Navigate to **Settings > Configuration > Call Recording Core > Call Recording Core**.

Set the main core server in multi-site installations. Select the same server alias from both drop-down lists.

The screenshot shows the 'Call Recording CORE' configuration page. On the left is a navigation menu with options: Servers, Database, Call Recording Core (selected), Drivers and Readers, and SMTP setting. Below the menu are two buttons: 'Save configuration' and 'Reload configuration'. The main content area is titled 'Call Recording CORE' and is divided into three sections: 'Application Communicator', 'Core settings', and 'Core rmi'. In the 'Application Communicator' section, the 'Registry address' is set to 'core'. In the 'Core settings' section, the 'API registry address' is set to 'core' and the 'Observe core' checkbox is checked. In the 'Core rmi' section, the 'RMI callback port (0=anonymous)' is set to 30600 and the 'RMI export port (0=anonymous)' is set to 30601.

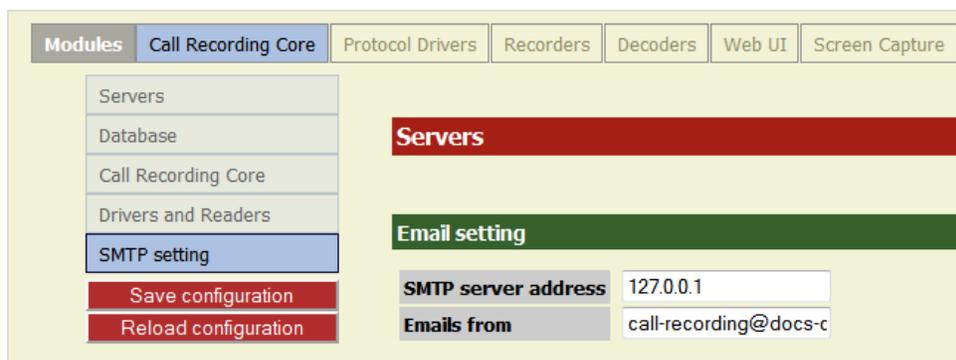
Figure 43: Call Recording CORE Settings

1. **Registry address:** points to the server to where the application communicator service is running (RMI service).
2. **API registry address:** points to the Call Recording API that is always running on the primary core server.
Observe core enables monitoring of the core server.
3. **Core RMI:** sets the RMI callback port and export port.
4. Click **Save Configuration**.

Changing the SMTP Settings

Navigate to **Settings > Configuration > Call Recording Core > SMTP Setting**.

The **SMTP setting** enables Call Recording to email users and administrators.



The screenshot shows a web interface for configuring the Call Recording Core. At the top, there is a navigation bar with tabs for 'Modules', 'Call Recording Core', 'Protocol Drivers', 'Recorders', 'Decoders', 'Web UI', and 'Screen Capture'. Below this, a sidebar menu lists 'Servers', 'Database', 'Call Recording Core', 'Drivers and Readers', 'SMTP setting', 'Save configuration', and 'Reload configuration'. The 'SMTP setting' option is selected. The main content area is divided into two sections: 'Servers' (highlighted in red) and 'Email setting' (highlighted in green). Under 'Email setting', there are two input fields: 'SMTP server address' with the value '127.0.0.1' and 'Emails from' with the value 'call-recording@docs-c'.

Figure 44: SMTP Settings

To change the IP address of the Call Recording SMTP server (initially defined during Call Recording installation).

1. Type the new address in the **SMTP server address** field.
2. Click **Save configuration**.

Changing the Admin Email Notifications "From" Address

To change the name of the email sender that was set during installation:

1. Change the XML property in webadmin.xml:

```
Property name="email.address" value="callrec@docs-  
callrec1.office.zoomint.com"/>
```

2. Type the new address in the `value` field.
3. Restart the WebGUI with the following command.

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

Chapter

7

Configuring Protocol Adapters and Protocol Drivers

Protocol adapters and protocol drivers, translate telephony signaling events into the unified messages that Call Recording Core requires to control recording. A protocol driver is the equivalent of a protocol adapter with its own drivers and readers combined in one module. The use of protocol adapters and protocol drivers, also enables the support of new protocols as they are introduced to IP telephony without radical changes to Call Recording Core.

This chapter contains the following sections:

[Protocol Adapters and Protocol Drivers Overview](#)

[Protocols Supported By Protocol Adapters and Protocol Drivers](#)

[Configuring Drivers and Readers for JTAPI Adapters](#)

[Adding a New Reader](#)

[Configuring JTAPI adapter](#)

[Downloading JTAPI Library from CUCM \(JTAPI Signaling\)](#)

Protocol Adapters and Protocol Drivers Overview

Protocol adapters and protocol drivers, translate telephony signaling events into the unified messages that Call Recording Core requires to control recording. A protocol driver is the equivalent of a protocol adapter with its own drivers and readers combined in one module. The use of protocol adapters and protocol drivers, also enables the support of new protocols as they are introduced to IP telephony without radical changes to Call Recording Core.

Protocols Supported By Protocol Adapters and Protocol Drivers

Call Recording supports the following protocols using protocol adapters and their associated readers:

- Cisco Skinny
- Cisco JTAPI
- SIP

Call Recording supports the following protocols using protocol drivers:

- Genesys SIP and T-Lib
- Avaya JTAPI and DMCC

The role of each protocol driver or adapter is to translate the signaling from a particular protocol used in the call center equipment into standard messages for the Core. These messages inform Core about events such as:

- Call establishment
- The start and end of RTP streams
- Transfers
- Conferences
- Calls on-hold

Configuring Drivers and Readers for JTAPI Adapters

Navigate to **Settings > Configuration > Call Recording Core > Drivers and Readers**.

Drivers and readers are configured during installation, there is no reason to modify them. Readers are responsible for communication with the protocol adapters. Every protocol adapter must have its own reader. If more protocol adapters are used, for example, to listen on more network interfaces, then create more readers.

Ensure that all readers are configured properly:

The screenshot displays the 'Drivers and Readers Configuration' page. On the left, a sidebar contains navigation links: 'Servers', 'Database', 'Call Recording Core', 'Drivers and Readers' (highlighted), and 'SMTP setting'. The main area features a red header 'Drivers and Readers Configuration'. Below it, the 'Drivers' section shows 'Genesys' with a checked checkbox. The 'Sniffer Readers' section contains a table with two entries. The first entry has 'Name' 'MSRSniffer', 'Server and port' 'core' and '30350', and a 'Remove' button. The second entry has 'Name' 'Reader name', 'Server and port' 'core' and '30300', and a 'New' button. At the bottom left, there are 'Save configuration' and 'Reload configuration' buttons.

Figure 45: Drivers and Readers

1. Select the appropriate checkbox to enable the appropriate Driver for the **Protocol Adapter**. If a driver is disabled, the particular signaling protocol is not processed, regardless of the **Protocol Adapter** settings.
2. Type a unique name for the reader, select the correct server from the drop-down list, and type a unique port number.

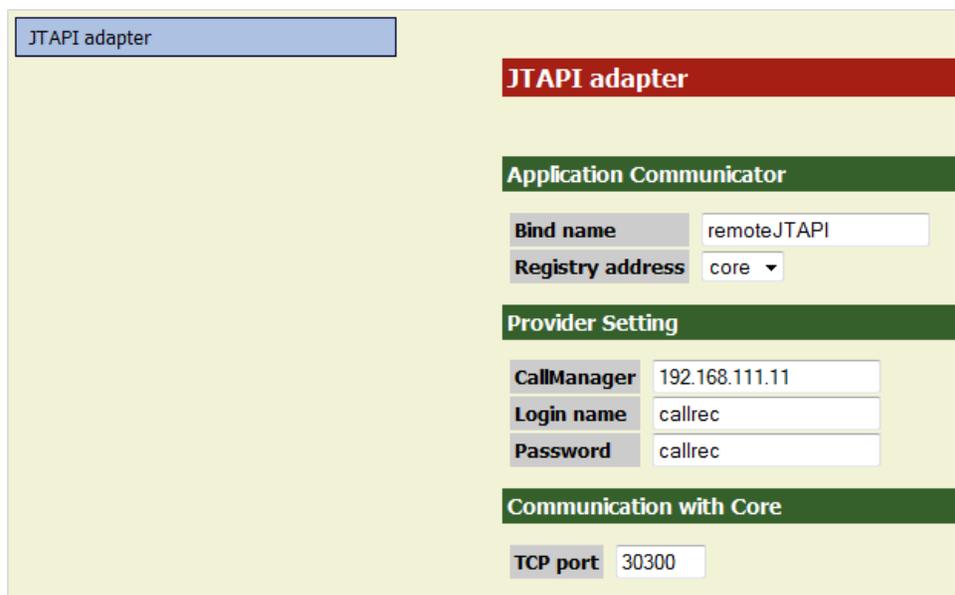
Adding a New Reader

To add a new reader:

1. Type a name for the reader in the **Add new reader** field.
2. Select the **Server and port**.
3. Click **New**.
4. Click **Save configuration**.

Configuring JTAPI adapter

Navigate to **Settings > Configuration > Protocol Adapters > JTAPI adapter**.



JTAPI adapter	
JTAPI adapter	
Application Communicator	
Bind name	remoteJTAPI
Registry address	core
Provider Setting	
CallManager	192.168.111.11
Login name	callrec
Password	callrec
Communication with Core	
TCP port	30300

Figure 46: JTAPI Adapter Configuration

Configuration of the **JTAPI adapter** includes the following parameters:

Application Communicator:

- **Bind name:** the registered name of JTAPI RMI service.
- **Registry address:** the server where the RMI service runs.

Provider Setting:

- **CallManager:** the IP address for CUCM.
- **Login name:** the login name for CUCM.
- **Password:** the password for Login name.

The login and password must correspond to the login and password created for the applications user in CUCM to communicate with Call Recording.

Communication with Core:

- **TCP port:** the Core server communication port, for example, the port that the Core connects to.

To function correctly the **JTAPI adapter** must have correctly configured **Drivers and Readers**.

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.

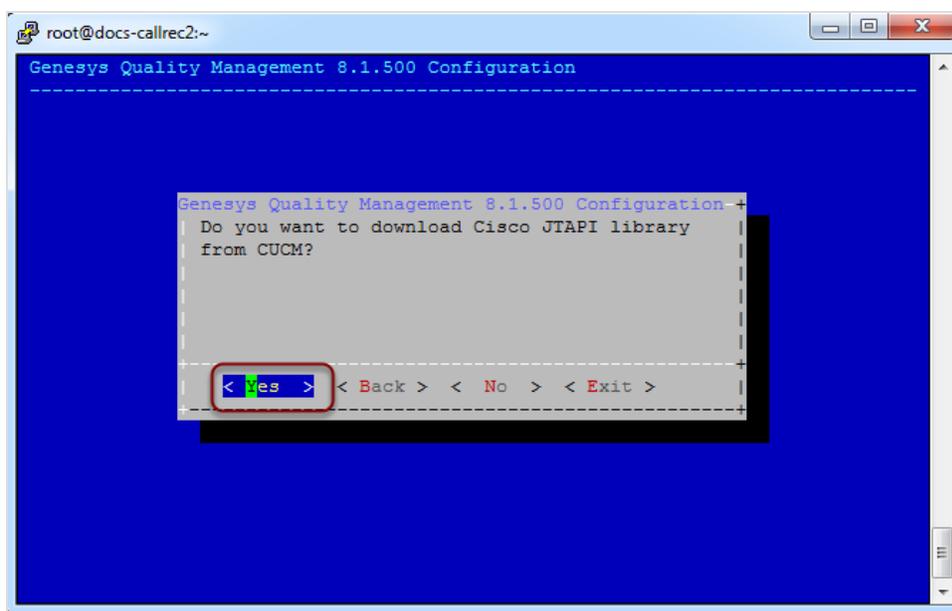


Figure 47: Download JTAPI from CUCM Configuration

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.

Chapter

8

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](#)

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' page. On the left, there is a sidebar with two tabs: 'Genesys Driver' (selected) and 'Avaya Driver'. The main content area has a red header 'Genesys Driver Configuration' and a green sub-header 'General Configuration'. Below this, there are several input fields: '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' (selected), 'Enhanced Passive Recording', and 'Active Recording Replay Server'. At the bottom left, there are two red buttons: 'Save configuration' and 'Reload configuration'.

Figure 48: 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)
- Save configuration:** (red button)
- Reload configuration:** (red button)
- Only Connect to Tenants Listed Below:**

Figure 49: 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 50: 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.

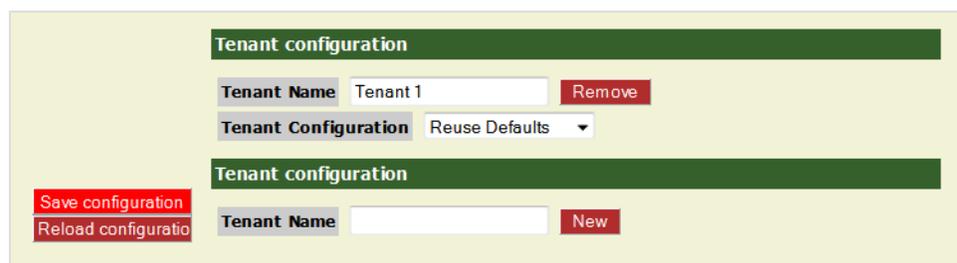


Figure 51: Tenant Configuration

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 present 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:** Contains settings for audio and video recording, including enablement checkboxes and user data keys for mandatory and optional parts. Below these are user data values for various recording states (Recording Yes, No, No Longer Recording, Prerecording, Undefined).
- 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, Names Order (FirstName LastName), and a Delimiter dropdown (Space (Example: "John Doe")).
- Tenant Configuration (Bottom):** A section for adding a new tenant, featuring a Tenant Name field and a New button.

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

Figure 52: Override Defaults

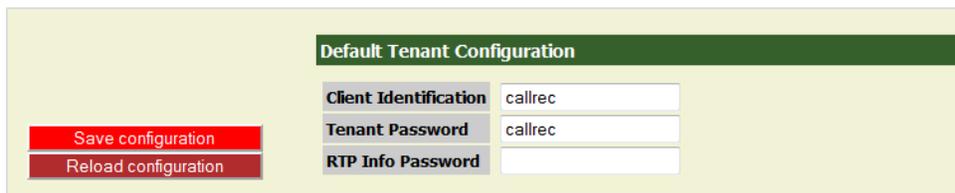
Configure the setting for each tenant in its **Tenant Configuration** section starting with the **Tenant Name**. If the tenant has more than one T-Server the T-Servers must use the same parameters for **Include DN Range**, **Exclude DN Range** and login.

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.



Default Tenant Configuration	
Client Identification	<input type="text" value="callrec"/>
Tenant Password	<input type="text" value="callrec"/>
RTP Info Password	<input type="text"/>

Save configuration
Reload configuration

Figure 53: 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 3: 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**.

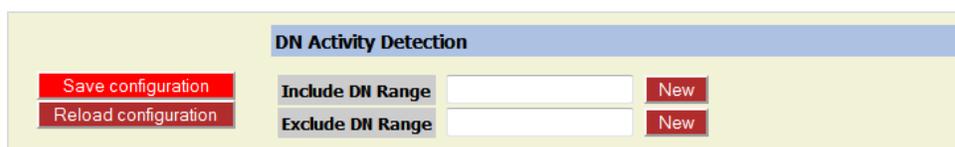


Figure 54: DN Activity Detection Configuration

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 55: 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 ThisDN.

Table 4: 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 56: 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 5: 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 6: 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.

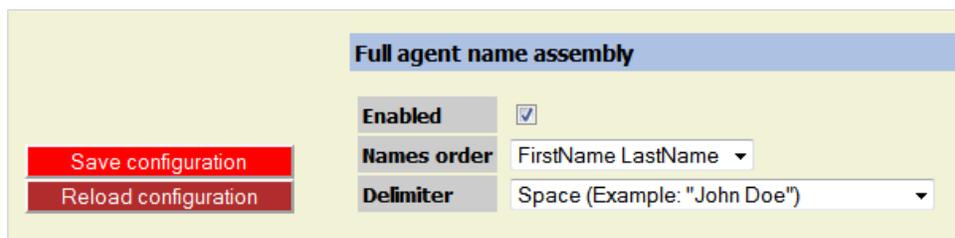


Figure 57: Full Agent Name Assembly

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 7: Agent Name Configuration

Chapter

9

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](#)

[Preparing for Avaya Communication Manager](#)

[Creating a TSAPI CTI User](#)

[Enabling the CTI User](#)

[Configuring the DMCC Port](#)

[Enabling the Security Database](#)

[Finding out What the Alias for the Switch Is](#)

[Setting the IP Address for the H.323 Gatekeeper](#)

[Finding out the Tlink Name](#)

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

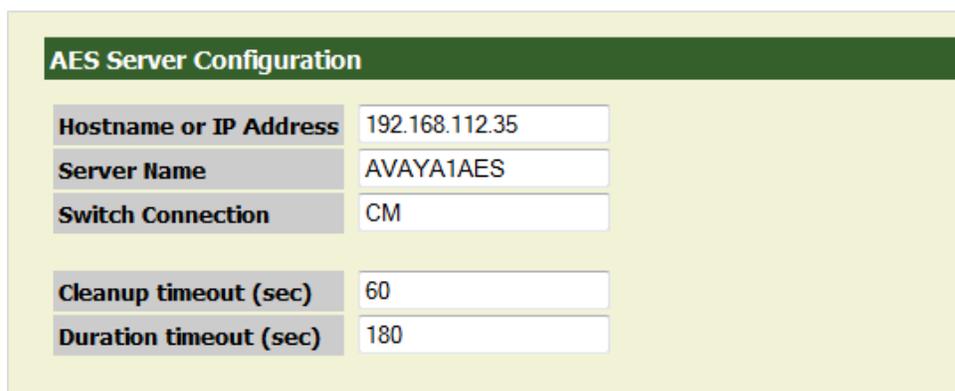
Save configuration
Reload configuration

Figure 58: 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 59: 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 60: 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

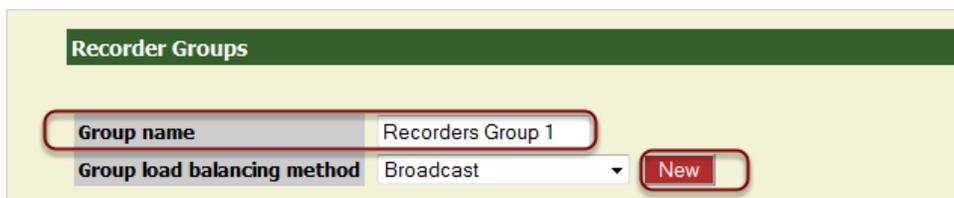
Figure 61: CM Server Configuration

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**.



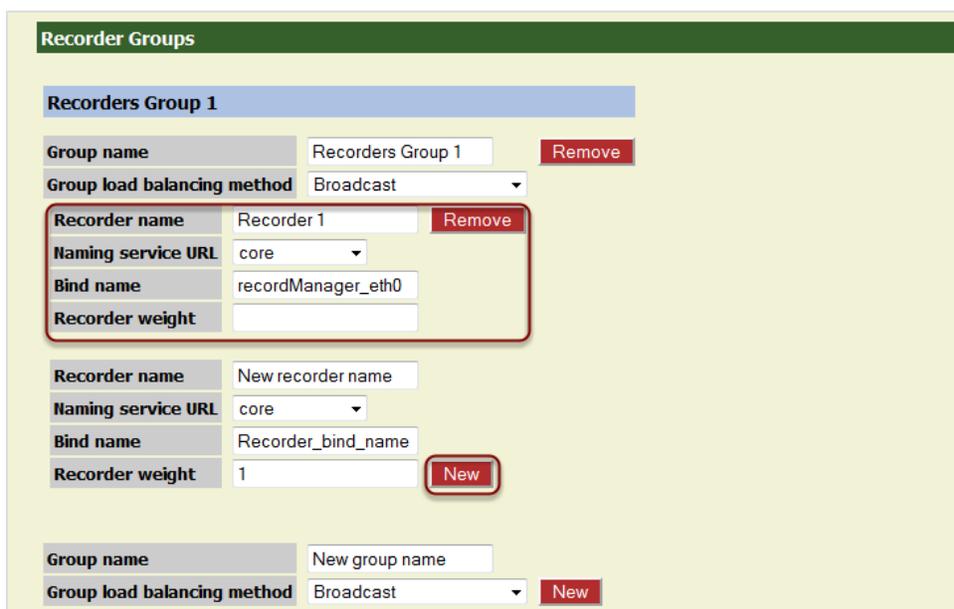
The screenshot shows the 'Recorder Groups' configuration page. At the top, there is a green header with the text 'Recorder Groups'. Below the header, there is a form with two main sections. The first section has a 'Group name' text input field containing 'Recorders Group 1' and a 'Group load balancing method' dropdown menu set to 'Broadcast'. To the right of these fields is a red 'New' button. The second section is a 'Recorder' configuration area, which is currently empty.

Figure 62: 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' configuration page with the 'Recorders Group 1' section expanded. The section has a blue header 'Recorders Group 1'. Below the header, there are two 'Recorder' configuration blocks. The first block is highlighted with a red border and contains the following fields: 'Recorder name' (text input with 'Recorder 1' and a red 'Remove' button), 'Naming service URL' (dropdown menu with 'core'), 'Bind name' (text input with 'recordManager_eth0'), and 'Recorder weight' (text input). The second block contains: 'Recorder name' (text input with 'New recorder name'), 'Naming service URL' (dropdown menu with 'core'), 'Bind name' (text input with 'Recorder_bind_name'), and 'Recorder weight' (text input with '1' and a red 'New' button). At the bottom of the page, there is a 'Group name' text input field with 'New group name' and a 'Group load balancing method' dropdown menu with 'Broadcast' and a red 'New' button.

Figure 63: 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 64: 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.

Figure 65: 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.

Preparing for Avaya Communication Manager

The Network Administration must:

- assign the AES server address.
- assign the CM server address.
- create a CTI user and provide a TSAPI user name and password.
- create a DMCC user and provide a DMCC user name and password.
- provide a DMCC port number.
- provide the IP Station security code.

Configure the recording device range on the Avaya server or choose unrestricted mode for the user.

The user must have sufficient Medpro, DMCC and TSAPI licenses.

Creating a TSAPI CTI User

Access the OAM web interface of the **Applications Enablement Services**. The **Management Console** login page displays.

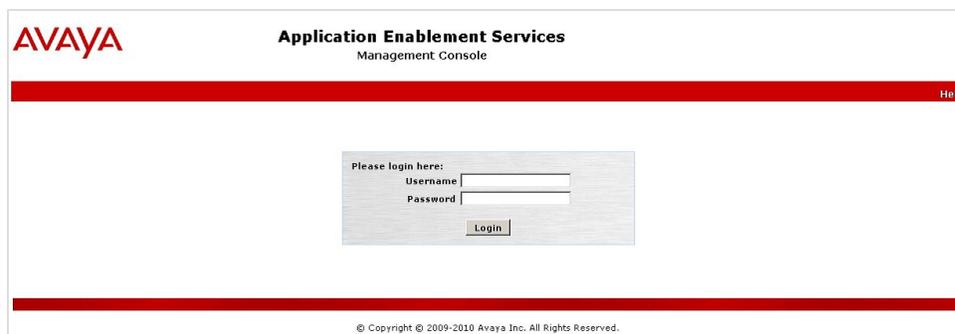


Figure 66: AES Login

Log on to the AES Management console using the appropriate username and password.

The **Welcome to OAM** page displays.

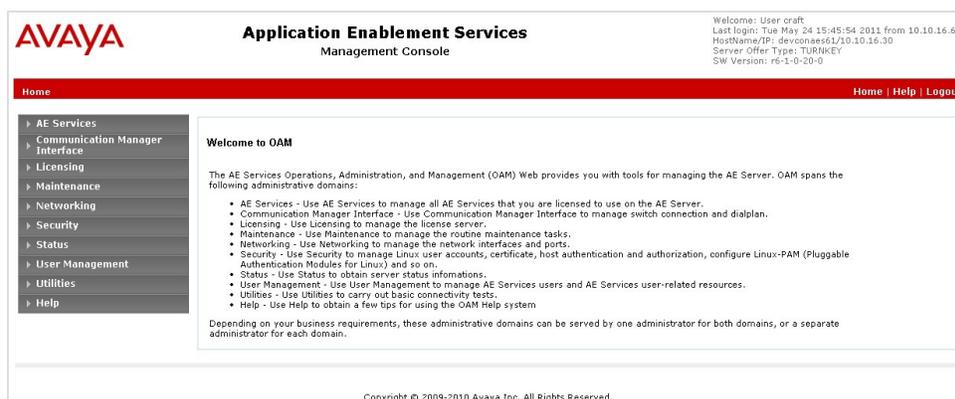


Figure 67: Welcome to OAM Page

On the AES Management Console navigate to **User Management > User Admin > Add User**.

The **Add User** page displays.

AVAYA Application Enablement Services Management Console

User Management | User Admin | Add User

> AE Services
 > Communication Manager Interface
 > Licensing
 > Maintenance
 > Networking
 > Security
 > Status
 > User Management
 > Service Admin
 > User Admin
 ▪ Add User
 ▪ Change User Password
 ▪ List All Users
 ▪ Modify Default Users
 ▪ Search Users
 > Utilities
 > Help

Add User

Fields marked with * can not be empty.

* User Id

* Common Name

* Surname

* User Password

* Confirm Password

Admin Note

Avaya Role

Business Category

Car License

CM Home

Cms Home

CT User

Department Number

Display Name

Employee Number

Figure 68: Add User Screen

1. Type the username in the **User Id** field, for example, `zoom`.
Type the name in the **Common Name** field.
Type the name in the **Surname** field.
2. Type the password in the **User Password** field.
Confirm the password in the **Confirm Password** field.
3. Select **Yes** from the **CT User** drop-down list.

Click **Apply** at the bottom of the screen.

Retain the user ID and password so that they can be used when setting up Call Recording.

Enabling the CTI User

On the AES Management Console navigate to **Security > Security Database > CTI Users > List All Users**.

In the **CTI Users** window, select the **User ID** set up in the **Add User** page and select the **Edit** option.

The **Edit CTI User** page displays.

Verify that the user created appears in the list.

The screenshot shows the Avaya Application Enablement Services Management Console. The breadcrumb trail is Security | Security Database | CTI Users | List All Users. The left navigation menu is expanded to Security Database > CTI Users > List All Users. The main content area is titled 'Edit CTI User' and contains the following configuration fields:

User Profile:	User ID	zoom2
	Common Name	zoom2
	Worktop Name	NONE
	Unrestricted Access	<input checked="" type="checkbox"/>
Call and Device Control:	Call Origination/Termination and Device Status	None
Call and Device Monitoring:	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	<input type="checkbox"/>
Routing Control:	Allow Routing on Listed Devices	None

At the bottom of the configuration area are two buttons: 'Apply Changes' and 'Cancel Changes'.

Figure 69: Setting Unrestricted Access

1. Select the **Unrestricted Access** checkbox.
2. Click **Apply Changes**.

Configuring the DMCC Port

On the AES Management Console navigate to **Networking > Ports**.

The Networking Ports screen displays.

Ports		Enabled	Disabled	
CVLAN Ports	Unencrypted TCP Port	9999	<input checked="" type="radio"/>	<input type="radio"/>
	Encrypted TCP Port	9998	<input checked="" type="radio"/>	<input type="radio"/>
DLG Port	TCP Port	5678		
TSAPI Ports	TSAPI Service Port	450	<input checked="" type="radio"/>	<input type="radio"/>
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	1050		
Encrypted TLINK Ports				
TCP Port Min	1066			
TCP Port Max	1081			
DMCC Server Ports		Enabled	Disabled	
Unencrypted Port	4721	<input checked="" type="radio"/>	<input type="radio"/>	
Encrypted Port	4722	<input checked="" type="radio"/>	<input type="radio"/>	
TR/87 Port	4723	<input checked="" type="radio"/>	<input type="radio"/>	

Figure 70: Configuring the DMCC Port

In the **DMCC Server Ports** section, set the Unencrypted Port (usually 4721) and select **Enabled**.

Click **Apply Changes**.

Enabling the Security Database

On the AES Management Console, navigate to **Security > Security Database > Control**.

The SDB Control for DMCC and TSAPI page displays.

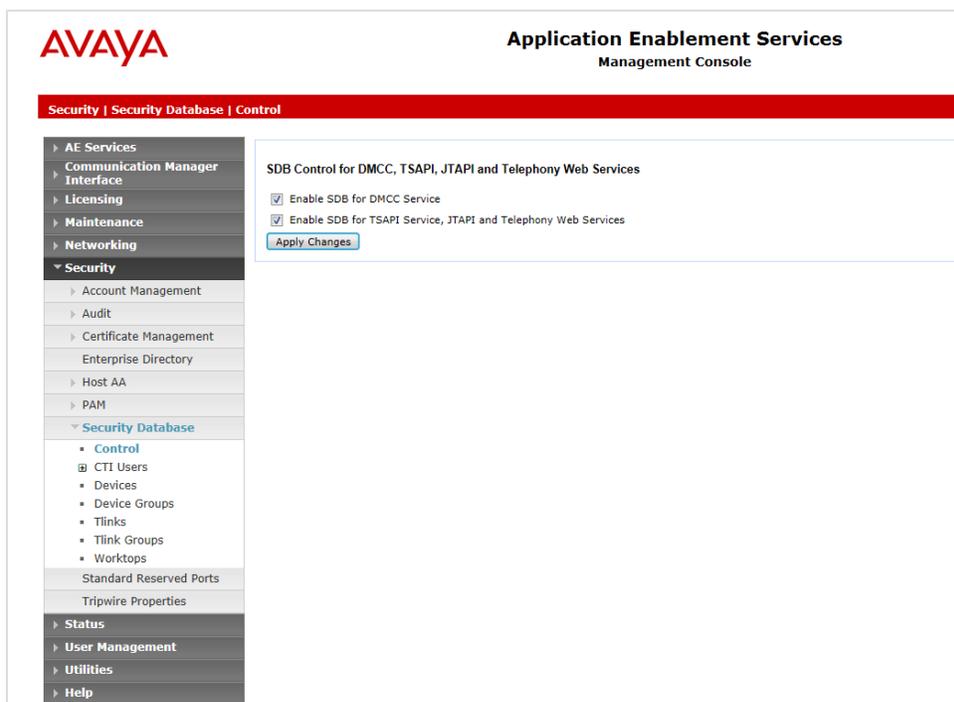


Figure 71: Enabling the Security Database

1. Select the **Enable SDB for DMCC Service** checkbox.
Select the **Enable SDB TSAPI Service, JTAPI and Telephony Service** checkbox.
2. Click **Apply Changes**.

Finding out What the Alias for the Switch Is

On the AES Management Console navigate to **Communication Manager Interface > Switch Connections**.

The **Switch Connections** page displays.

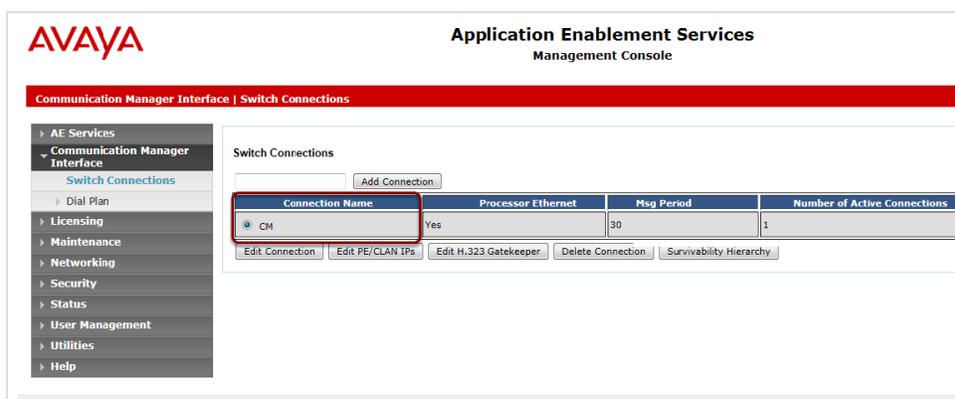


Figure 72: Switch Connections

The Alias for the switch is in the **Connection Name** field.

Setting the IP Address for the H.323 Gatekeeper

On the AES Management Console navigate to **Communication Manager Interface >Switch Connections**.

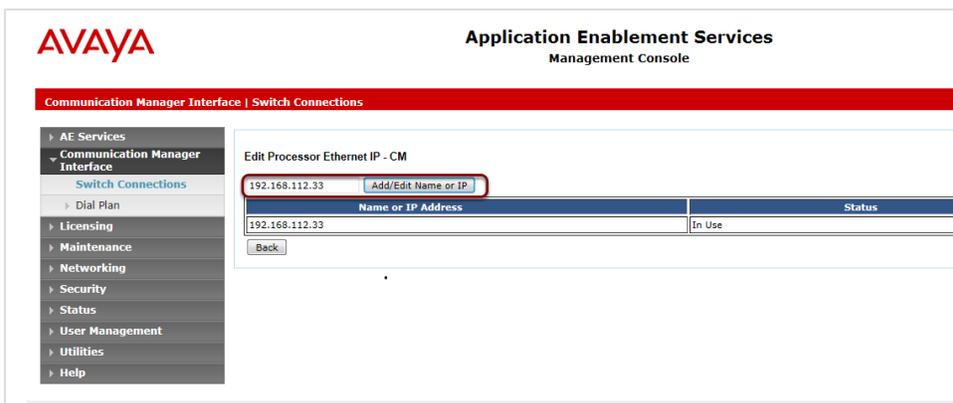


Figure 73: Editing Processor Ethernet IP- CIM

Add a Name or IP Address.

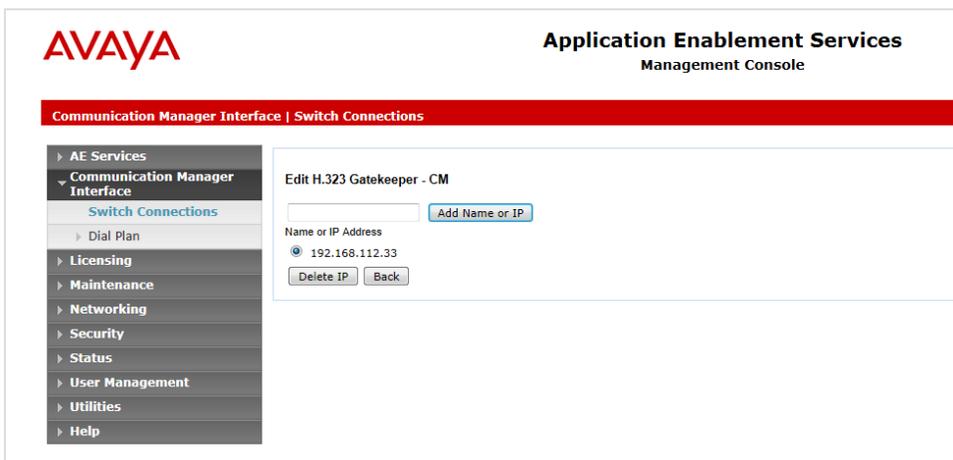


Figure 74: H.323 Gatekeeper

Finding out the Tlink Name

On the AES Management Console navigate to **Security > Security Database > Tlinks**.

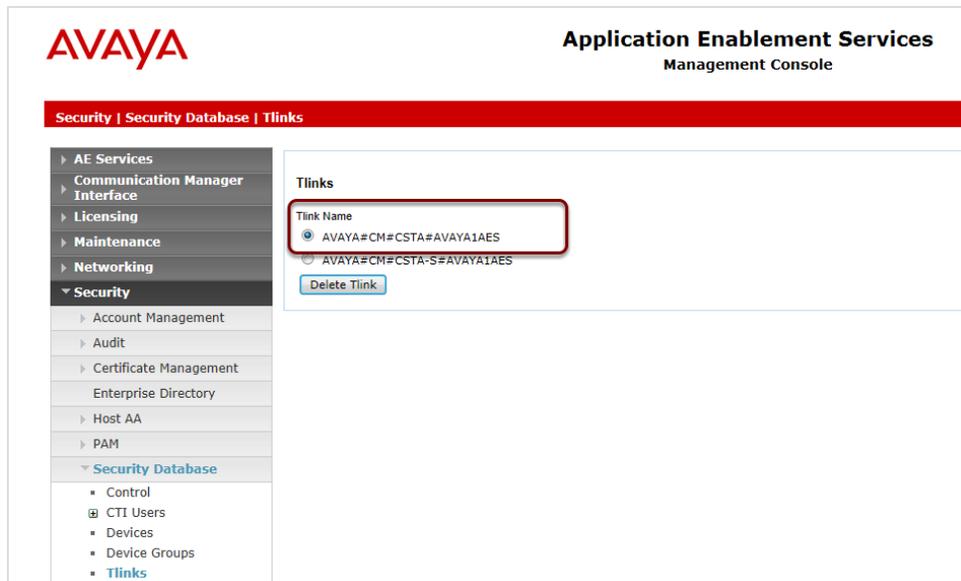


Figure 75: Finding out the Tlink Name

Configuring Recorders

This chapter describes how to configure connection settings for all recorder servers in the **Recorders** tab.

This chapter contains the following sections:

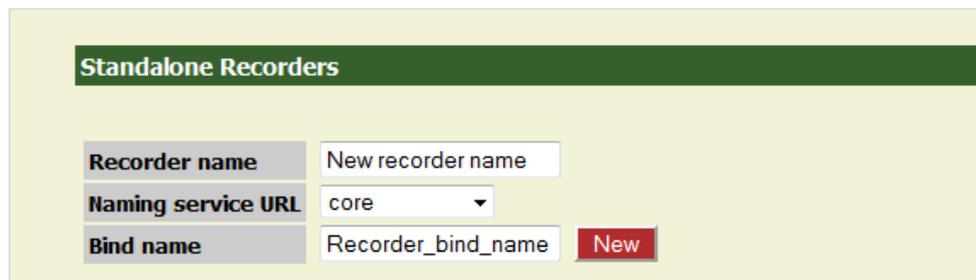
[Configuring Standalone Recorders](#)

[Adding and Configuring Recorder Groups](#)

[High Availability](#)

Configuring Standalone Recorders

Navigate to **Settings > Configuration > Recorders > Standalone Recorders**.



The screenshot shows a web interface for configuring standalone recorders. At the top, there is a dark green header with the text "Standalone Recorders". Below the header, there are three input fields and a button. The first field is labeled "Recorder name" and contains the text "New recorder name". The second field is labeled "Naming service URL" and is a dropdown menu with "core" selected. The third field is labeled "Bind name" and contains the text "Recorder_bind_name". To the right of the "Bind name" field is a red button with the text "New".

Figure 76: Adding a Recorder Group

To add a standalone recorder:

1. Type a unique **Recorder name**.
2. Select the server running RMI from the **Naming service URL** drop down list.
3. Enter the **Bind name** for the Recorder server.
4. Click **New**. The new Recorder server is added.
5. Click **Save Configuration**.

Adding and Configuring Recorder Groups

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



The screenshot shows the 'Recorder Groups' configuration page. 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' and 'Group load balancing method'. The 'Group name' field contains the text 'Recorders Group 1'. The 'Group load balancing method' is a dropdown menu currently set to 'Broadcast'. To the right of these fields is a red 'New' button.

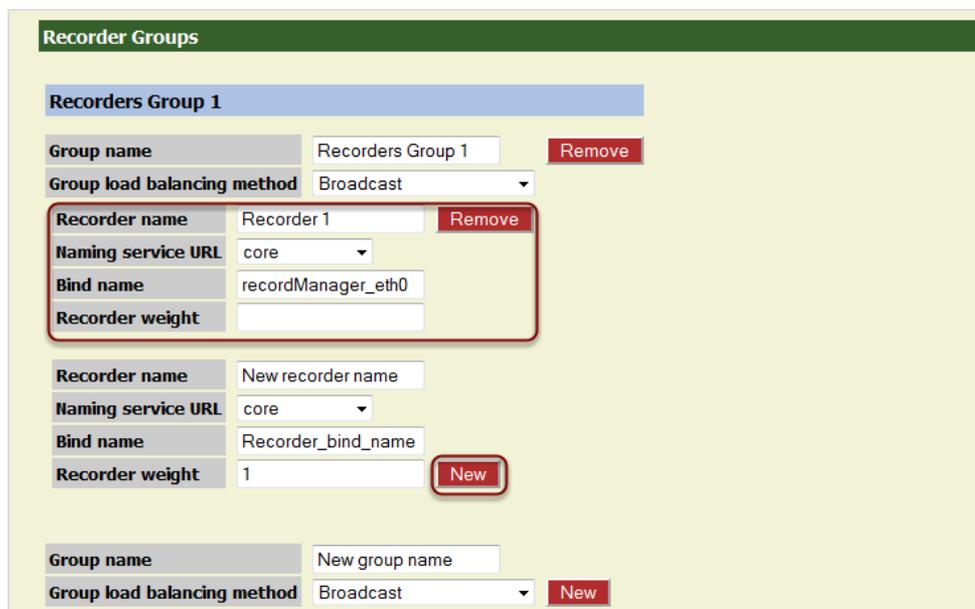
Figure 77: Adding a Recorder Group

To add a **Recorder Group**:

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

The default **Group load balancing method** is **Broadcast**. Do not change the **Group load balancing method** unless Cisco SPAN based recording is used.

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



The screenshot shows the 'Recorder Groups' configuration page with 'Recorders Group 1' selected. The page has a green header with 'Recorder Groups'. Below it, a blue header identifies the selected group as 'Recorders Group 1'. The configuration for this group includes: 'Group name' (Recorders Group 1) with a 'Remove' button; 'Group load balancing method' (Broadcast) with a dropdown arrow; and a list of recorders. The first recorder is 'Recorder 1' with a 'Remove' button. Its configuration includes: 'Naming service URL' (core) with a dropdown arrow; 'Bind name' (recordManager_eth0); and 'Recorder weight' (empty field). Below this, there is a form for adding a new recorder with fields for 'Recorder name' (New recorder name), 'Naming service URL' (core) with a dropdown arrow, 'Bind name' (Recorder_bind_name), and 'Recorder weight' (1), followed by a 'New' button. At the bottom, there is a form for adding a new group with fields for 'Group name' (New group name) and 'Group load balancing method' (Broadcast) with a dropdown arrow, followed by a 'New' button.

Figure 78: Recorder Groups

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

2. Select the **Naming service URL** from the drop-down list. The server must be specified in **Settings > Call Recording Core > Servers**. For Avaya each Recorder must be in a different server and therefore have in its own IP address. Multiple Recorders on the same IP Address are not supported.
3. Type the RMI **Bind name**. This may be a non empty string.

The **Recorder weight** only applies to SPAN based recording where a Group load balancing method. If three recorder groups, each with a **Recorder weight** of one then each recorder group records a third of the calls. If one recorder group has a recorder weight of two and the others have recorder weights of one each then the recorder with a **Recorder weight** of two records 50% of the calls and the others with a **Recorder weight** of one records 25% each.

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 before these settings take effect. If there are further tasks to configure that require a restart of Call Recording, wait until these are completed before doing so.

The API Section Recorder of Server Communicator

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

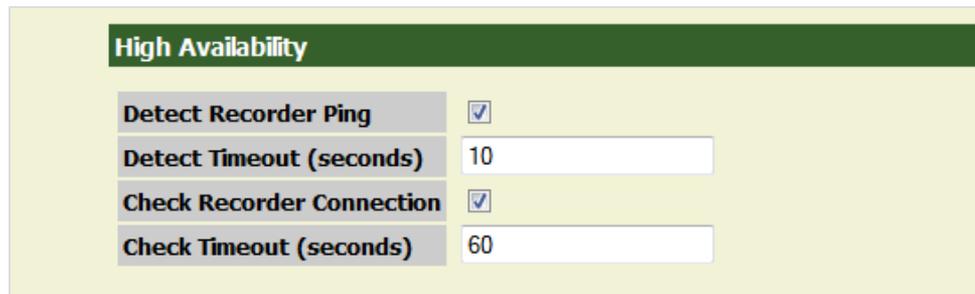
API	
Proxy port start	4000
Proxy port end	5000
Datagrams port start	37000
Datagrams port end	37100

Figure 79: The API Section Recorder of Server Communicator

The API section is used for specific configurations, and in most cases does not need to be changed. Consult the Genesys Support team for more information at <http://genesyslab.com/support/contact>

High Availability

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



High Availability	
Detect Recorder Ping	<input checked="" type="checkbox"/>
Detect Timeout (seconds)	10
Check Recorder Connection	<input checked="" type="checkbox"/>
Check Timeout (seconds)	60

Figure 80: High Availability

Select the **Detect Recorder Ping** checkbox. The Recorder ping occurs every five seconds while the recorder is recording.

Set a timeout in seconds. The default timeout is two pings or ten seconds. Do not set a timeout of less than ten seconds.

Select the **Check Recorder Connection** checkbox. The **Check Recorder Connection** monitors the recorder even when it is in idle mode.

The **Check Timeout (seconds)** default is 60 seconds.

Configuring Decoders

This chapter describes how to identify the decoder servers and configure decoding parameters in the **Decoders** tab.

This chapter contains the following sections:

[Configuring Decoder1](#)

[Adding a New Decoder Server](#)

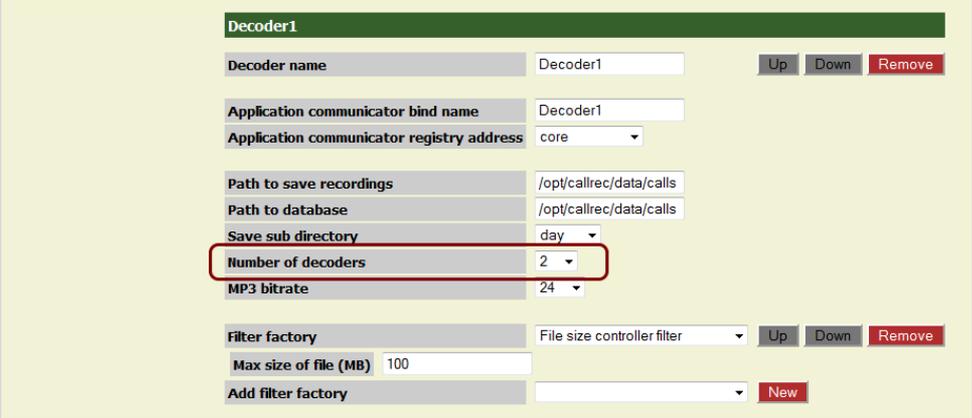
[Changing Audio Gain Settings for the Decoder](#)

[Configuring Decoder Server Communicator](#)

Configuring Decoder1

Navigate to **Settings > Configuration > Decoders > Decoder Servers Configuration**.

By default on a single server installation Call Recording has one decoder with two decoder processes running. In installations with a lot of concurrent calls, two decoder processes may not be sufficient leading to extended waiting times to play the media. It is possible to add new decoding processes.



The screenshot shows the configuration page for 'Decoder1'. The interface includes several input fields and buttons. The 'Number of decoders' field is highlighted with a red box. The 'Filter factory' section includes a dropdown menu, a 'Max size of file (MB)' input field, and an 'Add filter factory' button.

Decoder1		
Decoder name	Decoder1	Up Down Remove
Application communicator bind name	Decoder1	
Application communicator registry address	core	
Path to save recordings	/opt/callrec/data/calls	
Path to database	/opt/callrec/data/calls	
Save sub directory	day	
Number of decoders	2	
MP3 bitrate	24	
Filter factory	File size controller filter	Up Down Remove
Max size of file (MB)	100	
Add filter factory		New

Figure 81: Decoder 1

To add decoder processes:

1. Increase the value of the **Number of decoders** in **Decoder1**. This value must always be less than the number of available CPUs on the server.
2. Click **Save Configuration** to save the new Decoder server settings.

Additional Parameters for Decoder1

In addition to the parameters below for a new decoder, **Decoder1** has extra parameters, enabling you to define a **Filter Factory**. There are two filters included in a default Call Recording installation, available in the **Filter factory** drop down list:

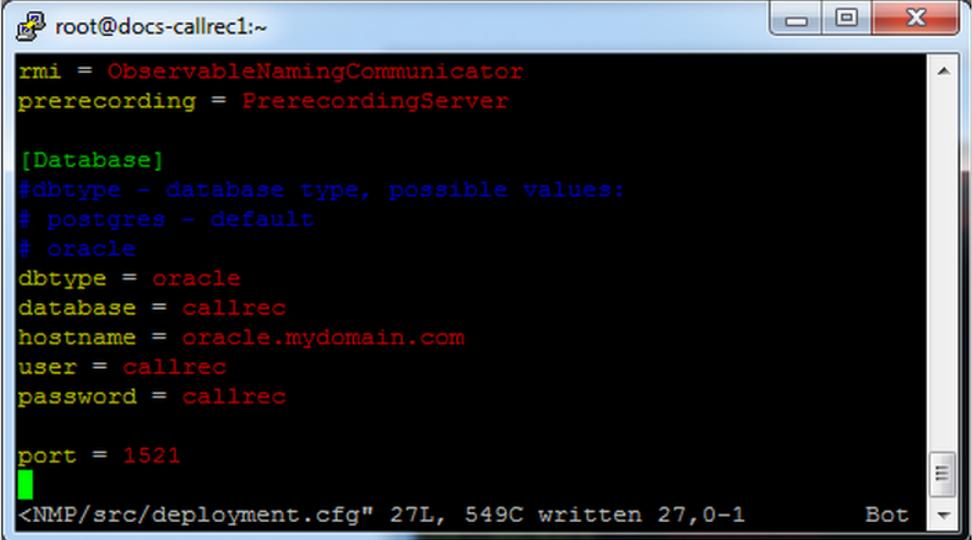
File size controller: This filter must define a **Max size of file**, in megabytes, the maximum size of created files. If the file size is larger, it is split into multiple files.

Blowfish ciphering filter: When you select this filter, you are asked for the **Path to key file** – the path where the ciphering key is stored. Please note that the key size is limited to 16 bytes. It is possible to use any random string with a maximum of 16 characters.

Adding a New Decoder Server

In multi server installations it is possible to have decoders on more than one server. If there are sufficient concurrent calls then the installation may even require a dedicated server for decoding. In either case add a new decoder server.

To add a new decoder server:



```

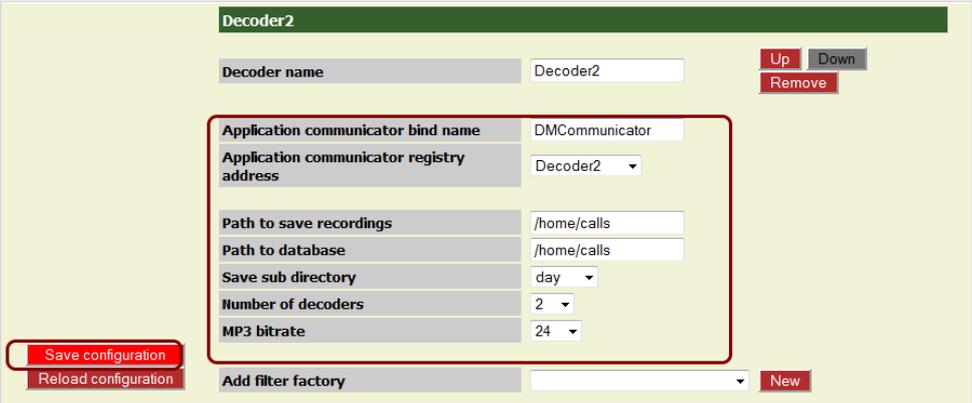
root@docs-callrec1:~
rmi = ObservableNamingCommunicator
prerecording = PrerecordingServer

[Database]
#dbtype - database type, possible values:
# postgres - default
# oracle
dbtype = oracle
database = callrec
hostname = oracle.mydomain.com
user = callrec
password = callrec

port = 1521
<NMP/src/deployment.cfg" 27L, 549C written 27,0-1
  
```

Figure 82: Adding a Decoder

1. Scroll down to the **Add new decoder** form.
2. Click **New** to create a form for the new decoder.
3. Type a unique **Decoder name**: for the new decoder server, for example, Decoder2.
4. Click the **Application communicator bind name** field and the name of the new decoder server updates.



Decoder2

Decoder name: Decoder2 Up Down Remove

Application communicator bind name: DMCommunicator

Application communicator registry address: Decoder2

Path to save recordings: /home/calls

Path to database: /home/calls

Save sub directory: day

Number of decoders: 2

MP3 bitrate: 24

Save configuration Reload configuration Add filter factory New

Figure 83: Decoder2

5. Enter the following parameters:
 - **Application communicator bind name**: This is the RMI bind name for the selected decoder. This must be the same for all decoders; for example,

DMCommunicator.

- **Application communicator registry address:** This is the server that this decoder runs on, for example, `Decoder2`. Select the server from the drop-down list. These are defined in **Settings > Call Recording Core > Servers**.
 - **Path to save recordings :** This is the Path for storing recorded files – the local path on the server selected in the **Application communicator registry address** drop down list.
 - **Path to database:** This is the media file path stored in the database the local path on the server selected in the **Application communicator registry address** drop down list.
 - **Save sub directory:** This is the time interval selected for the creation of unique subdirectories – if **day** is selected, a new subdirectory is created every 24 hours. The subdirectory name is generated as a timestamp, for example, 20100424.
 - **Number of decoders :** This is the number of decoder processes on this server. The default number is two processes, increase the number if necessary. This value must always be less than the number of available CPUs on the server.
 - **Time to destroy decoder:** Timeout in seconds. If a decoder stops responding within the time of this interval, the connection is terminated and reinitiated.
 - **MP3 bitrate :** The quality of recorded audio if you are using the MP3 codec. The bitrate can be selected from **16 – 128** kbps, where 8 kbps is the lowest quality and 128 kbps is the highest. The default value is **24** kbps.
6. Click **Save Configuration** to save the new Decoder server settings.

Audio Quality settings

By default Call Recording stores all decoded calls as MP3 files with a 24 kbps bitrate. You can also choose uncompressed WAV. Change the quality settings to minimize storage space, or maximize audio quality.

MP3 Codex Quality Settings:

Bitrate (kbps)	Storage Space for 1 min (MB)
16	0,11
24	0,17
32	0,23
40	0,29
48	0,34
56	0,4
64	0,46
80	0,57
96	0,69
112	0,8
128	0,92

Table 9: MP3 Quality and Bit Rate

Important:

The following are known limitations of the decoder:

- WAV files are uncompressed in the Call Recording system, and the bit rate cannot be adjusted.
 - The decoder server requires both streams to be in the same payload or codec, otherwise the decoder cannot process the voice data. For example, if one channel is encoded by the G.711 codec and other by G.729, decoding of the call fails.
-

Changing Audio Gain Settings for the Decoder

If the volume of the MP3 files is too loud or too quiet, it is possible to change the gain that the decoder produces for new files.

The parameter for mp3 gain change is in `decoders.xml` in

```
<SpecifiedConfiguration name="decoders"> <EqualGroup
name="decoder" egName="Decoder1"> <Group
name="decoderSetting"> <Value
name="mp3gainChange">0</Value>.
```

If the value is not present then the default value is 0, this is normal gain. One step in value equals + or - 1.5dB. To double the volume of the mp3 use a value of 4 (+ 6dB). The value can be between -128 and 127. Only new files are affected.

Configuring Decoder Server Communicator

Navigate to **Settings > Configuration > Decoders > Decoder Servers Configuration**.

The screenshot shows the configuration page for the Decoder Server Communicator. On the left, there is a sidebar with two items: 'Decoder Servers Configuration' and 'Decoder Server Communicator'. The main content area has a red header 'Decoder Server Communicator'. Below the header, there is a 'Keep source files' checkbox which is currently unchecked. Underneath, there are two sections: 'File type preference' and 'Email type preference', both with green headers. Each section contains three rows of options: 'mp3', 'zip', and 'wave'. Each row has a checkbox, the format name, and 'Up' and 'Down' buttons. In the 'File type preference' section, 'mp3' and 'zip' are checked, while 'wave' is not. In the 'Email type preference' section, 'mp3' and 'zip' are checked, while 'wave' is not.

Figure 84: Decoder Server Communicator Settings

Select or deselect the file types in **File type preference** and **Email type preference**.

The **Decoder Server Communicator** settings specify the decoder registry address, for example, the RMI bind path, and determine the format for saving audio files and sending them via email. If the first format is unavailable, the second is used. Use the **Up** and **Down** buttons to change the order.

- **mp3**: default storage format
- **zip**: compressed into a zip file (according to primary audio format)
Note: ZIP cannot be selected as the primary format.
- **wave**: uncompressed WAV audio

If a format is deselected, this file type is not available.

Important:

The Store source files option is only for testing. If this option is selected, both raw and compressed recordings are stored on the decoder server, consuming a large amount of disk space.

Configuring the Web UI

This chapter describes how to configure the web based user interface.

This chapter contains the following sections:

[Configuring the User Interface](#)

[Configuring Database and User Interface settings](#)

[Configuring Passwords](#)

[Enabling LDAP Authentication](#)

[LDAP User Account](#)

[Configuring the LDAP Server Settings](#)

[Configuring Group Filtering](#)

[Backup LDAP Server](#)

[Adding LDAP users](#)

[Importing LDAP users](#)

[Setting up Advanced Searches](#)

[Creating an Advanced Search with External Data](#)

[Customizing Columns Setup](#)

Configuring the User Interface

Navigate to **Settings > Configuration > Web UI > Web Interface**.

The screenshot shows the 'User Interface Configuration' page. On the left is a sidebar with 'Web Interface' selected, and other options like 'LDAP', 'Search', and 'Columns setup'. The main content area is divided into several sections:

- Database Setting:** Pool name is set to 'callrec'. A note indicates this change will be loaded after tomcat restart.
- User Interface View Setting:** Includes checkboxes for 'Prerecording pin view', 'LDAP authentication', and 'Cut SIP number' (all checked). Other settings include 'Mask export file', 'Max search days' (31), 'Disable on demand video encoding' (unchecked), 'Export Size (in MB)' (50), and 'Force CRC Checks' (checked).
- Application Communicator:** Bind name is 'GUI_CallREC' and Registry address is 'core'. A note indicates this change will be loaded after tomcat restart.
- Media Restore:** Restore expiration time (Days) is set to 2.
- Core server:** Choose core server is set to 'core'.
- Mixer server:** Choose mixer server is set to 'core'.
- Filter factory:** Add new filter factory is set to 'New'.
- Recording Rules which are NOT listed in Recording rules tab:** Add rule to invisible list is set to 'PHONE' with a 'New' button.

At the bottom left of the main content area, there are two buttons: 'Save configuration' and 'Reload configuration'.

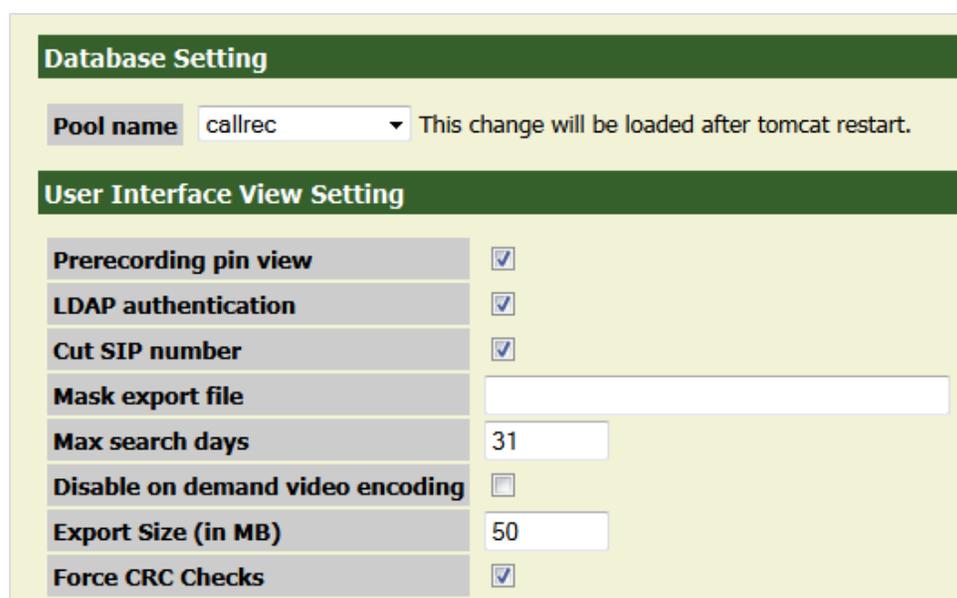
Figure 85: Web Interface Configuration

Call Recording enables the ability to set the levels of access and views for users. The **User Interface Configuration** screen controls these settings.

Configuring Database and User Interface settings

Navigate to **Settings > Configuration > Web UI > Web Interface** and scroll down.

Do not change the **Pool name** unless absolutely necessary. The default is “callrec”.



The screenshot shows a configuration page with two main sections. The first section, titled "Database Setting", contains a "Pool name" dropdown menu set to "callrec" and a note: "This change will be loaded after tomcat restart." The second section, titled "User Interface View Setting", contains a list of settings:

Setting	Value
Prerecording pin view	<input checked="" type="checkbox"/>
LDAP authentication	<input checked="" type="checkbox"/>
Cut SIP number	<input checked="" type="checkbox"/>
Mask export file	<input type="text"/>
Max search days	31
Disable on demand video encoding	<input type="checkbox"/>
Export Size (in MB)	50
Force CRC Checks	<input checked="" type="checkbox"/>

Figure 86: DB and User Interface View Settings

The **Pool name** drop down list displays all database pools defined on the **Database** tab. To view the database pools navigate to **Settings > Call Recording Core > Database**. The **Pool name** must be the primary pool where all call related data are stored.

User Interface View Settings

Determines which information and functions display in the user interface:

- **Prerecording pin view:** display pre-recorded calls with a special icon that looks like a pin.
- **LDAP authentication:** use LDAP to authenticate users. This feature requires additional configuration. Go to the Web UI tab and click the LDAP button.

- **Cut SIP number:** truncates the SIP information for caller and called number, storing it in the database in a simplified format.
- **Mask export file:** sets the template for naming exported data files. Examples are:
 - \$date\$ - date in format YYYYmmdd
 - \$time\$ - start of call in format hhmm
 - \$phone_from\$ - caller number
 - \$phone_to\$ - calling number
 - \$id_db\$ - database id couple

Max search days: maximum size of the range between the From and To date call search parameters. Default is 31, around 1 month. Max: 2999, around 7 years range. Higher numbers cause a large decrease in search performance; if search is slow, reduce this value to 31 or less.

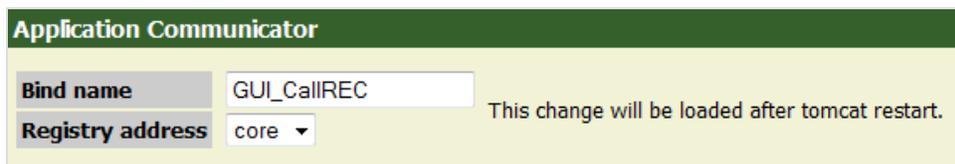
Disable on demand video encoding: check this option to prevent GUI users from running the Media Encoder on demand for un-encoded screen recordings. If this feature is disabled, then the Media Encoder still works in batch mode, improving overall performance.

Export Size (in MB): for customers that want to export large amounts of records at one time. This is configurable from 10 to 2000 MB. The default value is 50 MB.

Force CRC Checks: forces all media files to be CRC-checked before being played by a user. If a file fails a check, an alert displays and the file does not play. Note that files from older Call Recording versions may not have a correctly calculated CRC value, therefore this option is off by default.

Application Communicator

Navigate to **Settings > Configuration > Web UI > Web Interface** and scroll down.



Application Communicator	
Bind name	GUI_CallREC
Registry address	core ▼

This change will be loaded after tomcat restart.

Figure 87: Application Communicator Settings

The **Application Communicator** contains RMI bind options. Changing the **Bind name** or **Registry address** requires a restart of the web server.

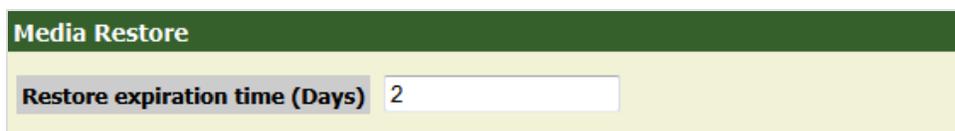
- **Bind name:** unique name for binding to RMI service.
- **Registry address:** where the RMI service is running. The drop down list displays the servers defined in the Call Recording Core tab.

Media Restore

Navigate to **Settings > Configuration > Web UI > Web Interface** and scroll down.

Media Restore sets, in days, the length of time restored calls are available to users. After this time period, the calls are removed from the **Restored calls** list, and the disk space is cleared, though calls can be restored again.

- Type the number of days to retain stored calls. Default is 2.



Media Restore	
Restore expiration time (Days)	2

Figure 88: Media Restore Settings

Core server

Navigate to **Settings > Configuration > Web UI > Web Interface** and scroll down.



Figure 89: Core Server Settings

- Choose core server: enables change of the Call Recording core server in multi-server environments. Servers are defined in the Call Recording Core tab.

Filter factory

Navigate to **Settings > Configuration > Web UI > Web Interface** and scroll down.

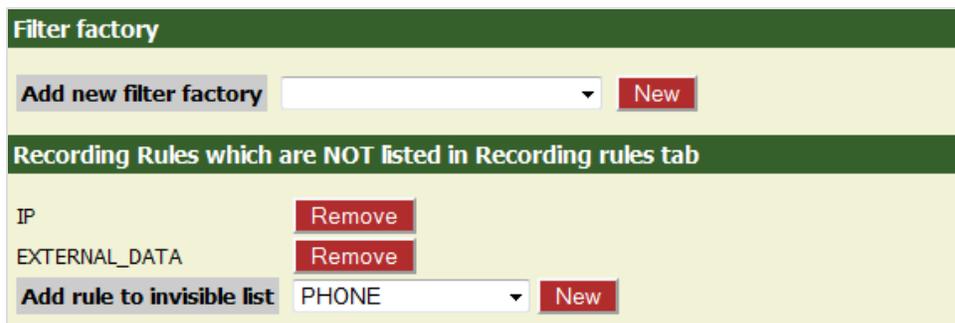


Figure 90: Filter Factory Settings

The **Filter factory** enables predefined settings for filters that are used by all users of the system, such as encryption. These filters are for read-only data.

- Use Up and Down to change filter order.
- To delete a filter click **Remove**.

Recording Rules that are not listed in the recording rules tab

This Invisible list of rules restricts the recording rules that are available to users. Calls excluded by the invisible rule list are no longer available to any users of the system.

This does not affect pre-existing rules.

Configuring Passwords

Navigate to **Settings > Configuration > Web UI > Web Interface**, and scroll down.

Password configuration	
Minimum characters	<input type="text" value="0"/>
Minimum lowercase characters	<input type="text" value="0"/>
Minimum capital characters	<input type="text" value="0"/>
Minimum numbers	<input type="text" value="0"/>
Minimum non alphanumeric characters	<input type="text" value="0"/>
Count of different recent passwords	<input type="text" value="4"/>
Password lifetime in days	<input type="text" value="90"/>
Unsuccessful logins before lockout	<input type="text" value="3"/>
Time for which account is blocked (minutes)	<input type="text" value="30"/>

Figure 91: Password configuration

One of the most important sections on this configuration tab is **Password configuration**. The security of the Call Recording system can be improved, or alternatively degraded, by the settings here. For a secure password policy, specify values for the following settings:

Setting	Description	Values
Minimum characters	The password must contain at least this number of characters of this type	Recommended: strong passwords have at least 8 characters, formed from a mixture of three types of characters (for example lowercase, capital letters, and numbers)
Minimum lowercase characters		
Minimum capital letters		

Setting	Description	Values
Minimum numbers		
Minimum non alphanumeric characters		
Count of different recent passwords	How many times a password must be changed before the same password can be used again	Recommended: at least 4
Password lifetime in days	Number of days before a password has to be changed	Must be between 1 and 365 days (recommended: 90 days)
Unsuccessful logins before lockout	How many times a wrong password can be entered at login before the account is blocked (must be unlocked by an administrator)	Recommended: 3 (must be between 2 and 10)
Time for which account is blocked (minutes)	Length of time an account remains blocked before automatically unblocking without administrator intervention	Must be between 1 and 65535 minutes (about 45.5 days)

Table 10: Password Properties

Enabling LDAP Authentication

Enable **LDAP authentication** before configuring the settings in LDAP Configuration.

Navigate to **Settings > Configuration > Web UI > Web Interface > User Interface View Settings**.

The screenshot shows the 'User Interface Configuration' page. On the left, a navigation menu is visible with options: 'Web Interface' (selected), 'LDAP', 'Search', and 'Columns setup'. The main content area is titled 'User Interface Configuration' and is divided into sections: 'Database Setting' and 'User Interface View Setting'. In the 'Database Setting' section, the 'Pool name' is set to 'callrec' with a note: 'This change will be loaded after tomcat restart.' The 'User Interface View Setting' section contains several settings:

Setting	Value
Prerecording pin view	<input checked="" type="checkbox"/>
LDAP authentication	<input checked="" type="checkbox"/>
Cut SIP number	<input checked="" type="checkbox"/>
Mask export file	<input type="text"/>
Max search days	31
Disable on demand video encoding	<input type="checkbox"/>
Export Size (in MB)	50
Force CRC Checks	<input checked="" type="checkbox"/>

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

Figure 92: Enable LDAP Authentication

1. Select the **LDAP authentication** checkbox.
2. Click **Save configuration**.

For more information concerning LDAP integration, configuration and maintenance contact Genesys Support at

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

LDAP User Account

Create a read-only user account in the LDAP Server to access the LDAP data.

This LDAP connection is only used to import the users into CallREC initially.

The information and credentials for this account are necessary to configure the LDAP Server Settings.

Configuring the LDAP Server Settings

Use **LDAP Configuration** to identify and enable one or more LDAP servers, and Group Filtering.

Navigate to **Settings > Configuration > Web UI > LLDAP > LDAP Server**.

LDAP server	
IP Address	ldap.mydomain.net
Port	389
Base DN	DC=mydomain,DC=net
Search Filter	Active Directory <input type="text" value="((objectClass=user)(objectClass=inetOrgPerson))!(objectClass=computer)"/>
User DN	callrecldap
Password	callrepasswd
Login Attribute	sAMAccountName
First Name Attribute	firstname
Last Name Attribute	name
Email Attribute	mail
Use LDAPS protocol	<input type="checkbox"/>

LDAP server address is critical for the correct functionality of the application. Change only if you know what you are doing.

Figure 93: LDAP ID

Configure all the settings according to the LDAP server configuration and click **Save configuration**.

- **IP Address:** IP address or hostname in full format, for example, ldap.mydomain.net instead of just ldap.

Important:

This is a critical configuration parameter and any changes lead to disabling LDAP authentication.

- **Port:** port number for connection with the LDAP server. By default 389.
- **Base DN:** tree root or particular branch of your domain. In standardized format used by LDAP, for example, DC=mydomain,DC=net.
- **Search Filter:** select a search filter from the drop-down list. The choices are Active Directory, Open LDAP or Custom LDAP. The field on the right hand side enables the filter to be modified.
- **User DN:** the user ID of the user account created in the LDAP Server for access to the LDAP database. This is case sensitive.

- **Password:** password of user account created in the LDAP Server for access to the LDAP database > This is case sensitive.
- **Login Attribute:** name of the LDAP key with user's login name.
- **First Name Attribute:** name of the LDAP key with user's first name.
- **Last Name Attribute:** name of the LDAP key with user's last name.
- **Email Attribute:** name of the LDAP key with user's email address.
- **Use LDAPS protocol:** enable the LDAP over SSL protocol.

Typical key values for Microsoft Active Directory are as follows:

First Name Attribute = `givenName`

Last Name Attribute = `sn`

Configuring Group Filtering

Navigate to **Settings > Configuration > Web UI > LLDAP > Group filtering**.



Group filtering	
Enable group filtering	<input type="checkbox"/>
Filtering attribute	memberOf
Group specification	CN=group.OU=Prague,I New
This server	Up Down Remove

Figure 94: Group Filtering

1. Click **New** to add additional filters.
2. Use the **Up** and **Down** buttons to change the order of multiple filters.
3. Select the **Enable group filtering** checkbox to enable group filtering.
 - **Filtering attribute:** name of LDAP key used for filtering, usually `memberOf` (contains user's groups).
 - **Group specification:** location (full path) of parameter in LDAP tree (e.g. Distinguished Name), in standardized format – for example `CN=group, OU=department, DC=mydomain, DC=net` where CN is Common Name, OU stands for Organization Unit and DC is Domain Component.

Example:

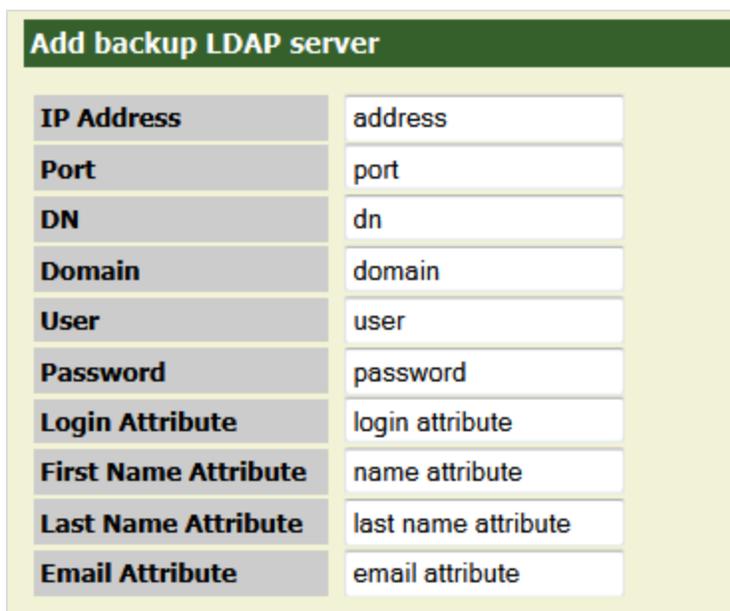
Only select staff from the Prague call center. The common name is Prague, that is part of the call center organization unit, so the Group specification is:
`CN=Prague, OU=callcenter, DC=mydomain, DC=net`

Backup LDAP Server

Navigate to **Settings > Configuration > Web UI > Web Interface** and scroll down.

To add or edit the configuration of a backup LDAP server, follow the same steps as Configuring Database and User Interface settings.

If the configuration of the backup LDAP is the same as the primary LDAP server, then use the same filtering rules. Otherwise, configure the filtering rules to correspond with the backup LDAP configuration.



The screenshot shows a web form titled "Add backup LDAP server" with a green header. The form contains ten rows, each with a label on the left and a text input field on the right. The labels and their corresponding input values are: IP Address (address), Port (port), DN (dn), Domain (domain), User (user), Password (password), Login Attribute (login attribute), First Name Attribute (name attribute), Last Name Attribute (last name attribute), and Email Attribute (email attribute).

Label	Input Value
IP Address	address
Port	port
DN	dn
Domain	domain
User	user
Password	password
Login Attribute	login attribute
First Name Attribute	name attribute
Last Name Attribute	last name attribute
Email Attribute	email attribute

Figure 95: Add Back up LDAP Server

After entering the parameters click **Save configuration**.

Adding LDAP users

When LDAP is configured correctly and the LDAP directory is running, import users, according to the entered criteria, into Call Recording. The import process adds only user names, emails, and passwords that are checked against the LDAP on every login. The following flowchart demonstrates the user authentication process.

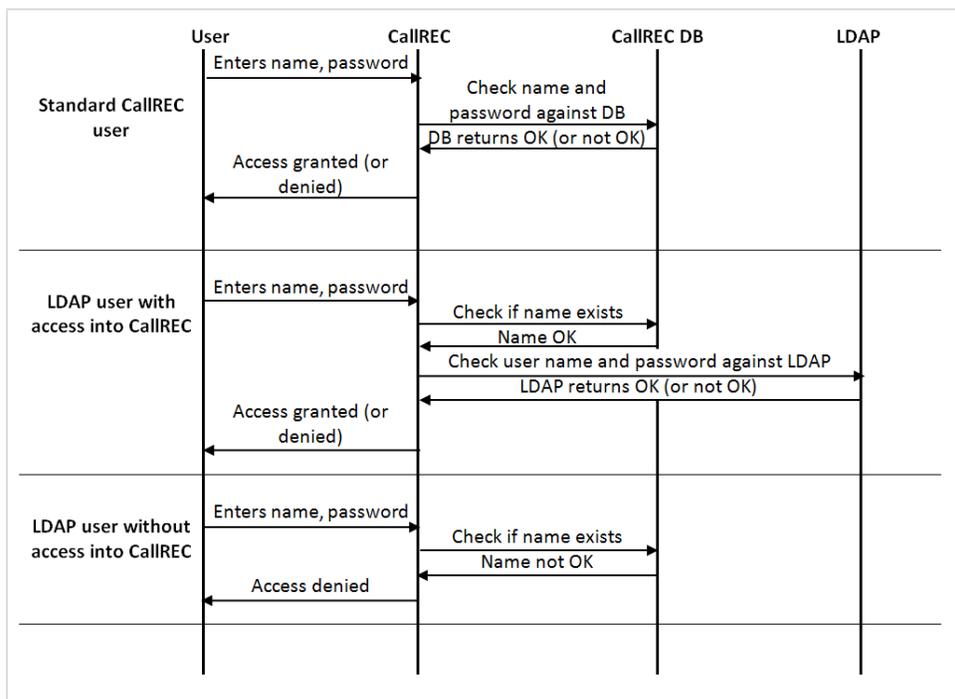


Figure 96: LDAP Add User Flow Chart

Importing LDAP users

To import users from LDAP, login as admin and navigate to **Users**. Select a group or create new group for all LDAP users, according to the defined group filter etc, and click **Insert new user**.



Figure 97: Insert New User Button in Users Tab

On the **Insert new user** page click **Insert from LDAP** and wait until the import finishes, a new dialog displays showing additional information about the import.

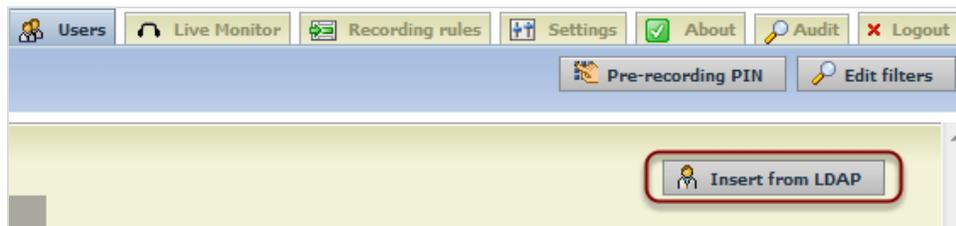


Figure 98: Insert from LDAP Button on Add User Page

In the **Insert LDAP user** list, all LDAP users that correspond with the criteria entered in the configuration and select users for import.

Insert LDAP user				
	Surname	Name	Login	E-mail
<input type="checkbox"/> Insert	 Akio Saico		 saico	
<input type="checkbox"/> Insert	 Ando Masahashi		 masahashi	
<input type="checkbox"/> Insert	 Fuji No Benitaka Go Suzuwa		 suzuwa	
<input type="checkbox"/> Insert	 Hidakaze Akenosow		 akenosow	
<input type="checkbox"/> Insert	 Hiro Nakamura		 h.nakamura	
<input type="checkbox"/> Insert	 Li-tin O've'Widle		 litin	
<input type="checkbox"/> Insert	 Manlötens Utokusii		 utokusii	
<input type="checkbox"/> Insert	 Mara-Shimas Kuni-Nishiki		 kuni	
<input type="checkbox"/> Insert	 Mara-Shima Timo		 timo	
<input type="checkbox"/> Insert	 Minimeadow Arko		 arko	
<input type="checkbox"/> Insert	 Minimeadow Kageboshi		 kageboshi	
<input type="checkbox"/> Insert	 Tengu No Ginryuu Go Hamamatsu		 tengu	
<input type="checkbox"/> Insert	 Tetsuyukime Daitaso		 te.daitaso	
<input type="checkbox"/> Insert	 Tsunechikara Daitaso		 t.daitaso	

Figure 99: LDAP Users List

Users are imported into the group currently open in Call Recording.

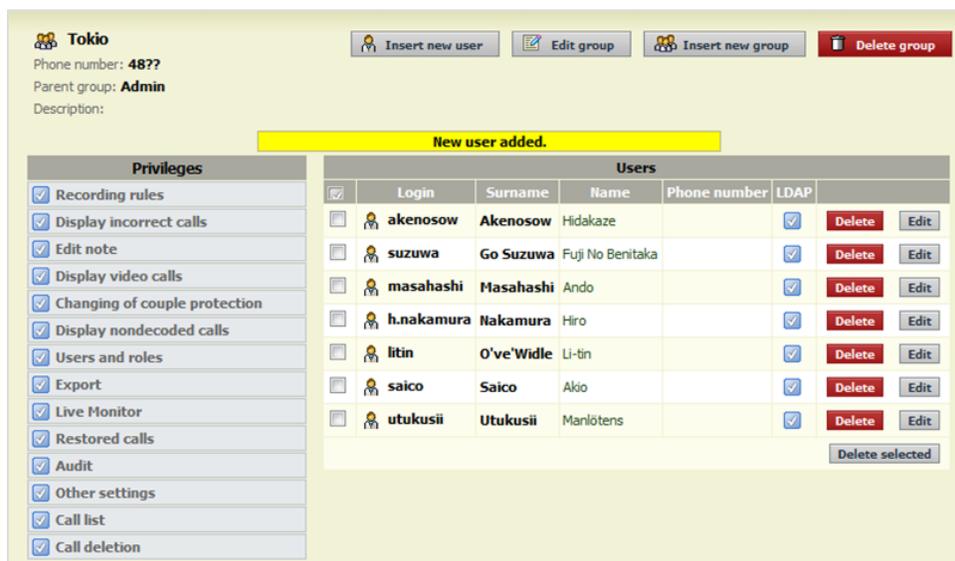


Figure 100: Newly Imported Users from LDAP

1. All imported users are marked with an LDAP user checkbox on their User details page. If the LDAP user checkbox is not selected, then the user is not authorized against LDAP and becomes a standard Call Recording user.
2. Editing of users details, except **Phone number:** and **Group:**, is disabled. Imported users also do not have an option to edit their passwords on this page because the password from LDAP directory is used. If a password change is required for this user, then change the password in LDAP.

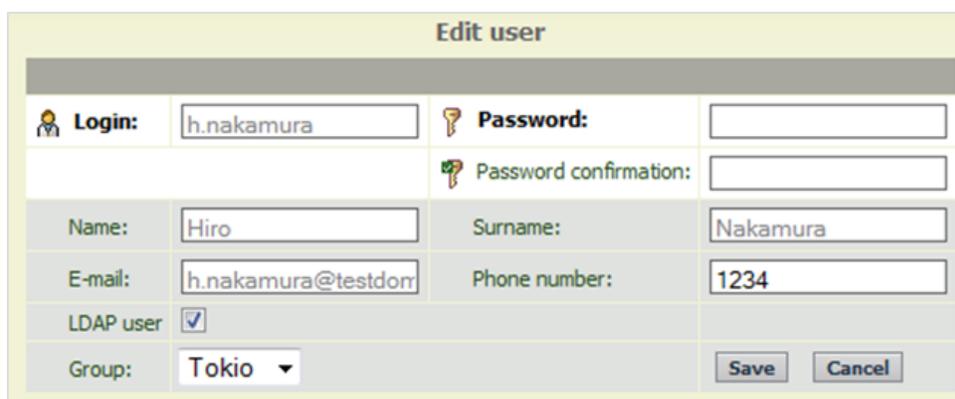


Figure 101: LDAP Imported User Detail

1. As final step of the LDAP import process enter the user's **Phone number:** in the **Edit user** dialog.
2. Click **Save**.

Setting up Advanced Searches

Navigate to **Settings > Configuration > Web UI > Search**.

Advanced Search

Currently are used 0 of 15 database columns.
Please, reload search frame (RMB - on search frame) or logout to see changes made in search frame.

Item key	Text	Type	Match	Sort
CallRecCalledURL	Called URL	AutoSelect	Equals	<input checked="" type="checkbox"/>
Used in #filters/#view restrictions: Not used.				
Up Down Remove				
CallRecCallingURL	Calling URL	AutoSelect	Equals	<input checked="" type="checkbox"/>
Used in #filters/#view restrictions: Not used.				
Up Down Remove				
CiscoCallManagerID	CCM ID	Input	Contains	<input type="checkbox"/>
Used in #filters/#view restrictions: Not used.				
Up Down Remove				
CallRecCalledURL	value		Equals	<input type="checkbox"/>
New				

Autogenerated options

Time of reloading daily at (0:00-23:59):

Figure 102: Advanced Search Definition

Up to 15 external data keys can be used as **Advanced Search** criteria. The **Advanced Search** functionality enables the user to set up and save common database searches, so that they are available to users in the web interface. The searches can be defined using any Call Recording external data, including data from Genesys Contact Center, or data records.

External data with at least one record in the Call Recording database can be searched for. Unused items are not listed in the **Item key** drop-down list. Item key drop-down lists are re-generated once per day and entered into **Autogenerated options**.

After making changes in **Advanced Search**, log out from the Call Recording web interface and log in again to see the changes. On large installations with many records the changes may take a few minutes to process, on smaller installations the changes should appear immediately after logging in.

Important:

Ensure that the server time comes from a reliable source (for example, UTC) and that it is correct if changing the **Time of reloading**. An incorrect server time may also affect the recording of calls.

Creating an Advanced Search with External Data

The values available for the search depend on the external databases. The following is a general description of the steps required for adding a new **Advanced Search**.

Navigate to **Settings > Configuration > WebUI > Search**.

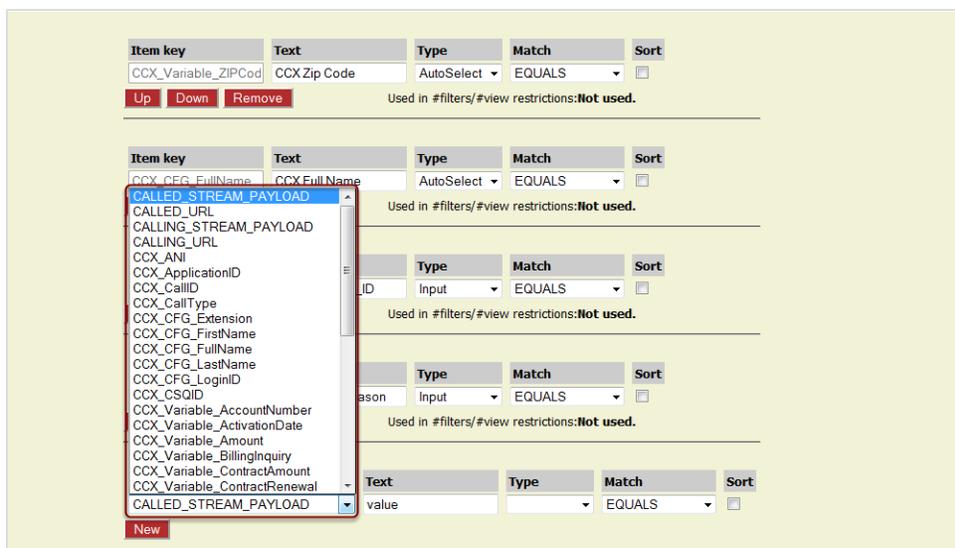


Figure 103: Selecting Data for Search Dropdown

Select an **Item key** from the drop-down list of available external data.

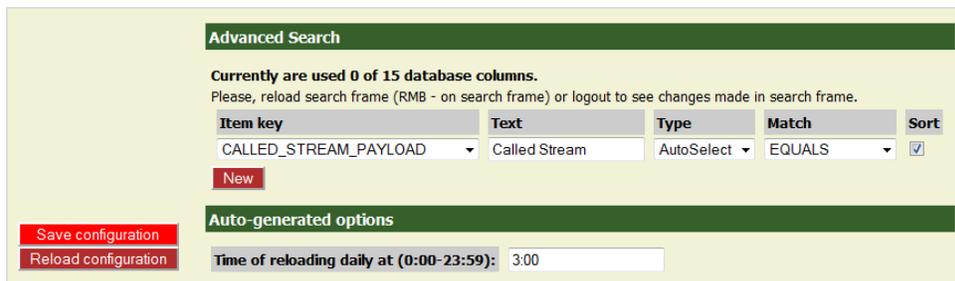


Figure 104: Advanced Search Showing Dropdown

1. Type a **Text** name for the search. This is the name that appears in the **Advanced Search**.
2. Select the **Type** of search from the drop-down list:

- Selecting **AutoSelect** creates a drop down menu with all existing values of selected Item.
This is recommended for items like agent's groups where there is only a few items in the list.
This is not recommended for items with lots of unique values, names, numbers etc.
- Selecting **Input** the user enters a value manually into the classic search text box. This can be used any search.
- Selecting **Select** and clicking **New** enables the search to be refined within the selected Item key by defining the values that can be searched for. See the drop-down menu in the figure Search with Call Type Advanced Search Added at the end of this section.
- The **Add all rows** dialog opens.

Advanced Search

Currently are used 1 of 15 database columns.
Please, reload search frame (RMB - on search frame) or logout to see changes made in search frame.

Item key	Text	Type	Match	Sort
CALLLED_STREAM_PA	Call Type	Select	EQUALS	<input type="checkbox"/>

Up Down Remove Used in #filters/#view restrictions: **Not used.**

Add all rows

Text	Enum value	Up	Down	Remove
Inbound Call	IN	Up	Down	Remove
Outbound Call	OUT	Up	Down	Remove
Internal Call	INT	Up	Down	Remove
text	value	New		

Figure 105: Add All Rows Dialog

1. In the **Text** field, type a description of the item.
2. In the **Enum value** field, type the value.
3. Click **New** to add the item to the list.
Repeat this for each item.

Item key	Text	Type	Match	Sort
CALLLED_STREAM_PAYLOAD	Called Stream	AutoSelect	EQUALS	<input type="checkbox"/>

New

Auto-generated options

Save configuration
Reload configuration

Time of reloading daily at (0:00-23:59): 3:00

Figure 106: Select Match Value

1. Select the **Match** value from the drop-down list.

- **Start or End:** item value found at start or end of match.
 - **Equals:** item value is an exact item match.
 - **Contains:** item value found in any location within an item.
2. Select **Sort** to present returned values alphabetically.
 3. Click **New**.
 4. Click **Save configuration** to save the search and make it available to users.
- Log out of Call Recording and back in again.

Navigate to **Recorded calls** and click **Search**. The Search filter dialog opens.

Search filter Close

Filters:

Choose filter: Choose filter Filter name:

All users

Calling numbers: and or Called numbers:

Description: Case sensitive: Type of call: All

Couples count: Random selection

Call length Min.: Max.: Locked only:

Calls with the same number from to or both which occurred more than

From: No filter To: No filter

March 2010 May 2012

Wk	Su	Mo	Tu	We	Th	Fr	Sa
9		1	2	3	4	5	6
10	7	8	9	10	11	12	13
11	14	15	16	17	18	19	20
12	21	22	23	24	25	26	27
13	28	29	30	31			
14							

3/6/10 12:00:00 AM Daily hours from:

Problem Status:
Just one stream recorded.
No stream recorded.
Unknown codec.

Condition connecting data above and below and or

Advanced search:
Condition between options displayed below and or

Case insensitive sensitive

CCX ANI: CCX Call Type:

CCX Login ID: CCX Account Number:

CCX Activation Date: CCX Service Type:

CCX Zip Code: CCX Full Name:
Insurance
Sales

JTAPI_CISCO_ID: Couple start reason:

Figure 107: Search with External Data

These fields display in the **Advanced search** area below standard searches. If the changes do not appear then reload the frame. To reload the frame, right click inside the **Search filter** dialog, select **This Frame** and then **Reload Frame**.

1. Select **and** or **or** in **Condition connecting data above and below**.
Selecting **and** means that the search only returns calls that satisfy both the

criteria in the top of the form and the **Advanced search** criteria.

Selecting **or** means that the search returns calls that satisfy one of the following:

- The criteria in the top of the form.
- The **Advanced search** criteria.
- Both.

2. Select **and** or **or** in **Condition between the options displayed below**.

Selecting **and** means that the search only returns calls that satisfy all the elected criteria in the **Advanced search** criteria.

Selecting **or** means that the search returns calls that satisfy one of the following:

- The criteria in the top of the form.
- The **Advanced search** criteria.

Select case **insensitive** if the data does not need to match the case in the external data selected or **sensitive** if it does need to match the case in the external data selected.

3. Depending on how each External data Key has been set up, type the criteria or Select from the drop-down lists for each Key to be searched for.

4. Click **Search**.

Important:

Due to the complexity of the links between configuration files, the database, and the Web interface, wait several seconds between saving the changes and reloading the frame to see the changes in effect.

Customizing Columns Setup

Columns setup controls the display of external data in the **Recorded calls** and **Restored calls** views in the Genesys Call Recording web interface. Each column that is added requires additional user screen space.

Adding a New Column

Navigate to **Settings > Configuration > Web UI > Columns setup**.

Figure 108: Columns Setup

1. Select the **Enable columns customization** checkbox. This checkbox affects all users. If this checkbox is not selected, then the customization is not applied and the new column does not display anywhere.
2. Select a **Key** from the drop-down list.
3. Type the **Label of column** to display in the header of the column.
4. Type the extended **Description** of the column, this is optional.
5. Click **New**.

Click **Save configuration** after adding the new columns.

- Use **Up** or **Down** to change the positions of the columns in the **Recorded calls** and **Restored calls** views.
- Click **Remove** to delete a column from the view.
- Click **Save configuration** after any adjustments.

To view the new column

Each user that must see the column must navigate to **Settings > Configuration > User Setup > Column Setup**.

Column name	Visible	Description
Date	<input checked="" type="checkbox"/>	
Call start time	<input checked="" type="checkbox"/>	
Call end time	<input type="checkbox"/>	
Length of call	<input type="checkbox"/>	
Calling number	<input checked="" type="checkbox"/>	
Called number	<input checked="" type="checkbox"/>	
Description	<input checked="" type="checkbox"/>	
Calling Stream	<input checked="" type="checkbox"/>	calling stream
Called URL	<input type="checkbox"/>	Called URL
Called Stream	<input type="checkbox"/>	Called Stream

Figure 109: User Column Setup

Select the checkboxes for the columns required. The columns apply to their **Recorded calls** and **Restored calls** views.

Chapter

13 Installing Screen Capture

This chapter covers the installation of the Screen Capture Server components, Capture Client and media player configuration.

This chapter contains the following sections:

[Screen Capture Server Components](#)

[Screen Capture Client](#)

Screen Capture Server Components

The Screen Capture server components, SRS, MUS, and SME are installed and enabled during GQM setup, if the **Screen Capture Service** and **Media Encoder Service** options are checked in the service list. This single server installation is suitable for small deployments; for larger, cluster, deployments a multi-server scenario is preferable.

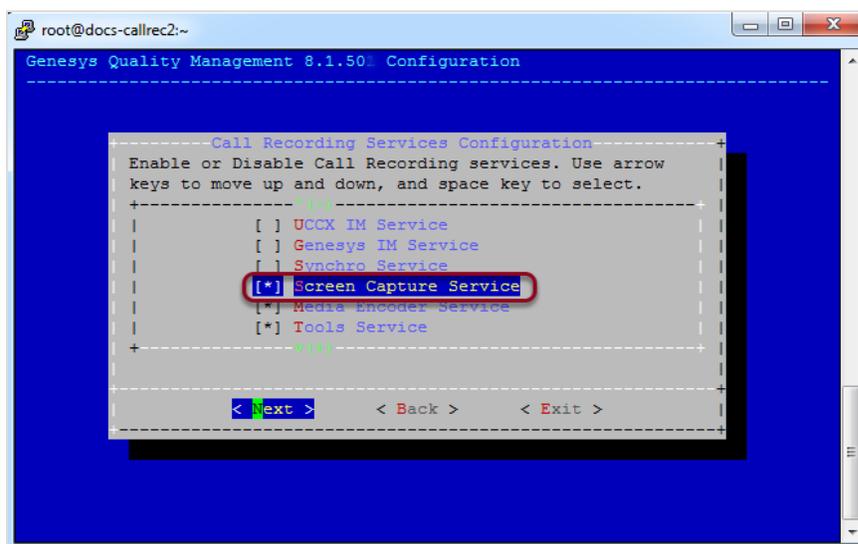


Figure 110: Screen Capture Services During GQM Setup

Important: Screen Capture Uploader Service

The `screenrec-uploader` service is a required part of the Screen Capture server-side installation. Although included as part of a new installation, this package is currently not installed during upgrade from GQM versions earlier than 8.0.47x. It must be installed manually after upgrade using the Linux RPM commands; refer to the RPM documentation for more information, or contact <http://genesyslab.com/support/contact>.

Screen Capture Client

The Screen Capture Client is a Windows screen recording client that, on execution, attempts to connect to a specified SRS server. If a server connection fails or disconnects and more than one server is specified, the SCC attempts to connect to the next server in the list, with a short pause between connection attempts. The client issues regular heartbeat messages to the current server during operation, to prevent timeouts and detect disconnections in a timely manner.

When a 'start recording' request is received from the SRS, screenshots are captured at intervals. This is specified in the **Recording Specifications** section of Screen Capture settings, split into tiles and sent in the intermediate `.rec` format to the *Media Upload Server*, until a 'stop recording' request is received. If an agent locks their screen while the capture client is capturing images, then the images do not display until the screen is unlocked.

The Capture Client can be deployed in two modes:

- **Service Slave Mode:** the Capture Client is installed together with the Client App Loader as a Windows Service, that runs in the background on the Agent PC. The Loader can multiplex messages between multiple running Capture Clients, such as in a Terminal Services environment, via Windows named pipes.
This mode is the standard operational mode, but requires access to the Windows Registry.
- **Standalone Mode:** the Capture Client is unpacked as a standalone executable, with no installation or access to the Windows Registry required (known as "zero-install"). This mode is provided for remote control of the Capture Client by an Agent Desktop. Information required by the Capture Client at startup is provided via command line parameters.

Service Slave Mode

The Capture Client Installer is deployed on each agent's desktop PC using a standard code-signed Windows installer file, that can be found at the following URL (where SERVER_URL is your main Call Recording URL):

```
http://SERVER_URL/callrec/plugins/screenrec-client-installer-8.0.490.msi.
```

Alternatively, it can be downloaded from the Call Recording Web GUI as follows:

Log in to the Call Recording Web GUI using any valid Call Recording account.

Navigate to **Settings > Configuration > User Setup > Plugins**.



Figure 111: Download Capture Client Installable

Click on the appropriate Screen Capture Client link to download the ~2MB installer file.

The standard Windows Installer package for Windows 7 must be used.

The Windows XP Installer version can be used for XP service pack 3 or Vista.

Capture Client Installation

Double click on the **Capture Client Installer** (.msi) file: The security warning dialog box displays.

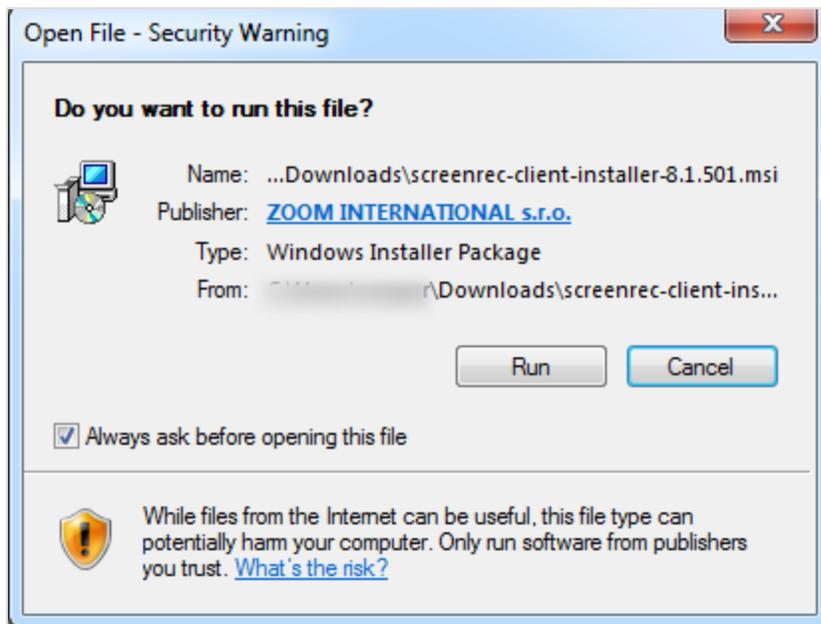


Figure 112: Security Warning

1. Click **Run**. The welcome dialog box displays.
2. On the welcome dialog box click **Next**. The server selection dialog box displays.

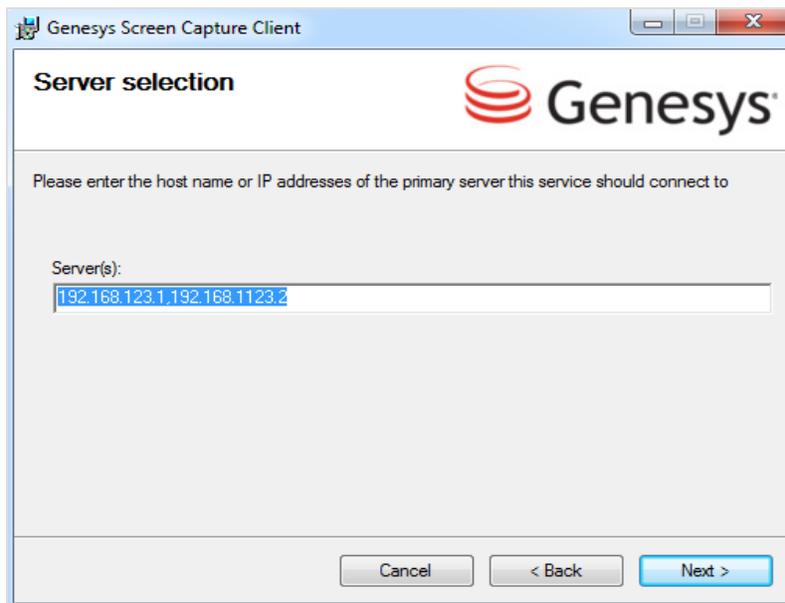


Figure 113: Server Selection

3. Enter one or more SRS server host addresses separated by a comma. There must not be a space. Click **Next**. The **Select Installation Folder** dialog box displays.



Figure 114: Selecting the Installation Folder

4. Click **Browse** and select the installation folder. Click **Next**. The **Confirm Installation** dialog displays.

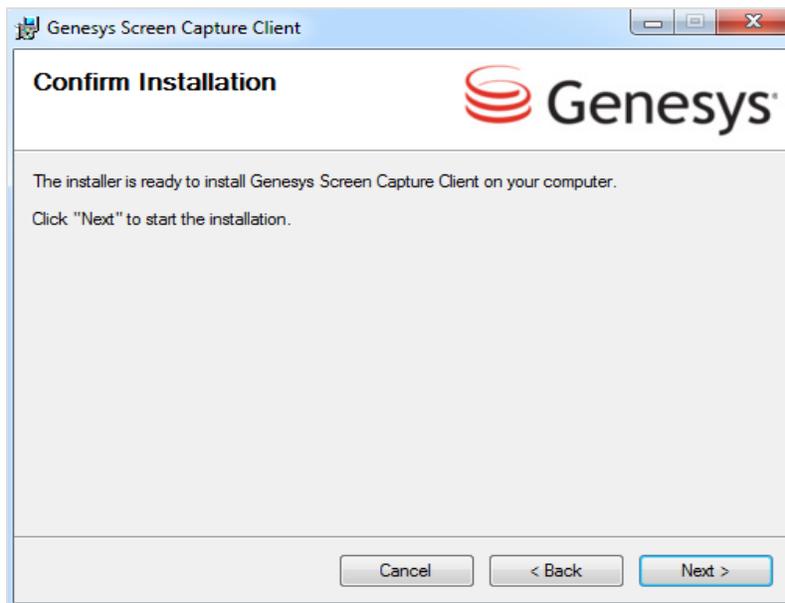


Figure 115: Confirming the Installation

5. Click **Next** to confirm the installation.

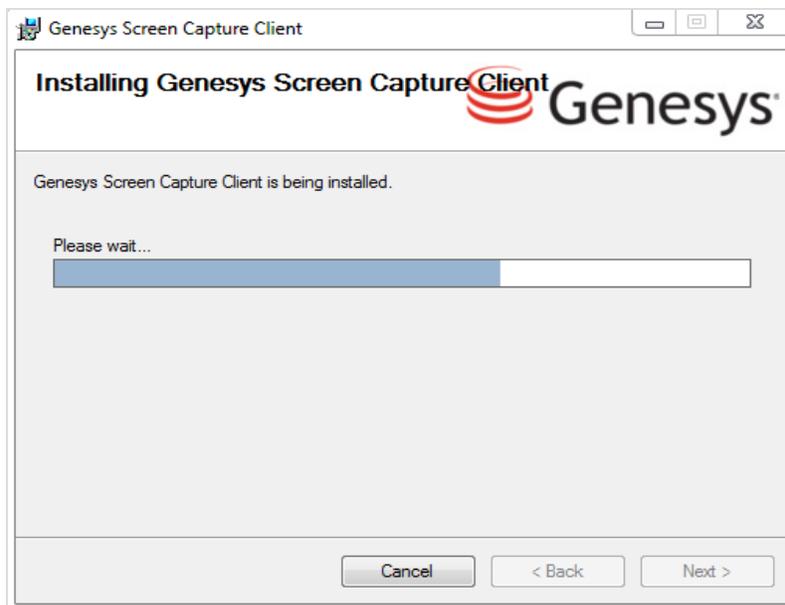


Figure 116: SCC Installation

6. Click **Close** when complete.

Once installation is complete, the Capture Client runs in the background. No icon is visible in the taskbar, but the SCC application ScreenREC.exe can be found in

the Windows Task Manager process list. Should this process ever be stopped manually by a user, the (hidden) ScreenRECStarter.exe process re-starts it within seconds.

The installer stores the settings entered during setup at the following Windows Registry location, dependent on PC architecture:

32-bit Windows installation:

```
HKEY_LOCAL_MACHINE\Software\ZOOM International\ZOOM  
ScreenREC Capture Client
```

64-bit Windows installation:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ZOOM  
International\ZOOM ScreenREC Capture Client
```

Standalone Mode

The *Standalone Capture Client Package* can be found only at the following URL (again where `SERVER_URL` is your main Call Recording server URL):

```
http://SERVER_URL/callrec/plugins/screenrec-client-binary-8.0.490.exe.
```

Double-clicking on the package file (`.exe`) unpacks the `ScreenREC.exe` binary executable in the current directory.

In standalone mode, the following command line arguments are required:

```
ScreenREC.exe -agent <agent_ID> -host <hostname or IP address>[:optional_port]
```

`-agent <agent_ID>`

The agent ID of the logged in agent, acquired by the Agent Desktop.

`-host <host_list>`

A list of one or more remote Screen Capture Recording Server (SRS) IPs or FQDNs, separated by spaces. In a single (standalone) GQM server scenario, the IP address of the Call Recording server is specified.

Each host can have an optional port appended after a colon (:). If no port is specified, the default port value of 7003 is assumed.

Examples

Agent 'jsmith', single host, port 7654 specified:

```
ScreenREC.exe -agent jsmith -host 192.168.200.132:7654
```

Agent 'jsmith', multiple hosts, default port (7003):

```
ScreenREC.exe -agent jsmith -host 192.168.200.132 -host 192.168.200.134 -host 192.168.200.164
```

Capture Client Security

For additional security, a suitable Windows group security policy should be determined for the `ScreenRECStarter.exe` and `ScreenREC.exe` applications.

Microsoft provides a free [Security Compliance Manager solution](#) for all currently supported Windows platforms, which includes group policy definition capabilities.

Capture Client Hostname Configuration

For correct communications between Screen Capture components, it is necessary to ensure that the agent PC has a correctly configured IPv4 `localhost` hostname.

There should be the following entry in

the `C:\Windows\System32\drivers\etc\hosts` file:

```
#::1 localhost  
127.0.0.1 localhost
```

Capture Client Logs

The Screen Capture Client binary supports six levels of logging, that records information including the timestamp, related module, and description.

Log files are found in several locations on Windows, this can vary depending on the version of Windows. In the paths below, [agentName] represents the Windows username of the agent.

Windows XP

- C:\Documents and Settings\[agentName]\Local Settings\Temp\screenrecService.log
- C:\Windows\Temp\screenrecService.log
- C:\Windows\Temp\screenrec.log

Windows 7

- C:\Users\[agentName]\AppData\Local\Temp\screenrecService.log
- C:\Windows\Temp\screenrecService.log
- C:\Windows\Temp\screenrec.log

Setting the Level of Logging

The current log level can be changed in the Windows Registry, in the following location, depending on PC architecture:

32-bit Windows installation:

```
HKEY_LOCAL_MACHINE\Software\ZOOM International\ZOOM  
ScreenREC Capture Client
```

64-bit Windows installation:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ZOOM  
International\ZOOM ScreenREC Capture Client
```

The registry value is named `log_level`, which takes a single integer as a value. Set one of 6 possible log levels:

- 0 : no logging
- 1 : errors only
- 2 : warnings and errors
- 3 : info, warn, error
- 4 : debug, info, warn, error
- 5 : trace, debug, info, warn, error

Chapter

14 **Configuring Screen Capture in the Call Recording Settings**

This chapter describes how to configure Screen Capture. The Screen Capture module tab is only visible if the Screen Capture service is selected during setup and the correct license is installed.

This chapter contains the following sections:

[Pre-requisites for Configuring Screen Capture in the Call Recording GUI](#)

[Configuring MasterScreen Capture](#)

[Configuring the Resolver](#)

[Configuring the Registry address](#)

[Configuring the Output File and Uploader Settings](#)

[Configuring the Uploader Settings](#)

[Configuring the Recording Specifications](#)

[Recording Specifications \(Advanced\)](#)

[Configuring the Uploader global settings](#)

[Pairing Screen Capture Agents to Their Desktops](#)

[Screen Capture Communicator Settings](#)

[Configuring the Media Encoder](#)

Pre-requisites for Configuring Screen Capture in the Call Recording GUI

The following are required to ensure that Screen Capture functions properly:

1. The Screen Capture service must be running. To check that the Screen Capture service is running, view the output from `/opt/callrec/bin/callrec_status`.
2. The Call Recording license must include Screen Capture activation.
3. Agent IP phones must be paired to their PC IP addresses.
4. At least one recording rule must be defined with the Screen Capture checkbox selected, and a Screen Capture Usage (%) value above zero.

The remainder of the configuration continues to take place in the Call Recording Web GUI **Settings > Configuration > Screen Capture tab**:

- Specify quality and format settings on the Screen Capture Configuration page.
- Use the Screen Capture Communicator settings tab to set the main RMI address and the recording initiation/stopping selection.
- Use the Media Encoder settings tab to set audio and video mixing options.

Configuring MasterScreen Capture

Navigate to **Settings > Configuration > Screen Capture > Screen Capture**.



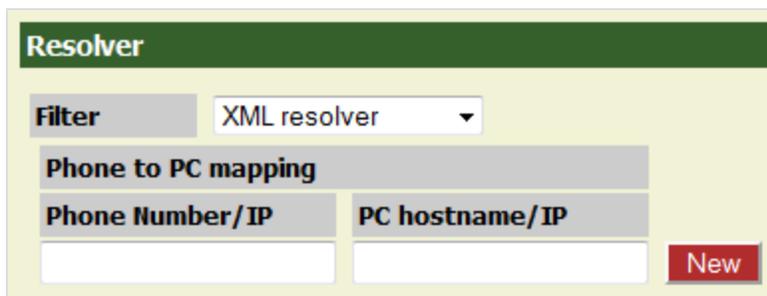
The screenshot shows a configuration window titled "MasterScreenREC". It contains two settings: "Server status" is a dropdown menu currently set to "master", and "Load coefficient" is a text input field containing the number "1".

Figure 117: Screen Capture Master Configuration

Use the default settings, **Server status** set to `master` and **Load coefficient** set to `1`.

Configuring the Resolver

Navigate to **Settings > Configuration > Screen Capture > Screen Capture**.



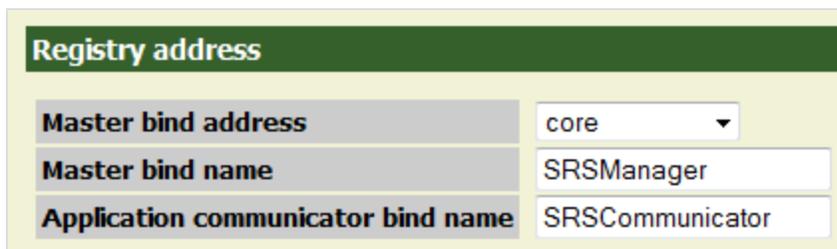
Resolver	
Filter	XML resolver
Phone to PC mapping	
Phone Number/IP	PC hostname/IP
<input type="text"/>	<input type="text"/>
	<input type="button" value="New"/>

Figure 118: Resolver Settings

Filter:the method to determine desktop PC to IP telephone pairs. Filter configuration was described earlier in this document. If a dynamic XML based web service for setting pairs is used, consult the Genesys Support team at support@genesyslab.com.

Configuring the Registry address

Navigate to **Settings > Configuration > Screen Capture > Screen Capture**.



The screenshot shows a configuration form titled "Registry address" with a dark green header. Below the header, there are three rows of configuration fields:

Registry address	
Master bind address	core
Master bind name	SRSManager
Application communicator bind name	SRSCommunicator

Figure 119: Registry Address

Screen Capture **Registry address** sets standard binding information. Select the server where Screen Capture is running. Servers are defined in the Call Recording Servers tab.

Configuring the Output File and Uploader Settings

Navigate to **Settings > Configuration > Screen Capture > Screen Capture**.

These settings relate to the *Media Upload Server* (MUS).

The screenshot shows a configuration interface with two main sections: 'Output Files Settings' and 'Uploader Settings'. The 'Output Files Settings' section has a green header and contains four rows of settings, each with a label and a text input field. The 'Location in filesystem' field contains '/opt/callrec/data/calls'. Below this field is a note: 'Uploader directory and location on file system should be in sync on single server installation.' The 'Path used in database' field also contains '/opt/callrec/data/calls'. The 'Directory pattern' field contains 'yyyyMMdd/'. The 'Date pattern' field is empty. The 'Uploader Settings' section has a green header and contains one row with the label 'Uploader address' and a dropdown menu showing 'core'.

Figure 120: Output file and Uploader Settings

- Location in filesystem** is the path to the directory containing intermediate (.recd) screen capture files.
 If Screen Capture is installed as part of a single GQM server, this path is the same as the path used in database setting, for example, `/opt/callrec/data/calls`.
 In a Screen Capture cluster scenario, where the *Media Upload Server* (MUS) is installed on a separate server, this setting is the full mount path from the MUS server to the remotely mounted Call Recording Core file system directory, for example, `/mnt/core/opt/callrec/data/calls`.
- Path used by database:** internal path to directory containing intermediate (.recd) screen capture.
 This remains the same whether a standalone or cluster installation is used, for example, `/opt/callrec/data/calls`.
- Directory pattern:** the template for creating subfolders in the storage directory. By default Call Recording stores calls in a new folder every day, the default template `yyyyMMdd` means that recordings from 24.12.2009 are stored in a folder named `20091224`. If this setting is changed in Call Recording, update this template to match your setting.

- **Date pattern:** use this template for customizing the date format. Default: empty. The Date pattern setting is not necessary for most Call Recording installations, since it overrides the standard date template. Leave this field blank.

Configuring the Uploader Settings

Navigate to **Settings > Configuration > Screen Capture > Screen Capture**.

Uploader address: the Screen Capture *Media Uploader Server* can be selected if different to the Core server, the server can be defined in the Call Recording Core settings in the Web GUI. Note that the MUS must be mapped to the Core server file system, the file paths must point to the same location.

Configuring the Recording Specifications

Navigate to **Settings > Configuration > Screen Capture > Screen Capture**.

Recording Specifications	
Frames per second	2
Maximum uploading bandwidth	No Limit
Maximum recording length (0=no limit)	0
Recorded screens	All
Scale factor	Do not scale
Captured screen quality	High
Timeout in seconds	10

Figure 121: Recording Specifications

The **Recording Specifications** settings affect screen capture quality.

- **Frames per second:** [default: 2] The number of frames per second. Value can be in the range **0.5 – 5**. A higher value results in smoother animation, but much greater demands on system resources (encoder processor load, file storage).
- **Maximum uploading bandwidth:** [default: **No Limit**]. A method of restricting the bandwidth used by the *Screen Capture Client (SCC)*. A lower speed value reduces bandwidth, but slows upload operations. Value range: **96kb/s – 1024kb/s**. The value **No Limit** cancels this restriction.
- **Maximum recording length:** [default: 0 = no limit]. A value, in seconds, formatted as `hh:mm:ss`, after which all recordings are terminated. A range of `0 – 23:59:59` is permitted; the value of 0 cancels this restriction.
- **Recorded screens:** [default: **All**] Record one (**Primary Only**) or **All** monitors and displays that are connected to the computer.
- **Scale factor:** [default: **Do not scale**]: Affects scaling. Value can be between **20%** and **75%** (**50%** corresponds to a final video screen size 50% smaller than the original screen, which reduces bandwidth requirements and stored file size). Small details can be lost in down-scaled screen recordings.
- **Captured screen quality:** [default: **High**]: Parameter for output of JPEG compression. Value can be within the range **Maximum – Low**. Typically it is set to a value of **High**. A lower quality value corresponds to a lower bandwidth required from SCC to MUS, but results in reduced capture quality.

- **Timeout in seconds:** [default: 10]: Upload timeout for *Screen Capture Client* (SCC) before a new file is created (in the event of network issues etc.). Possible range is 1 – 60 seconds.

Recording Specifications (Advanced)

The advanced recording specifications provide additional flexibility in configuring SCC performance:

Navigate to **Settings > Configuration > Screen Capture > Screen Capture**.

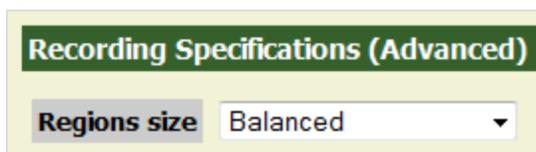


Figure 122: Advanced Recording Specifications

- **Regions size:** [default: **Balanced**]: dictates how the screen recording regions are defined.
 - Prefer lower bandwidth:** smaller regions requiring less bandwidth but more encoder processing.
 - Balanced:** a compromise achieving reasonable encoder performance and medium bandwidth requirements.
 - Prefer encoder performance:** larger regions requiring more bandwidth, but enabling the best encoder performance.

Configuring the Uploader global settings

Navigate to **Settings > Configuration > Screen Capture > Screen Capture**.

These settings are global, for all Screen Capture *Media Upload* (MUS) servers added on this configuration screen. For this reason, these settings are found at the very bottom of the page.

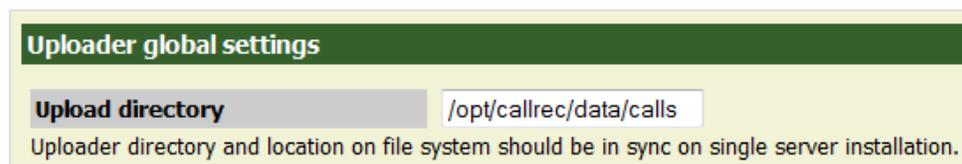


Figure 123: Global Media Upload Server (MUS) Settings

Upload directory: The global upload directory location for *Media Upload Server* (MUS) configuration. For a single GQM server, this path should be the same as the **Location in filesystem** setting in the **Output Files Settings** section above.

For the correct settings and procedures for a clustered Screen Capture installation, contact Genesys Support.

Pairing Screen Capture Agents to Their Desktops

Each agent's desktop PC and IP phone must be associated (paired) to each other; a process known as 'resolution'. This setting then tells Screen Capture which desktop to record when a call is initiated. There are four different methods of configuration, depending on the Filter setting:

- Option 1: XML Resolver
- Option 2: Agent ID Resolver
- Option 3: Property Resolver
- Option 4: IP to IP Resolver

Option 1 - XML Resolver

This is the simplest option, suitable for a small number of Screen Capture enabled agents. On the configuration screen, use the default XML resolver to associate agent IPs and phones.

Navigate to **Settings > Configuration > Screen Capture > Screen Capture**.



Figure 124: XML Resolver Pairing

1. In the **Filter** drop-down list, select **XML Resolver**.
2. Click **New**.
3. Enter the **Phone** extension or IP address, and **IP** PC hostname or IP address, for an agent. Repeat this until all agents' phone and IP information are entered.
4. Click **Save configuration**.

Each mapping that pairs a phone extension to a PC IP address must be unique for Screen Capture to operate correctly.

Option 2 - Agent ID Resolver

Navigate to **Settings > Configuration > Screen Capture > Screen Capture**.

The **Agent ID resolver** can only be used with Call Recording installations incorporating one of the following Contact Center integration components:

- Genesys Active Recording Ecosystem
- Genesys Enhanced Passive Recording (EPR)
- Genesys Integration Module

The Windows login ID on the Agent's PC is matched with the Agent's Contact Center login ID, obtained as external data by the SRS from the Call Recording integration component.

UCCE requires the External Data Key `IPCC_LOGIN_NAME` to be defined.



Figure 125: Agent ID Resolver

Option 3 – Property Resolver

To specify a large number of pairs, the use of a separate configuration file can be easier to maintain. This file is located on the Call Recording server, or can be created, at the following location:

```
/opt/callrec/screenrec/properties/cz/zoom/callrec/srs/addresses.properties
```

Each pair can be any combination of IP address, hostname, or phone extension; for example, IP address to hostname, extension to IP address, extension to hostname, and so on. However, a pair consisting of a desktop IP address and an agent extension number must be unique. Screen Capture does not operate correctly if more than one extension number is paired to the same desktop IP address.

Use a separate line for each pair, for example, if the agent's IP phone is 192.168.50.12 and the agent's desktop PC IP address is 192.168.110.32, enter:

```
192.168.50.12=192.168.110.32
```

If the desktop IP and phone IP are identical, for example, if the agent is using a software IP phone, enter the same IP address twice:

```
192.168.110.50=192.168.110.50
```

If all Screen Capture enabled agents are using the same IP address for both desktop PC and IP phone, see the next option: IP to IP resolver.

After updating the addresses.properties file, select the Property resolver filter option in the Screen Capture Resolver configuration, then restart Screen Capture.

Use the command:

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

Option 4 – IP to IP Resolver

If all agent pairs use the same IP address for both desktop PC and IP phone (as in all agents use a software IP phone), this option may be the most appropriate. If screen capture is requested according to the recording rules, Call Recording automatically attempts to contact the *Screen Capture Client* using the same IP address as for the agent's IP phone.

The IP to IP Resolver supports:

- Cisco SCCP
- Cisco JTAPI + SPAN
- Cisco JTAPI SPANless
- SIP
- Genesys Driver in EPR mode

Important:

The IP to IP Resolver does not support, Genesys Driver in MSR (Active Recording Ecosystem) mode or Avaya.

These two platforms do not supply the required information about the phone's IP address.

Screen Capture Communicator Settings

Navigate to **Settings > Configuration > Screen Capture > Screen Capture Communicator**.

The screenshot displays the configuration page for the Screen Capture Communicator. On the left, a sidebar lists 'Screen Capture', 'Screen Capture Communicator' (selected), and 'Media Encoder'. Below the sidebar are 'Save configuration' and 'Reload configuration' buttons. The main content area has a red header 'Screen Capture Communicator' and a green sub-header 'Communicator Setting'. The settings are as follows:

Setting	Value
Registry address	core
Filter	OnEndCouple stop method
Stop recording after delay (seconds)	0

Figure 126: Screen Capture Communicator Configuration - OnEndCouple Stop

The Screen Capture Communicator is configured with the following settings:

Registry address: the server running the RMI service.

Stop Setting: the method of determining the end of the screen capture. Depending on this setting, the remaining fields change as follows:

OnEndCouple Stop

- **Stop Setting: OnEndCouple stop:** stops at the end of the associated audio call.
- **Stop recording after delay (seconds):** specify any additional delay before stopping.
- **Wait for Agent ID in external data:** the Communicator only stops when the Agent ID is found in at least one of the indicated external data fields (**External Data name for Agent ID of the calling party / External Data name for Agent ID of the called party**).

OnExternalData Stop

Communicator Setting	
Registry Address	core
Stop Setting	OnExternalData stop method
Name of external data	EXTERNAL_DATA_Nr
Max waiting time for external data (seconds)	0
Wait for Agent ID in External Data	<input checked="" type="checkbox"/>
If wait is enabled, make sure at least one of the external data names is filled below	
External Data Name for the Agent ID of the Calling Party	GEN_TEV_AgentID
External Data Name for the Agent ID of the Called Party	GEN_TEV_OTHER_A

Figure 127: Screen Capture Communicator Configuration - OnExternalData Stop

- **Stop Setting: OnExternalData stop** Screen capture stops when a particular external data key is received after the call ends.
- **Name of external data:** specify the name of the data key to be found.
- **Max waiting time for external data (seconds):** timeout value for external data key. After the call ends, if the specified key is not found in the external data within this time period, screen capture stops automatically.

Important:

This feature is not yet supported by the Genesys platform.

Configuring the Media Encoder

Navigate to **Settings > Configuration > Screen Capture > Media Encoder**.

The Screen Capture *Media Encoder* is configured with the following parameters:

The screenshot shows the 'Media Encoder Configuration' page. On the left, a sidebar contains three items: 'Screen Capture', 'Screen Capture Communicator', and 'Media Encoder', with 'Media Encoder' selected. The main content area is titled 'Media Encoder Configuration' and is divided into several sections:

- Database Setting:** 'Database Pool' is set to 'callrec'.
- ApplicationCommunicator:** 'Master registry address' is set to 'core'.
- Media Encoder Settings:** 'Schedule task run' is checked; 'Run period in minutes' is 30; 'Range of processed calls' is 'older than 30 minutes'.
- Filter factory:** 'Add factory' is empty, with a 'New' button.
- MasterEncoder:** A table lists the configuration for a 'MasterEncoder':

Media Encoder Name	MasterEncoder	Remove
Is Master?	<input checked="" type="checkbox"/>	
Load Balancer Weight	1	
Registry address	core	
Location in filesystem	/opt/callrec/data/calls	
Path used in database	/opt/callrec/data/calls	
Remove unmixed files after mixing	<input type="checkbox"/>	
Video Codec	H.264	
Key frames rate in seconds	5.0	
Encoded video quality (bitrate)	High	
- Add New Media Encoder:** 'Media Encoder Name' is 'SlaveEncoder', with a 'New' button.

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

Figure 128: Media Encoder Configuration

Database Setting

- Database Pool: the database pool to use for the *Media Encoder*; usually `callrecon` a single server.

Application Communicator

- Registry address: the server running the RMI service (core on a single server).

Mixer Task Settings

- **Schedule task run:** when checked, the Media Encoder performs batch encoding of capture files at regular intervals. When unchecked, the Media Encoder functions on demand only, on the command line or selecting a capture file to export in the list of call recordings in the Call Recording Web GUI.
- **Run period in minutes:** determines the wait period for the Media Encoder when no calls are queued for encoding.
- **Range of processed calls:** defines the time range of the calls for encoding. In some cases it is important not to process recordings right after they are saved, in which case this parameter enables you to define that only recordings older than x minutes get processed. Use a variable time window, since it speeds up the selection of recordings from the database.

Encoder Settings

The following settings are assigned to each individual Encoder. After GQM installation, only one Master Encoder is defined, but more can be added if required.

- Media Encoder Name: a user defined name for this Encoder.
- Is Master?: specify by selecting this option that this is a Master Encoder.
- Load Balancer Weight: relative weight / priority compared to other Encoders.
- Registry address: the server running the RMI service.
- Location in filesystem: path to directory containing both intermediate (.recd) screen capture (input) files and the encoded files output by the Media Encoder.

If Screen Capture is installed as part of a single (standalone) GQM server, this path is the same as the Path used in the database setting:

For example, `/opt/callrec/data/calls`.

In a Screen Capture cluster scenario, where the Screen Capture Media Encoder (SME) is installed and configured on a separate server to the database, this setting is the full mount path from the SME server to the remotely mounted Call Recording Core file system directory:

For example `/mnt/core/opt/callrec/data/calls`

- Path used in database – Internal path (prefix) to directory containing both intermediate (.recd) screen capture (input) files and the encoded files output by the Media Encoder:

For example `/opt/callrec/data/calls`

This value is checked by the Screen Capture Media Encoder (SME) in order to resolve the complete file system path to the directory specified in the location in filesystem parameter:

If the current path prefix found in the database is the same as the path used in database parameter prefix, the SME replaces the prefix found in the database with that found in the location in filesystem parameter. This is typically used in a Screen Capture cluster scenario, where the SME(s) and database are on different servers.

If the current path prefix found in the database is different to the path used in database parameter prefix, including if left blank, the SME uses the prefix found in the database unchanged. This is typically the case with single server scenarios.

Important:

If the Relocation Tool is scheduled to move recd data files to a custom directory elsewhere, that directory must be writable by Call Recording (for example, by using the chown tool: `chown -R callrec:callrec /path/to/custom/directory`).

The Screen Capture Media Encoder writes encoded mp4 video files to the same directory as the source recd files, so this fails with the default permissions assigned by the Relocation Tool.

- **Remove unmixed files after mixing:** If selected, the original intermediate format files (`.recd`) are deleted after mixing. By default, this option is not checked, so all source files are retained. This assumes that a media lifecycle policy (archive/delete) are applied to the directories specified by the path to calls to be processed and the path to save the encoded file parameters above.
- **Video Codec [default: H.264]:** Video codec for encoded video, either H.264 or MPEG 4:2.
- **Key frame rate in seconds [default: 5]:** Value (in seconds) specifying how often to force a key frame in the output video; value range: 1 – 60
- **Encoded video quality (bitrate) [default: High]:** Quality of encoded video for playback; value range between Maximum and Low. Maximum quality utilizes the most system resources.

Configuring a Custom Temporary Directory for the Media Encoder

For reasons of performance, by default the media encoder is set up to use the system tmp directory. Many other applications use the existing system tmp directory to store information. Files marked for deletion, but not yet deleted, can use up vital space. This can lead to insufficient space for the media encoder to process large video files, and in severe cases, the media encoder stops encoding. The solution is to give the media encoder its own temporary directory independent of the system tmp directory.

Step 1

Specify a different temporary directory for the mixer module by adding the mixer parameters line at the end of `/opt/callrec/etc/callrec.derived` configuration file as follows:

```
JAVA_OPTS_MIXER="-server -Xms32m -Xmx1024m -DTMPDIR=/opt/callrec/tmp"
```

Step 2

Restart the configuration service, then the mixer module:

```
/opt/callrec/bin/rc.callrec_configmanager restart  
/opt/callrec/bin/rc.callrec_mixer restart
```

15 **Screen Capture High Availability Options**

To provide High Availability for Screen Capture:

- There must be two Call Recording clusters deployed and these clusters must have a Screen Capture server configured.
- Each cluster must have its own uploaders and media encoders, as these can not be shared.
- The Screen Capture Client must be configured to connect to all of the Screen Capture Servers by entering the list of addresses during installation of the Capture client.

The Screen Capture Client connects to a primary Screen Capture server. The primary Screen Capture server controls the Screen Capture Client. Upon failure of the primary Screen Capture server, control passes to the secondary Screen Capture server.

Recordings are uploaded to the primary uploader. In the event of a failure of the primary uploader, the Screen Capture Client can connect to the secondary Screen Capture server and process requests.

If there is a failure of the Screen Capture server during recording, the current recording is lost. After reconnection to the other Screen Capture server, new requests process normally.

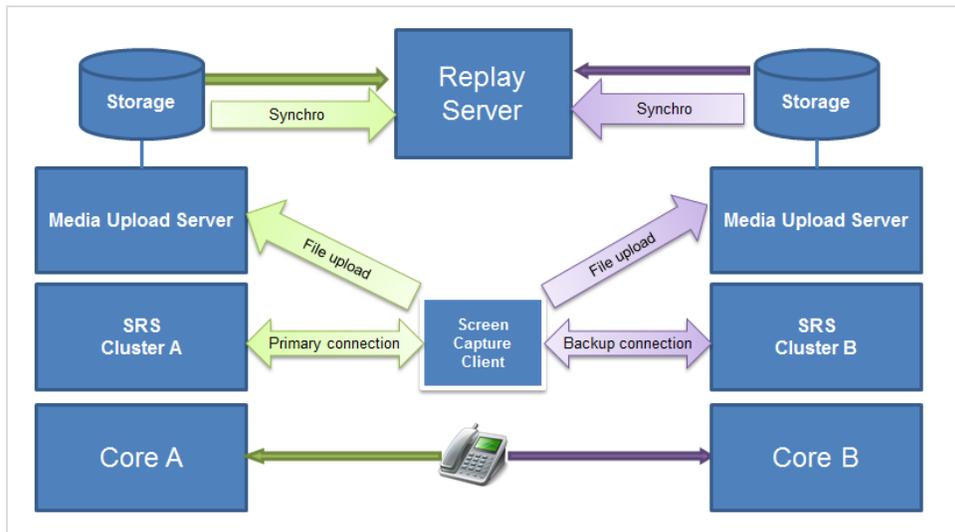


Figure 129: High Availability for Screen Capture

Because all of the media are synchronized at the replay server; if Screen Capture fails on the primary server (A), but the call recording is ok, then it is possible to replay the screen captures from the backup connection (B) with the audio from the primary.

Java Standalone Thin Client

The integration of the standalone *Capture Client* with Java-based agent desktops is provided by the `screenrec-controller.jar` file that must be present in the classpath of the agent desktop application. This file can be found at the following default location on the Call Recording server:

```
/opt/callrec/screenrec/screenrec-controller-5.0.0.jar
```

The `screenrec-controller.jar` bundles a (compressed) *Capture Client*. The actual spawning of the *Capture Client* is performed by creating a new instance of the `cz.zoom.screenrec.impl.controller.ScreenRecorderStarter` class.

The `ScreenRecorderStarter` constructor takes the following parameters:

- The agent name (login ID)
- A list of servers where to connect

The `ScreenRecorderStarter` instance runs a background thread that monitors the *Capture Client* and restarts it if it exits. The application is bundled in the form of a highly-compressed self-extracting `.exe` application.

The starter instance extracts the application to a temporary directory, executes the self-extraction and runs the extracted binary application. A background thread deletes all old instances that may have been left over in the temporary directory.

To stop the capture client from the agent desktop, call `ScreenRecorderStarter.stop()` on this instance. This stops the monitoring thread and destroys the running client application.

.NET Standalone Thin Client

The integration of the standalone *Capture Client* with .NET-based agent desktops is provided by the ScreenREC.exe binary application, that can be downloaded in compressed form from the Call Recording server at the following URL (where `SERVER_URL` is the Call Recording server address):

```
http://SERVER_URL/callrec/plugins/screenrec-client-binary-8.0.490.exe
```

Running the downloaded executable extracts the ScreenREC.exe binary application.

To start the application from C/C++ code, call the following method:

```
System.Diagnostics.Process.Start (appName, arguments)
```

where:

- `appName` is the full path to the *Capture Client* binary;
- `arguments` is obtained by calling:

```
System::String::Format ("-agent {0} -host {1}", agentName, serverHostName)
```

The `-host` parameter may be used several times, in which case the format specification needs to be changed accordingly.

Screen Capture Port Usage Guide

The Screen Capture server accepts incoming connections on predefined port 7003. The port is currently not configurable.

The **Capture Client** application does not use any predefined port.

In the Windows service mode, there is additional inter-process communication, between the service and running Screen Capture **Capture Client** applications. This inter-process communication uses the Named Pipes Windows API rather than sockets.

The **Capture Client** application connects as a client to the Screen Capture Media Upload Server (MUS), and the Screen Capture server specifies the server endpoint that the **Capture Client** application uploads to. This endpoint is typically port 80 and on the same server that the Call Recording UI is installed. This port number can be changed from the Screen Capture configuration.

Chapter

16 **Configuring CUCM Prerecording**

This chapter describes prerecording.

This chapter contains the following sections:

[Prerecording Overview](#)

[Configuring Prerecording in CUCM 5 and higher](#)

[Configuring Prerecording in CUCM 4](#)

[Configuring Prerecording in Genesys Call Recording](#)

Prerecording Overview

Prerecording enables users to selectively record calls. Prerecording saves all calls, but only temporarily. The user has an adjustable time period to select the call to be converted to a file and saved. If a call is not selected by the user, it is erased from memory.

The call processed by the prerecording service, goes through three stages:

1. Recording: the call was selected to be recorded.
2. Prerecording: the call is in progress and is recorded in the background.
3. Post-recording: the call ends and the recording is waiting.

Each stage has its own group of parameters in Call Recording that control what users can do with a call.

To set up Call Recording Prerecording, configure the service on the CUCM.

Configuring Prerecording in CUCM 5 and higher

To provide prerecording to selected end-points, log in to Cisco Unified Communications Manager Configuration and make these two changes:

1. Add Call Recording prerecording as a new service.
2. Enable this service on selected end-points.

Adding the Prerecording Service

The following figures may vary between CUCM versions, but the main concept remains the same.

1. Log into Cisco Call Manager Administration.
2. On the **Device** menu, navigate to **Device Settings > Phone Services**. The **Find and List IP Phone Services** page displays.

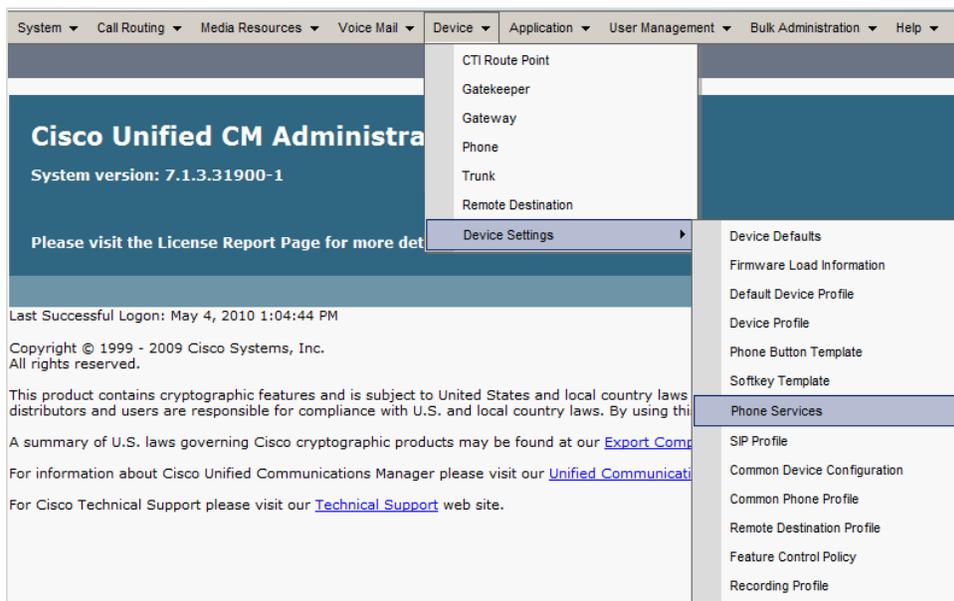


Figure 130: Phone Services Menu in CUCM 7

3. Click **Add New**. The **IP Phone Services Configuration** page displays.

Figure 131: IP Phone Services Configuration in CUCM7

4. Enter the following parameters:

- **Service Name**, for example, Call Recording.
- **ASCII Service Name**, for example, Call Recording.
- **Service URL**, `http://XXX.XXX.XXX.XXX/prerecording` where `XXX.XXX.XXX.XXX` represents the IP address of the Call Recording Core server.
- **Enable**, select this option to enable the service, only for CUCM 7 and higher.

In CUCM 7 and higher there are two other required fields. Leave those at their default values; these are **Service Category: XML Service**; **Service Type: Standard IP Phone Service**.

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

Making Prerecording Available for Users for CUCM 5 and Higher

The next step is to activate the service on users' phones.

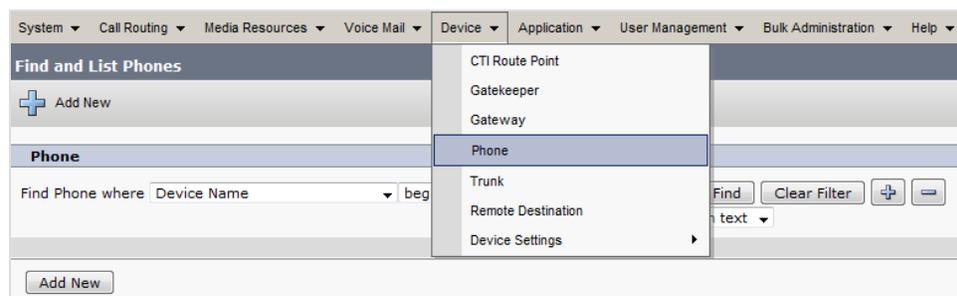


Figure 132: Phone Menu in CUCM 7

1. Select the device to enable prerecording on via **Device > Phone**.

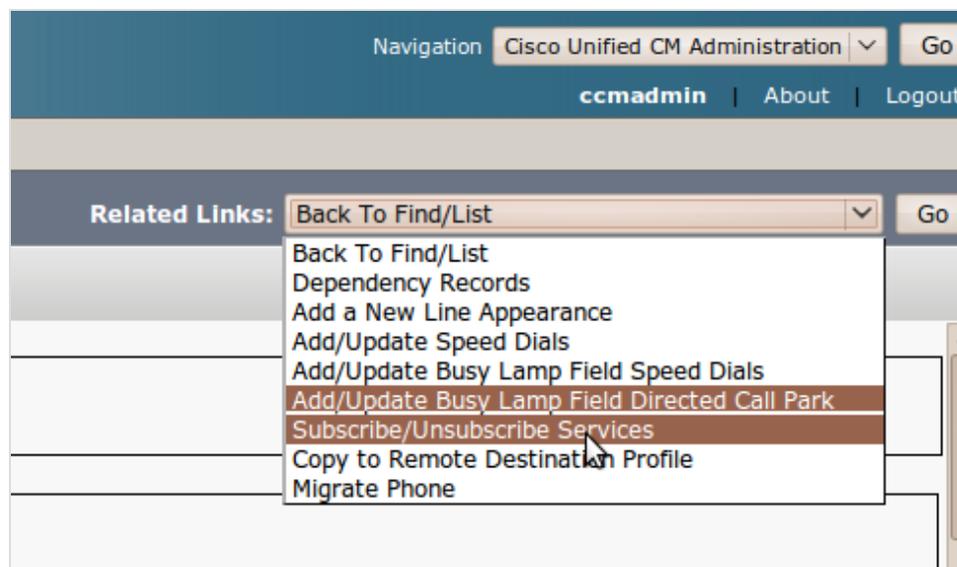


Figure 133: Related Links

2. Select **Subscribe/Unsubscribe Services** from **Related Links:** and click **Go**.

The **Subscribed Cisco IP Phone Services** page displays.

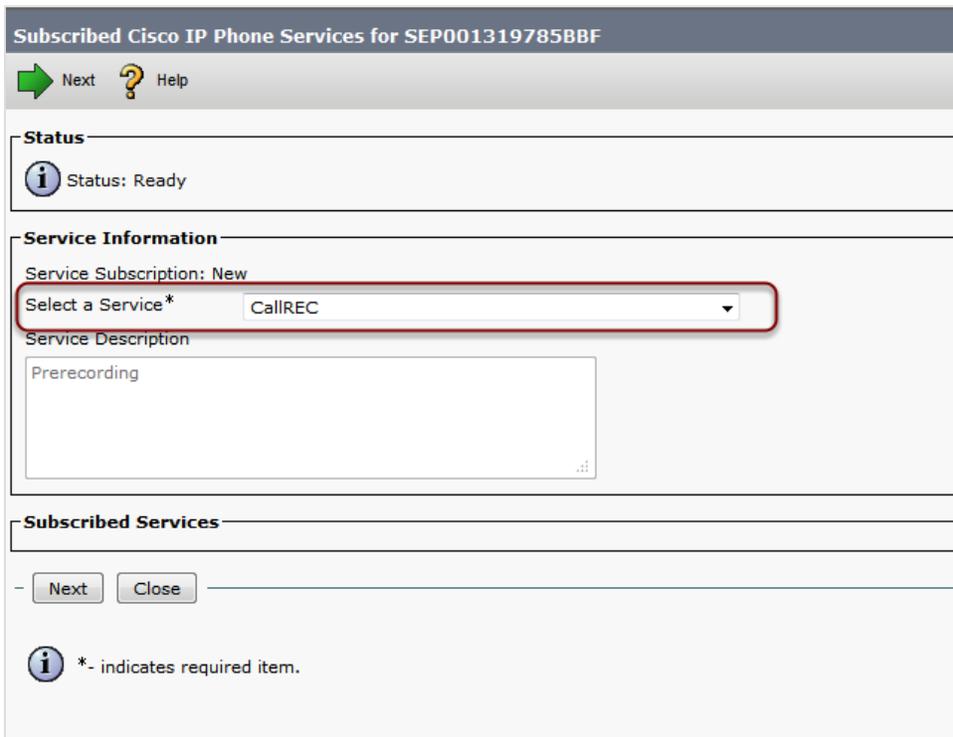


Figure 134: Select a Service Dropdown

3. Select the service from the **Select a Service*** drop-down list and click **Next**.

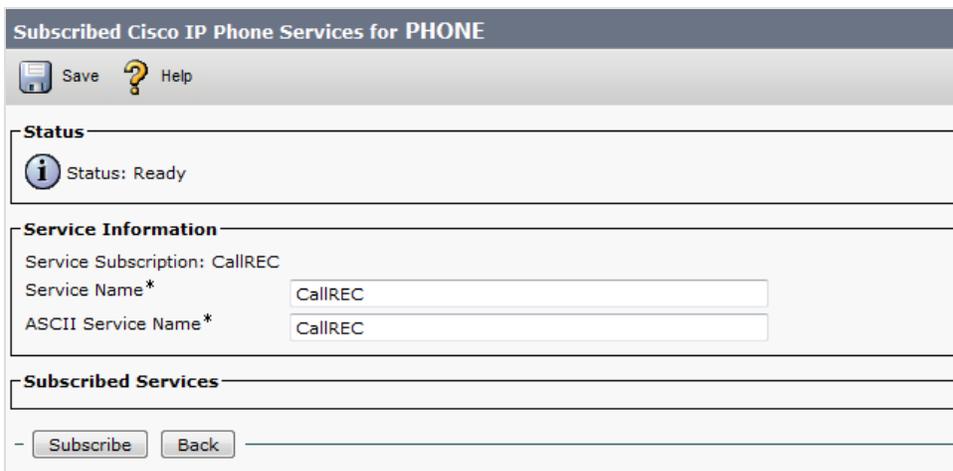


Figure 135: Subscribe to IP Phone Service CUCM 7

4. Click **Subscribe** and then **Save** to save the changes. This enables prerecording on the selected device.

5. Repeat these steps for each user or device that requires prerecording functionality.

To enable prerecording for multiple users simultaneously, edit the default Cisco Unified Communications Manager configuration and assign the prerecording service for the users and/or groups within the system. For more information, consult the *CUCM Administration Guide*.

Configuring Prerecording in CUCM 4

To provide prerecording to selected end-points, log in to Cisco Unified Communications Manager Configuration and make these two changes:

1. Add Call Recording prerecording as a new service.
2. Enable this service on selected end-points.

Adding the Prerecording Service in CUCM 4.3

1. Log into CUCM Administration.
2. On the **Feature** menu, select **Cisco IP Phone Service Configuration**. The **Find and List IP Phone Services** page displays.



Figure 136: Adding a New IP Phone Service

3. Click **Add a New IP Phone Service**. The **IP Phone Services Configuration** page displays.



Figure 137: IP Phone Service Configuration

4. Enter the following parameters:

- **Service Name** – for example **CallREC cr-show**
- **Service URL** –
`http://XXX.XXX.XXX.XXX:8080/prerecording/index.jsp`
 where XXX.XXX.XXX.XXX represents the IP address of the Call Recording Core server.
- **Character Set**: choose a character set according to the preferred language.

5. Click **Insert** to save the changes.

The **IP Phone Services Configuration** screen displays with a list of installed services.

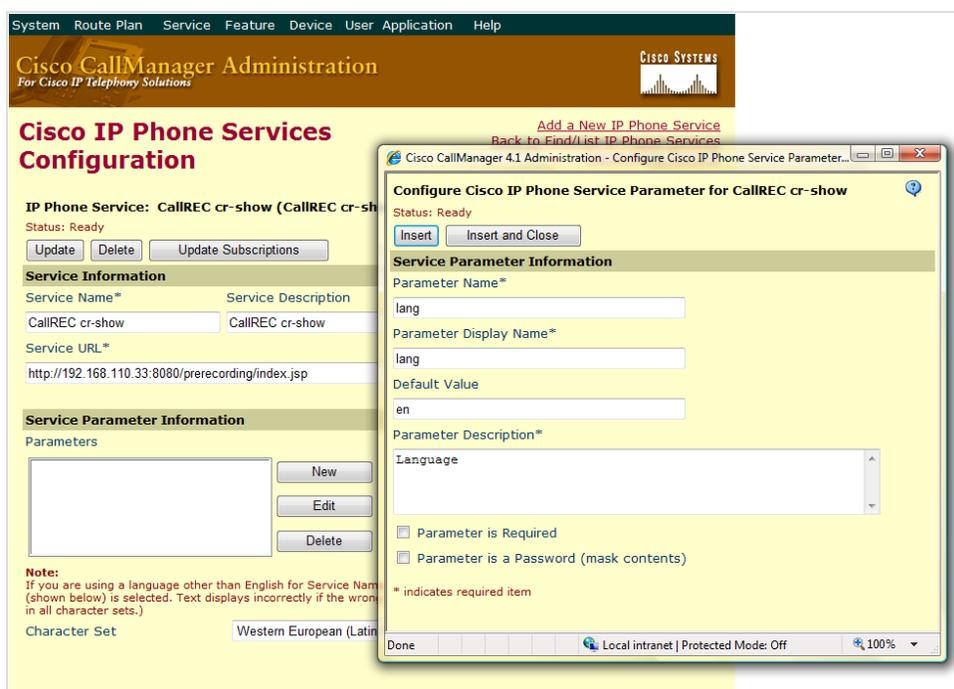


Figure 138: IP Phone Service Parameters

6. Select the Call Recording service from the list. If the service is not listed, try the search function on the top of the page.
7. In the Service Parameter Information area, click **New**.

Enter the following parameters to ensure the proper functioning of automatic language parameters passing from the end point device:

- **Parameter Name**: type “lang”
- **Parameter Display Name**: type “lang”
- **Default Value**: type “en” for English, “cs” for Czech, “ru” for Russian, etc.
- **Parameter Description**: type “Language”

8. Click **Insert** to save the changes.

Making Prerecording Available for Users in CUCM 4.3

Once prerecording is set up in CUCM and Call Recording, the next step is to activate it on users phones.

1. Log in to CUCM and select **User Options**. This is usually located on the server under `/ccmuser`.
2. Select the device to enable with prerecording from the drop-down list, and click **Configure your Cisco IP Phone Services**.

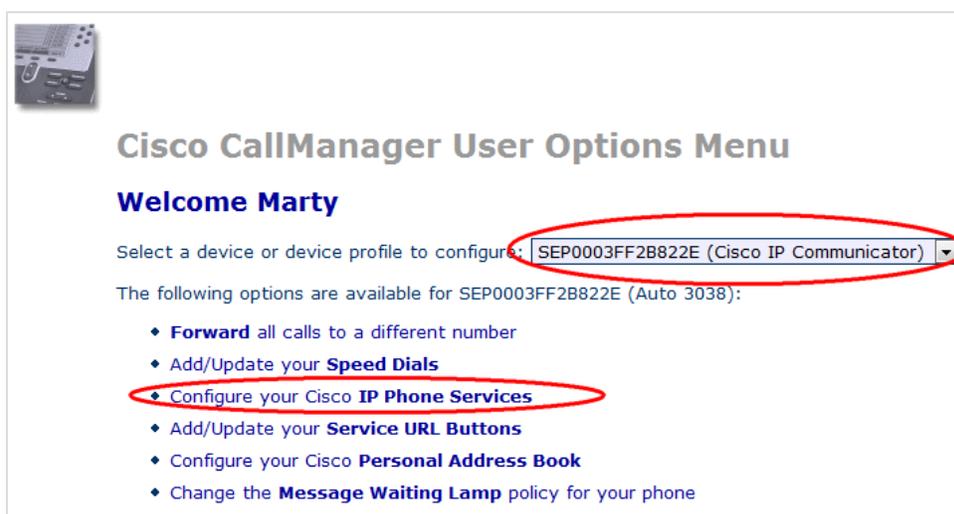


Figure 139: CUCM User Options

3. Click **Continue** to set its parameters.
4. In the **Service Name*** field, type the name to display on the IP phone in its Services menu.
5. In the **lang*** field, type the preferred language code, `en` for English, `cs` for Czech, `ru` for Russian, and so on.
6. Click **Subscribe** to save the changes.

Prerecording is now enabled on the selected device. Repeat these steps for each user who requires Prerecording.

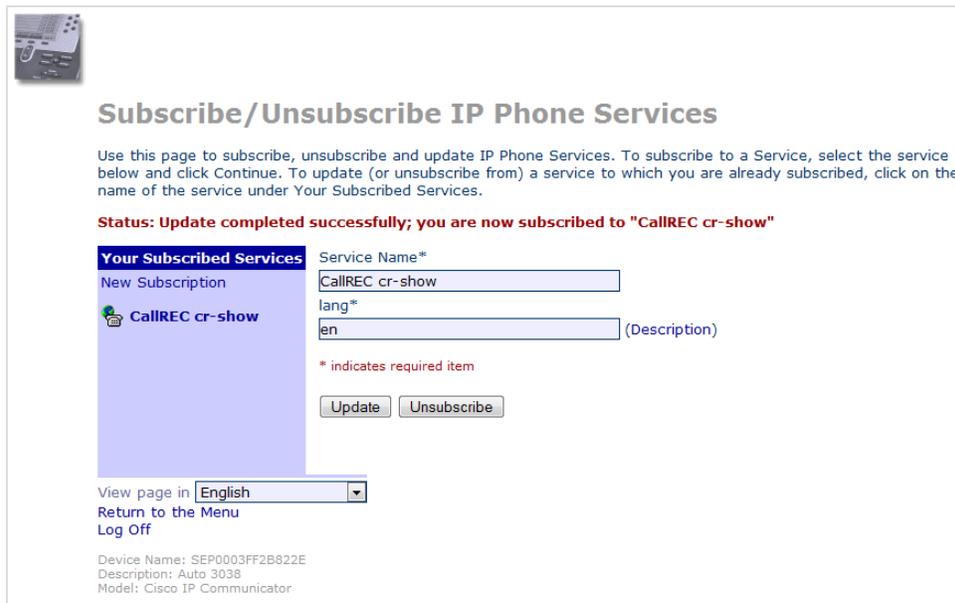


Figure 140: Subscribe to IP Phone Service

To enable Prerecording for multiple users simultaneously, edit the default CUCM configuration and assign prerecording service for the users or groups or users within the system. For details, consult the CUCM Administration Guide.

Configuring Prerecording in Genesys Call Recording

After adding Call Recording to the CUCM configuration, specify the available functions and prerecording settings within the Call Recording web interface. These settings add functions to the IP phone interfaces of all users .

Log in to Call Recording as `admin` and navigate to **Settings > Configuration > Extras > Call Recording Prerecording**. Prerecording is listed in the additional installed modules.

CallREC Prerecording Server Configuration

Main

Timeout call wait (minutes)

Record Status

Email

Edit email

Prerecording Status

PIH

Email

Edit email

Record

Email and record

Application Communicator

Bind name

Registry address

External data

Key

Value

New value

Figure 141: Prerecording Interface Options

Setting the Call Wait Timeout

Navigate to **Settings > Configuration > Extras > Call Recording Prerecording > Main**.

1. Set the **Timeout call wait (minutes)**: This defines the period in minutes, after the end of a call, during which the user can still save that call recording. The default value is 2 minutes.
2. Click **Save configuration** to save the changes.

Enabling the Send by Email Option for Record Status

Navigate to **Settings > Configuration > Extras > Call Recording Prerecording > Record Status**.

1. **Select Email:** This enables the **Send by email** option in the service menu. The recorded calls are emailed to the address defined in the user's profile.
 2. **Edit email:** This enables the **Send by email to...** option in the service menu. The user can define the recipient's email address before sending a call.
- Click **Save configuration** to save the changes.

Enabling the Send by Email Option for Prerecording Status

Navigate to **Settings > Configuration > Extras > Call Recording Prerecording > Prerecording Status**.

Enter the following settings:

PIN: When selected, requires users to enter their PIN to access to the service menu.

Email: Enables the **Send by email** option in the service menu. The recorded calls are emailed to the address defined in the user's profile.

Edit email: Enables the **Send by email to...** option in the service menu. User can define the recipient's email address before sending a call.

Record: Enables the ability to save selected calls – the prerecorded call is stored on the server only when the user chooses this option. In the service menu, this appears as **Save**.

Email and Record: Combines the email and record functions. The selected call is recorded, stored on the server, and sent to the user's e-mail address. This function is labeled as **Save and send by email** in the service menu.

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

Configuring the Application Communicator

Navigate to **Settings > Configuration > Extras > Call Recording Prerecording > Application Communicator**.

1. Set the **Bind name**: This is the name of the integration module for registering on RMI, for example, "Prerecording".
2. Set the **Registry address**: This is the Server with RMI service running. This is defined in the Servers part of configuration, for example "core".
3. Click **Save configuration** to save the changes.

Configuring the External Data Feature

External Data can be added by a phone user during or after a prerecorded call the **Timeout call wait (minutes)** applies the same as for saving a call. For example, an agent could mark the type of call received as “Presales”, “Sales”, or “Support” with a few button presses on their IP phone. The call is then tagged with this external data value and automatically marked for recording .

To configure the **External Data** feature:

Navigate to **Settings > Configuration > Extras > Call Recording Prerecording > External Data**.

1. Specify a **Key** (data name) and one or more **New values** (selectable values)
2. Click **New** for each New Value.
3. Click **Save configuration** to save the changes.

4. Follow the steps used earlier to create a second new IP Phone Service for the following service URL:

```
http://XXX.XXX.XXX.XX-
```

```
X:8080/prerecording/IpPhoneExternalData.jsp
```

(where XXX.XXX.XXX.XXX represents the IP address of the CallREC Core server).

5. Name the service, for example Call Recording call-info, and publish it for the appropriate users.

During or after a call, users can now access the new call-info service on their phone to tag the call with one of the text values configured earlier. Tagging a prerecorded call in this way automatically marks it for recording.

17 Recording CUCM in SRST Mode

To record in Secure Survivable Remote Site Telephony (SRST) mode, Call Recording must be integrated with CUCM and configured to record using the Cisco JTAPI adapter as the primary communication interface for recording. In addition to the primary adaptor the Skinny Adapter is enabled and only configured to listen on the IP address of the SRST router.

This means that in normal operation Call Recording records calls using the JTAPI interface. When CUCM falls down, then the SRST router starts to produce signaling that is captured by Skinny adapter and Call Recording records using the Skinny signaling.

The procedure to configure this is described below.

1. Access the Call Recording server via an ssh client for example PuTTY. Log in as admin and enter `su` - to login as root and enter the password `zoomcallrec`. Enter the following command to stop all Call Recording services:

```
/etc/init.d/callrec stop
```

2. Edit the configuration of the Skinny Adapter in the `/etc/callrec/callrec.conf` file. Find the line `RTS_PARAMS[1]` and add option `-l` followed by the IP address of your SRST router. See the example below (where 10.20.30.40 is the IP address of the SRST router):

```
RTS_COUNT=1
RTS_PARAMS[1]=" -d eth1 -p 30100 -l 10.20.30.40 "
```

Please note that the list of parameters must start and end with space.

3. Make sure both the Skinny and JTAPI adapters are enabled. Edit file `/etc/callrec/callrec.conf` as follows:

```
#
# Services to be run
#
RUN_RMI="1"
RUN_CONFIGMANAGER="1"
RUN_RTS_JTAPI="1"
RUN_RTS_SKINNY="1"
RUN_RTS_SIP="0"
```

4. Add the appropriate driver for Skinny protocol in Core configuration. Edit `/etc/callrec/core.xml` file as follows:

```
<SpecifiedConfiguration name="driversAndReaders">
<EqualGroup name="reader">
<Value name="name">Skinny</Value>
<Value name="port">30100</Value>
<Value name="server">core</Value>
</EqualGroup>
<EqualGroup name="reader">
<Value name="name">JTAPI</Value>
<Value name="port">30300</Value>
<Value name="server">core</Value>
</EqualGroup>
<EqualGroup name="driver">
<Value name="name">Skinny</Value>
<Value name="class">cz.zoom.callrec.driver.skinny.SkinnyDriver</Value>
<Value name="enabled">>true</Value>
</EqualGroup>
<EqualGroup name="driver">
<Value name="name">CiscoJTAPI</Value>
<Value name="class">
cz.zoom.callrec.driver.ciscojtapi20.CiscoJTAPI20Driver</Value>
<Value name="enabled">>true</Value>
</EqualGroup>
<EqualGroup name="driver">
<Value name="name">SIP</Value>
<Value name="class">cz.zoom.callrec.driver.sip.SIPDriver</Value>
<Value name="enabled">>false</Value>
</EqualGroup>
</SpecifiedConfiguration>
```

5. Start Call Recording using the command:

```
/etc/init.d/callrec start
```

6. Check that all services runs correctly. Test both modes of recording:

Connecting to two Independent CUCM Clusters

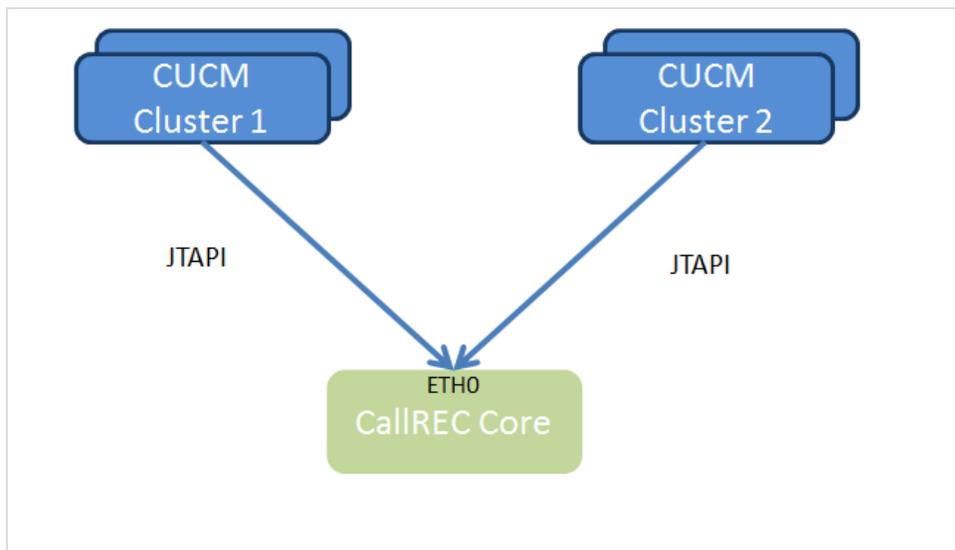


Figure 142: Two Call Manager Clusters into One Core

Two independent CUCM clusters, can record using one Call Recording server. This is only if the total number of devices being recorded does not exceed the maximum number of simultaneous calls for one server. To record two independent clusters on one server, create an extra JTAPI Adaptor. To do that modify the configuration. Before the configuration is modified, ensure that Call Recording is not running.

Preventing Call Recording from Restarting New Installations

If this is a new installation, then follow the instructions in the Implementation Guide and set up recording for CUCM cluster 1 as normal for CUCM until prompted as below:

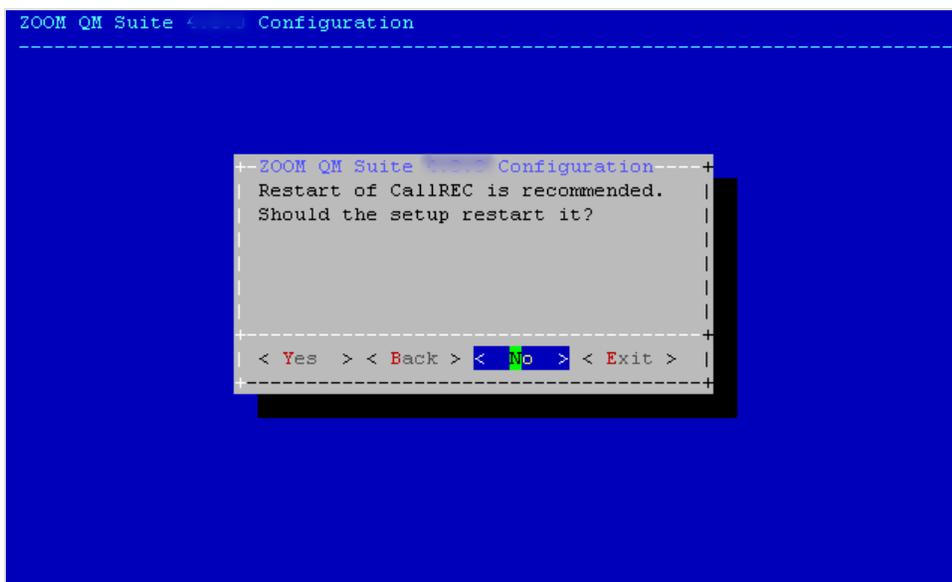


Figure 143: Should the Setup Restart?

Select **No** to modify the code to configure the second sniffer for cluster 2, it is safer to do this when Call Recording is not running.

Stopping Call Recording Existing Installations

If the Call Recording Recording server is already running, for example, if adding an extra CUCM cluster to an existing installation of Call Recording, then stop all Call Recording services before the configuration is changed.

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

Ensure the log in is as root and enter the following:

```
/etc/init.d/callrec stop
```

Creating an additional JTAPI Adaptor

1. Make a copy of `/opt/callrec/jtapi`, for instance:

```
cd /opt/callrec; cp -r jtapi jtapi2
```

2. Copy the JTAPI module startup script, for instance:

```
cp /opt/callrec/bin/rc.callrec_rts_jtapi /opt/callrec/bin/rc.callrec_rts_jtapi2
```

3. Edit `/opt/callrec/bin/rc.callrec`

Add the following below line 21:

```
[ -x $CALLREC/bin/rc.callrec_rts_jtapi2 ] && runme $RUN_RTS_JTAPI2  
$CALLREC/bin/rc.callrec_rts_jtapi2 start
```

Add the following below line 53:

```
[ -x $CALLREC/bin/rc.callrec_rts_jtapi2 ] && runme $RUN_RTS_JTAPI2  
$CALLREC/bin/rc.callrec_rts_jtapi2 stop
```

4. Edit `/opt/callrec/etc/callrec.conf`

Add the following below line 16:

```
RUN_RTS_JTAPI2="1"
```

add below line 82:

```
JTAPI2="$CALLREC/jtapi2"
```

5. Edit `/opt/callrec/etc/callrec.javapath`

Add the following below line 72:

```
CLASSPATHJTAPI2=`build-classpath-directory $JTAPI2`
```

6. Edit `/opt/callrec/bin/rc.callrec_rts_jtapi2`

Change line 16 to:

```
CLASSPATH=$CLASSPATHJTAPI2:$CLASSPATHLIB:/etc/callrec
```

Change line 25 to:

```
echo -n "Starting CallREC JTAPI2: "
```

Change line 27 to:

```
if [ -f "$PID_RTS_JTAPI2" ] ; then
```

Change line 28 to:

```
read pid < "$PID_RTS_JTAPI2"
```

change line 42 to:

```
echo $PIDNUM > "$PID_RTS_JTAPI2"
```

Change line 45 to:

```
until [ "`$CALLREC/bin/callrec_status -port $RMIPORT -host $RMIHOST -names  
2>%1 | grep \"remoteJTAPI2\\\"`" ] || [ $count -gt $WAIT ]
```

change line 68 to:

```
echo -n "Stopping CallREC JTAPI2: "
```

Change line 69 to:

```
$CALLREC/bin/callrec_status -host $RMIHOST -port $RMIPORT -name remoteJTAPI2  
-stop > /dev/null 2>&1 &
```

Change line 76 to:

```
if [ -f "$PID_RTS_JTAPI2" ]; then
```

change line 78 to:

```
read pid < "$PID_RTS_JTAPI2"
```

Change line 90 to:

```
rm -f "$PID_RTS_JTAPI2"
```

change line 113 to:

```
echo "Usage: rc.callrec_rts_jtapi2 {start|stop|restart}"
```

7. Edit /opt/callrec/etc/callrec.derived

Add the following below line 47:

```
JTAPI2_PARAMS=" -logger /etc/callrec/jtapi.log4j.properties -config $ZOOM_CONFIG/sniffers2"
```

Add the following below line 133:

```
PID_RTS_JTAPI2="$PID/rts_jtapi2.pid"
```

8. Copy /opt/callrec/etc/sniffers.xml to /opt/callrec/etc/sniffers2.xml for instance:

```
cp /opt/callrec/etc/sniffers.xml /opt/callrec/etc/sniffers2.xml
```

9. Edit /opt/callrec/etc/core.xml

Add the following below line 58:

```
<EqualGroup name="reader">  
<Value name="name">JtapiReader2</Value>  
<Value name="server">SnifferServer</Value>  
<Value name="port">30301</Value>  
</EqualGroup>
```

10. Edit /opt/callrec/etc/sniffers2.xml

Change line 6 to:

```
<Value name="bindName">remoteJTAPI2</Value>
```

Change line 15 to:

```
<Value name="port">30301</Value>
```

11. Edit /opt/callrec/etc/config_manager.xml

Add the following below line 60:

```
<EqualGroup name="manager">  
<Value name="id">sniffers2</Value>  
<Value name="class">cz.zoom.util.configuration.config.service
```

```
.FileSingleConfigurationManager</Value>
<Group name="view">
<Value name="file">sniffers.zip</Value>
</Group>
<Value name="configurationFile">sniffers2.xml</Value>
<EqualGroup name="mapping">
<Value name="source">servers</Value>
<Value name="target">_servers</Value>
<Value name="managerId">core</Value>
</EqualGroup>
</EqualGroup>
```

12. Start Call Recording using the command:

```
/etc/init.d/callrec start
```


19 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
```

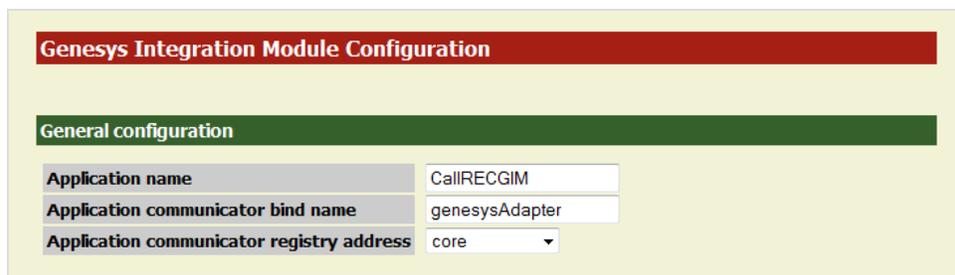
Configuring the Integration Module

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 rows of configuration fields:

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

Figure 144: 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	Reconnect enabled	YES ▾
Reload configuration	Reconnect time (sec)	30

Figure 145: 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 146: 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 11: 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

Figure 147: 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.

20 **Setting up Media Lifecycle Maintenance**

This chapter describes the Media lifecycle tools available in the Call Recording web interface to perform standard maintenance on the GQM system. Additional specialized maintenance tools including manually executed shell scripts are available from the command line interface.

This chapter contains the following sections:

[Managing the Media Lifecycle](#)

[Media Lifecycle Management Tools](#)

[Activating Changes, and Enabling Tools](#)

[Configuring Application Communicator](#)

[Archiving](#)

[Configuring Media Archive](#)

[Archiving and Deleting](#)

[Activating Deletion](#)

[Configuring Backup](#)

[Configuring Restore](#)

[Restored calls](#)

[Notifying Admin of a Restore Request](#)

[Synchro](#)

[Configuring the Replay Server Synchro Settings](#)

[Configuring Delete](#)

[Delete Database Records](#)

[Configuring Media Relocation](#)

[Restarting the Relocation Tool](#)

[Configuring the Disk Space Monitor](#)

[Viewing Disk Usage in the Disk Space Monitor](#)

[Custom Triggers](#)

[Alternative Source Paths](#)

[Alternative Target Paths](#)

[Time Specification](#)

Managing the Media Lifecycle

Regulations mandate the recording of calls in many industries. In some industries these recordings must be retained for years. This is a large amount of data. Contact centers record thousands of calls a day. To avoid running out of disk space on the recording server, manage the data by archiving, deleting, or relocating the data.

The recordings are useful for:

- evaluation
- training
- quality assurance
- settling disputes

Recent recordings of media files need to be available immediately. Media files must be stored on a hard drive for a period of time; after this initial period, some delay can be tolerated in accessing older files. It is generally sufficient to store older files in an archive. Hard drive storage is more expensive than archive storage, so where the media is stored is a trade-off between cost and availability. The Media Lifecycle tools enables the user to make the most efficient use of the storage by ensuring that media is stored in the appropriate type of storage.

How long to the media files on the recording server depends on business need and company policy.

How long data is archived depends on legal and regulatory requirements and company policy.

Media Lifecycle Management Tools

Media Lifecycle Management tools set up rules to store media. The tools are set up once and left running independently. External data can be used to specify the media to be affected. Multiple source and target paths can be used to specify more storage areas.

Navigate to **Settings > Configuration > Maintenance** to configure the Media Lifecycle tools.



Figure 148: Global Configuration

- **Global Configuration** contains settings for the application communicator used by maintenance tools.
- **Archive** contains settings for archiving of recordings and old database records.
- **Backup** contains settings for backing up files and database records, usually for disaster recovery.
- **Restore** contains settings for restoring files from backups.
- **Synchro** contains settings for synchronization between Call Recording servers in a multi server environment
- **Delete** contains settings for deleting files and related database records.
- **Relocation** contains settings for the relocation of files with the relevant database changes.
- **Disk Space Monitor** contains settings for the Disk space Monitor.

Activating Changes, and Enabling Tools

Media Lifecycle Management tools must be enabled and changes must be activated before they take effect.

Activating Tool Configuration Changes

To activate tool configuration changes in a tool, run a command line script to restart the tool. For example:

To restart just the delete tool after configuration changes use the following command:

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

To restart all tools use the following command:

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

Enabling Tools

The tools must be enabled at all three levels for them to function. To enable the tools:

1. Select the **Tools** service in Call Recording setup (callrec.conf).
2. Select the **Enabled** checkbox on each individual task level.
3. Navigate to **Global Configuration Settings > Configuration > Maintenance > Global Configuration:**
 - ensure that the details are correct in the Application Communicator Setting.
 - ensure that there is a valid email address for the Admin email address.

Running Tasks

The following tasks may be run as a Daemon, run manually as a one-shot task, or run once each day using cron:

- **Archive**
- **Backup**
- **Synchro**
- **Delete**
- **Relocation**

The **Daemon sleep period** determines the intervals between the daemon running.

If **Run as Daemon** is selected for a task, that task cannot be run manually as a one shot task. To invoke the daemon, restart the tool.

If **Run as Daemon** is not selected, then the tool is run each day, for example at midnight, the time is set by the `/etc/cron.d/callrec cron` configuration settings.

Restore is always run as a daemon.

Starting the Tools Manually One-shot

Ensure tools are active in `/etc/callrec/callrec.conf`.

To start the tools manually, use the following commands:

```
/opt/callrec/bin/tools
```

One-shot start of delete tool:

```
/opt/callrec/bin/deletetool
```

One-shot start of relocation tool:

```
/opt/callrec/bin/relocation
```

One-shot start of archive tool:

```
/opt/callrec/bin/archive
```

Restarting a Tool to Run Continually

The tool must be in daemon-mode.

Use these commands to restart each tool individually:

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

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

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

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

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

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

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

Troubleshooting

`/opt/callrec/logs/tools.log` shows all tools activities.

After a migration or upgrade ensure that the user `callrec` has access to the target directories for Archive and Restore. The command for changing the permission is:

```
chown callrec:callrec <path_to_directory>
```

Configuring Application Communicator

To configure **Global Configuration** navigate to **Settings > Configuration > Maintenance > Global Configuration**.

The **Global Configuration** tool contains one set of parameters: **Application Communicator Setting**.

The screenshot displays the 'Global Configuration' web interface. On the left is a sidebar menu with the following items: Global Configuration (highlighted), Archive, Backup, Restore, Synchro, Delete, Relocation, and Disk Space Monitor. The main content area has a red header 'Global Configuration'. Below it is a green header 'Application Communicator Setting'. This section contains five rows of configuration fields: 'Registry address' (a dropdown menu with 'core' selected), 'From address' (text input with 'notifier@yourcompany'), 'From name' (text input with 'CallREC Notifier'), 'Admin email address' (text input with 'admin1@yourcompany'), and 'SMTP server' (text input with 'your.smtp.host'). Below this is another green header 'Centera Configuration'. This section contains three rows of configuration fields: 'Full path to PEA file' (text input), 'Server name' (text input), and 'Server IP' (text input followed by ': 0'). At the bottom left of the main content area are two red buttons: 'Save configuration' and 'Reload configuration'.

Figure 149: Maintenance Global Configuration

1. Select the **Application Communicator** used by maintenance tools from the predefined list of **Registry addresses**.
2. Type the **From address** (name@domain.com) and **From name** (name of email sender).
3. Type the **Admin email address** (name@domain.com) – the recipient of maintenance messages.
4. Type the **SMTP server** host / IP address to enable email delivery.
5. Click **Save configuration**.

The **Centera Configuration** section is presently only for Support <http://genesyslab.com/support/contact>.

Archiving

Archiving enables the retention of media files in different storage mediums. Archiving regularly ensures that there is always sufficient space locally to store the new calls.

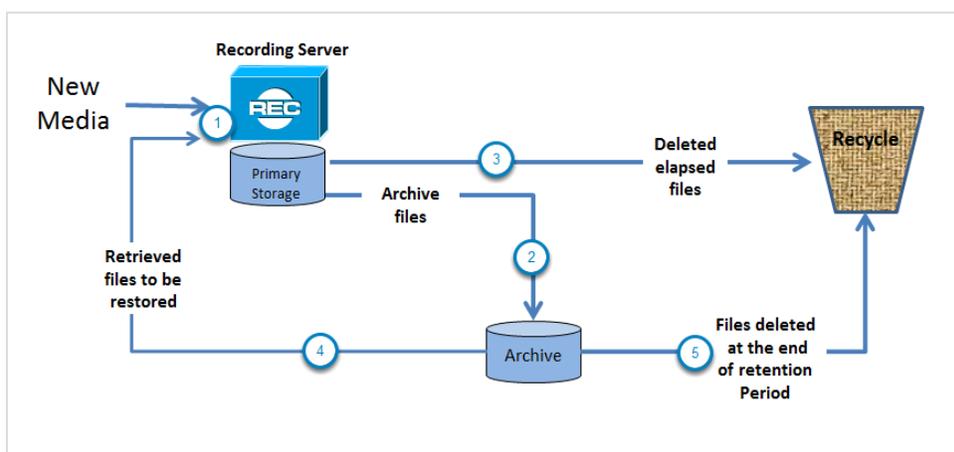


Figure 150: MLM Simple Archiving

1. The recorder records media files and the recording server stores this information as MP3s in a file system on its hard drives. The recording server also keeps a database of what files it has recorded and where the records are stored.
2. The Archive tool copies all non-archived MP3s to an archive file. Files that have been archived are marked so that they are not archived again. While the files are still on the recorder server, there are two copies of each file providing a backup. One copy on the server and one in archive saved as a zip file.
3. The MP3 files are stored on the recorder server's hard drive for a configurable period, for example, for six months. When that period has lapsed, the system checks that the MP3 files are marked as archived, and deletes them from the recorder file system.
4. The archived media files can still be accessed as they can be restored from the zip files using Restore. How long these restored files are available is configurable.
5. At the end of the retention period, the archived files are no longer needed and can be deleted from the archive by an administrator.

Configuring Media Archive

To configure archiving, navigate to **Settings > Configuration > Maintenance > Archive**.

Global Configuration

- Archive
- Backup
- Restore
- Synchro
- Delete
- Relocation
- Disk Space Monitor

Some values have been changed, changes are not saved.
Validation successful.

Media Archive Configuration

Enabled	<input checked="" type="checkbox"/>
Run as Daemon	<input checked="" type="checkbox"/>
Daemon sleep period (sec.)	60
Database pool	Maintenance
Subject	Archive Notification
Send to email	admin@acom.com
Send success emails	<input checked="" type="checkbox"/>
Send failure emails	<input checked="" type="checkbox"/>
Temporary directory	/tmp

Save configuration

Reload configuration

Figure 151: Configure Archive

1. Select the **Enabled** checkbox to enable the tool.
2. If the tool must run more frequently than once a day to even out performance, then select the **Run as Daemon** checkbox. Set a **Daemon sleep period** in seconds. If this field is empty when **Save configuration** is selected, the validation fails.
If the tool is required to run once a day, deselect the **Run as Daemon** checkbox and the tool runs as a one-shot task using Cron.
3. Type a subject for the notification email, for example, *Archive Notification*, and a valid email address. If these fields are empty, the validation fails.
4. Select the **Send success emails** checkbox to be informed by email of successful archiving.
Select the **Send failure emails** checkbox to be informed by email of failure.
5. Click **Save configuration**.

The Database pool should be set to **Maintenance**.

Temporary directory: full system path to temporary storage directory for example `/tmp`.

The `/tmp` file must have sufficient free space to accommodate the whole archive uncompressed. By default the temporary directory is 1 GB which is more than

sufficient if each individual archive file is no more than 650 MB. If the archive files need to be larger than 650MB then the temp file provided must be larger too. The temp file is where the MP3 are stored while they are being zipped.

Adding an Archive Task

Navigate to **Settings > Configuration > Maintenance > Archive**.

Figure 152: Add Archive Task

1. Enter a task name. Each task name must be unique. It is not possible to change a task name once it has been created.
2. Click **New**.

Figure 153: Enable Archive Task

1. Select **Enable this task**.

The **Centera Configuration** section is presently only for Support <http://genesyslab.com/support/contact>.

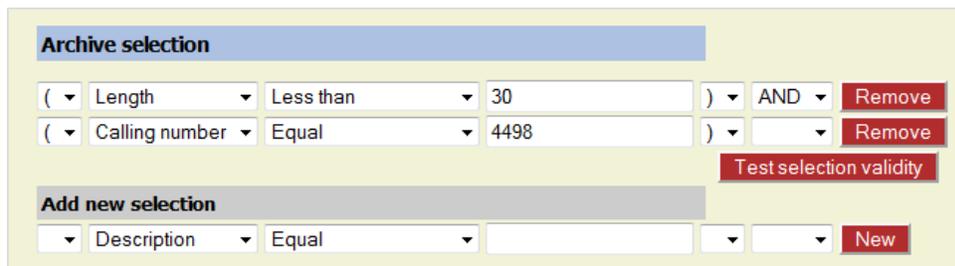
2. Select an **Interval period** from the drop-down list or specify a custom period by selecting **Use custom interval period**.
If **Use custom interval period** is selected, define the interval in the Custom interval period field. Use the standard Call Recording time specification format, described in the section [Time Specification](#).
3. Enter a unique name for the file. Only the first 6 characters of the prefix form the file name.
4. Set the archive maximum size in MB.

5. Optionally select **Archive not decoded streams** to archive .pcap files, the default is to archive MP3 files.
6. Optionally select which media type to exclude the choices are **Audio**, **Video** and **Nothing**.
7. Optionally select the **Exclude RECD** checkbox to exclude RECD files (raw screen captures).
8. Optionally select the **Delete archived files** to delete files as they are archived. Once deleted the original files cannot be recovered, only the zipped archive version exists.

To test the validity click **Save configuration**.

Selecting an Archive

Navigate to **Settings > Configuration > Maintenance > Archive**.



The screenshot shows a web interface for configuring archive selection. It features a section titled "Archive selection" with a blue header. Below this header, there are two rows of filter criteria. The first row shows a dropdown menu with "Length" selected, followed by a dropdown with "Less than", a text input field containing "30", a dropdown with "AND", and a red "Remove" button. The second row shows a dropdown menu with "Calling number" selected, followed by a dropdown with "Equal", a text input field containing "4498", a dropdown with a blank space, and a red "Remove" button. To the right of these rows is a red "Test selection validity" button. Below the filter rows is a section titled "Add new selection" with a grey header. This section contains a dropdown menu with "Description" selected, a dropdown with "Equal", a text input field, a dropdown with a blank space, and a red "New" button.

Figure 154: Archive Selection

To add a new selection filter for the task above:

1. Select a **Description**, **File path**, **Length** in seconds, **Calling number**, or **Called number** from the drop-down list.
2. Select a comparison expression. The alternatives are: **Equal**, **Not equal**, **Bigger than or equal**, **Less than or equal**, **Exist**, **Not exist**, **Begin**, **End**, **Contain**, **Regular expr..**
3. Enter an appropriate value, for example, 30 in seconds for the length or 4498 for the calling number.
4. Select a Boolean operator, for example, **AND** or **OR**, if there is another row to follow with further selection criteria.
5. If necessary click **New** to add a new row. To create a new filter use **Add new selection**.

Archive source paths

If no source path is set then all files stored in db are archived.

Additional paths	Priority	Balance	Low Watermark (MB)
Add alternative source paths			
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
New			

Archive target paths

If no target path is set default target path is used.

Default target path

Additional paths	Priority	Balance	High Watermark (MB)
Add alternative target paths			
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
New			

Figure 155: Archive Source Paths

Archive Source Paths: identify alternative sources for identifying files to be archived during the task. Unless at least one path is set, the task archives all files in the default database source path.

Archive Target Paths: designate alternative storage paths for files archived in this task.

Priority: Sets the priority for the target path.

Balance: Sets the load balancing for the archive task.

Watermark: Sets the capacity trigger for file storage.

Starting the Archive Tool Manually One-shot

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

Ensure tools are active in `/etc/callrec/callrec.conf`.

To start the tools manually, use the following command:

```
/opt/callrec/bin/archive
```

Restarting the Archive to Run Continually

The tool must be in daemon-mode. Use an SSH client. Log in as `admin`. Enter `su -` to log in as the root user. Enter the password, the default is `zoomcallrec`.

Use the following command:

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

Linux

In `/home/admin` view a file called `archive*` with a `.zip` extension, an associated file size and date.

In `/opt/callrec/data/calls`, select the associated date for the calls just archived. Open the file. View the MP3 files and associated details.

GUI

In **Recorded Calls** view all affected calls with the archived icon.

Archiving and Deleting

Call Recording archives older call recordings, storing them offline, and deletes the call recordings from the recording server. The call data remains available, and still displays in Call Recording. When a call is archived but not deleted, it behaves as a normal call recording.

Activating Deletion

Navigate to **Settings > Configuration > Maintenance > Archive**.

Scroll to an existing task.

Older than previous month		Remove
Enable this task	<input checked="" type="checkbox"/>	
Store in Centera	<input type="checkbox"/>	
Retention class	delete after 5yrs	
Interval period	Yesterday	
Archive filename prefix	archive	
Archive max size (MB)	650	
Archive not decoded streams	<input type="checkbox"/>	
Exclude media type	NOTHING	
Exclude RECD	<input type="checkbox"/>	
Delete archived files	<input checked="" type="checkbox"/>	

Save configuration
Reload configuration

Figure 156: Activate Delete Archived Files

1. Select the **Delete archived files** checkbox to delete the archived files.
2. Click **Save configuration**.

Viewing Results

Selecting the deletion of archived calls produces the following results:

Linux

In `/home/admin` there is a file called `archive*` with a `.zip` extension, an associated file size, and date.

In `/opt/callrec/data/calls`, select the associated date for the archived calls. Open the file. It is empty.

GUI

In the **Recorded calls** tab, all selected calls with the archived icon can be viewed. An additional icon shows that the call has been deleted.

When a call has been both archived, and or backed up, and deleted from the main database, the call must be restored to be able to listen to it again.

Configuring Backup

With the **Backup** tool, all files are backed up whether they are archived or not. A delete tool must be configured to delete any files that are no longer needed on the recording server.

Navigate to **Settings > Configuration > Maintenance > Backup**.

Global Configuration	
Archive	
Backup	
Restore	
Synchro	
Delete	
Relocation	
Disk Space Monitor	
Save configuration	
Reload configuration	

Media Backup Configuration	
Enabled	<input checked="" type="checkbox"/>
Run as Daemon	<input type="checkbox"/>
Database pool	Maintenance
Subject	Backup Notification
Send to email	admin@acom.com
Send success emails	<input checked="" type="checkbox"/>
Send failure emails	<input checked="" type="checkbox"/>
Temporary directory	/tmp

Figure 157: Configure Backup

1. Select the **Enabled** checkbox to enable **Backup**.
2. Select a **Database pool** from the drop-down list.
3. Ensure there is a valid email address and set a subject for the email. If these fields are empty when **Save configuration** is selected, then the validation fails.
4. Check **Send success emails** to be informed by email of successful archiving.
Check **Send failure emails** to be informed by email of failure.
5. Use the default `/tmp` **Temporary directory** . If the directory is changed then ensure that the `callrec` user has read and write permissions in the new directory.
6. Click **Save configuration**.

Backup cannot run as daemon.

Creating a Backup Task

Navigate to **Settings > Configuration > Maintenance > Backup**



Figure 158: Add Backup Task

1. Enter a unique task name for the new task. It is not possible to change a task name once it is created.
2. Click **New**. The form below appears.

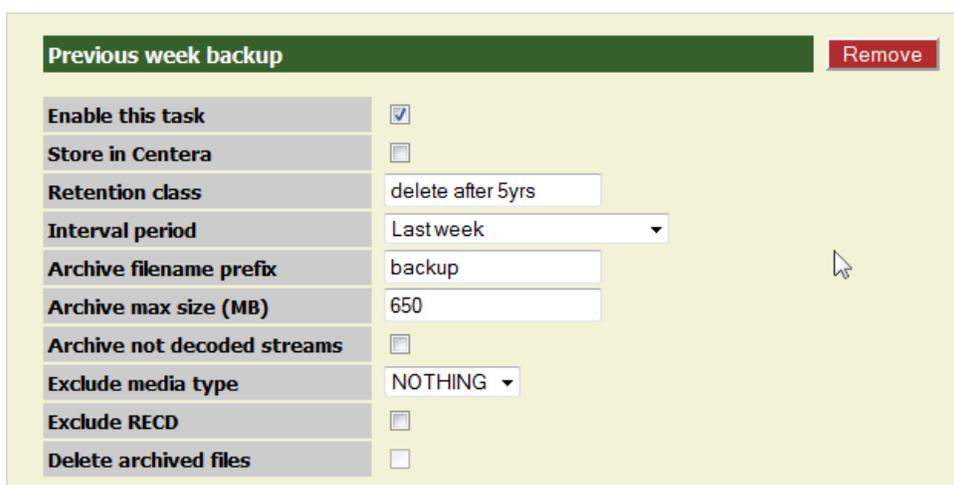


Figure 159: Enable the Backup Task

3. Select the **Enable this task** checkbox to enable the task.
4. Select an **Interval period** or enter a custom interval period.
Only the first 6 characters of the prefix forms the file name.
5. Set the **Archive max size (MB)**. Default value 650 MB.
6. To archive .pcap files, select this box, the default is to archive MP3 files.
7. Select the media type to exclude.
8. **Exclude RECD** excludes raw image files.
9. To delete files as they are archived select **Delete archived files**.

Test selection validity, click **Save configuration**.

Ensure tools are active in `/etc/callrec/callrec.conf`.

Starting the Backup Tool Manually One-shot

One shot run:

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

Enter the following command:

```
/opt/callrec/bin/backup
```

Starting the Backup Tool Manually Continually Using Cron

In the Linux console, enter the command:

```
/opt/callrec/bin/backup start
```

Note that the Archive tool running in Cron (non-daemon mode) is most commonly used as backup does not mark archived files in db.

Viewing Results

Note that `/home/admin` is default path but can be changed.

Linux

In `/home/admin` there is a file called `backup*` with a `.zip` extension, an associated file size, and date containing the html, xml, and media files.

GUI

There is nothing reflected in GUI: backing up files does not affect the database. When a call is archived (and/or backed up) and deleted from the main database, the call must be restored to be able to listen to it again.

Configuring Restore

Calls can be restored, backed up, and archived when they have been deleted from the main database and made available to users. The user makes a request identifying the calls to be restored, and the restore function periodically checks for these calls and makes them available in the user interface under the **Restored calls** tab.

Navigate to **Settings > Configuration > Maintenance > Restore**.

Figure 160: Restore Configuration

1. Select the **Enabled** checkbox.
2. Select the correct **Database pool** from the drop-down list.
3. Set the **Daemon sleep period (min.)**. If this field is empty when **Save configuration** is selected, then the validation fails.
4. The **Restore ZIP from directory** location should be the target location of the archived files.
5. There are two options for **Restore based on**:
 - **Restore based on UI requests**: once the file is archived, the file displays an icon in the **Recorded calls** list

. Click  and it is replaced by  indicating that the file is being restored. If selected, **Restore based on UI requests** processes these restore requests from the UI. The **Backup** operator is then responsible for copying the archive file back into the location from which Call Recording can restore just the file selected for restoration (that is, other files that have not been requested, that are archived in the same zip file are not restored). Once restored the **Recorded calls** list displays  showing that the call is restored and available to play.

- **Restore based on files:** provide a list of files to be restored, all files contained in the zip files containing the requested files are restored even if they have not been requested). Enter the **Archive filename** and **Archive file mask**.

Configuring Requests



The screenshot shows a web form titled "Restore Request" with a green header. The form contains the following fields and sections:

- Subject:** Restore Calls in Aug11
- Admin email address:** admin@yourco.com
- Restore target paths:** A blue header section.
- Restore to directory:** /opt/callrec/data/calls
- Additional paths:** Priority, Balance, High Watermark (MB)
- Add alternative target paths:** A blue header section.
- Buttons:** "Save configuration" (red), "Reload configuration" (dark red), and "New" (dark red).

Figure 161: Restore Request

1. Ensure there is a valid email address and set a subject for the email. If these fields are empty when **Save configuration** is selected, then the validation fails.
2. Calls are restored to the default restore directory unless another has been created.
3. Click **Save configuration**.

Starting the RestoreTool Manually

Ensure tools are active in `/etc/callrec/callrec.conf`.

Use an SSH Client. Log in as `admin`. Enter `su -` to log in as the root user.
Enter the password, the default is `zoomcallrec`. Enter the command:

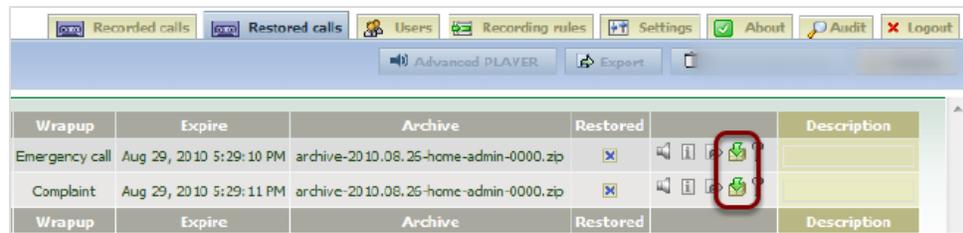
```
/opt/callrec/bin/restore start
```

Viewing the archived files

In `/opt/callrec/data/calls` select the associated date for the calls archived. Open the file. View the MP3 files and associated details.

Restored calls

Once the archive and deleted calls are selected for restore, the restored calls appear in the **Restored calls** tab.



Wrapup	Expire	Archive	Restored	Description
Emergency call	Aug 29, 2010 5:29:10 PM	archive-2010.08.25-home-admin-0000.zip	⏮ ⏪ ⏩ ⏭ 🎧	
Complaint	Aug 29, 2010 5:29:11 PM	archive-2010.08.25-home-admin-0000.zip	⏮ ⏪ ⏩ ⏭ 🎧	
Wrapup	Expire	Archive	Restored	Description

Figure 162: Restored Calls

The icon changes from call available for restore to the play icon that enables the user to listen to the call.

Another icon appears when the call is restored.

Setting the Expiration Time

This sets how long the media file is available.

Navigate to **Settings > Configuration > Web UI > Web Interface**.



Figure 163: Set Expiration Time

Scroll to **Media Restore**:

1. Enter a **Restore expiration time (Days)** for the media in days.
2. Click **Save configuration**.

Notifying Admin of a Restore Request

The screenshot shows a web-based configuration form titled "Restore Request". The form has a green header bar with the title. Below the header, there are several sections:

- Subject:** A text input field containing "Restore Calls in Aug1".
- Admin email address:** A text input field containing "admin@yourco.com".
- Restore target paths:** A blue header bar.
- Restore to directory:** A text input field containing "/opt/callrec/data/calls".
- Additional paths:** A section with three sub-fields: "Priority", "Balance", and "High Watermark (MB)".
- Add alternative target paths:** A blue header bar.
- Buttons:** On the left, there are two red buttons: "Save configuration" and "Reload configuration". On the right, there are four empty text input fields and a red "New" button.

Figure 164: Restore Request

When a user restores a file, a notification email is generated and sent by Call Recording.

- **Subject:** type the default subject line for email notifications.
- **Admin email address:** type the email address used for receiving restore notifications (system.administrator@domain.com).
- **Restore target paths:** enables the user to designate alternative storage paths for files restored in this task.
 - Priority :** sets the priority for the target path.
 - Balance:** sets the load balancing for the restore task.
 - High Watermark (MB):** sets the capacity trigger for file storage.

Synchro

Synchro is required only if a replay server is used.

At the central location in a multi site deployment, the replay server uses Synchro to collect sound and video files and database records from remote recorders for centralized playback, storage, life cycle management, and user access. Synchro always runs as a daemon.

Each of the recording servers supplying sound and video files must be configured using the command line.

Configuring the Replay Server Synchro Settings

To set up the replay server, navigate to **Settings > Configuration > Maintenance > Synchro**.

Synchro Settings	
Enabled	<input type="checkbox"/>
Run as Daemon	<input checked="" type="checkbox"/>
Daemon sleep period (sec.)	10
Calls to process in one period	200
Synchronize couples without streams	<input type="checkbox"/>
Synchronize voice tags	<input checked="" type="checkbox"/>

Source Setup	
Mark erroneous	<input type="checkbox"/>
Only processed calls	<input checked="" type="checkbox"/>

Figure 165: Synchro Settings

1. Select the **Enabled** checkbox to enable Synchro.
2. Set a **Daemon sleep period (sec.)** in seconds. The default is 10 seconds. If this field is empty when **Save configuration** is selected, the validation fails. The daemon sleep period affects how often the daemon runs and therefore the load on the processor. Increasing the sleep period decreases the load on the processor.
3. Set the number of **Calls to process in one period**. The default is 200.

Important:

Do not enable the **Synchronize couples without streams** option. Although not present in the Web GUI screen, the `onlyfinished` option present in the `/opt/callrec/etc/tools.xml` configuration file, `synchro` section must be set to `true`, as it is by default, otherwise Synchro attempts to synchronize calls before the MP3 is created, and potentially causes major problems in operation.

Only enable **Mark Erroneous** if there are problems synchronizing. **Mark Erroneous** marks calls that failed during synchronization, and the daemon ignores these for the next run. This prevents the daemon from attempting to synchronize the same damaged calls over and over again.

With **Only processed calls** enabled, only processed recordings, not raw data, are synchronized (set as default). Disabling **Only processed calls** can only be done in the configuration, and is only used for trouble shooting purposes.

Adding a New Source

Navigate to **Settings > Configuration > Maintenance > Synchro**.

Add each recording server to be synchronized as a new source.



Figure 166: Add New Source

Type a unique name for the recording server in **Source Sysname**, for example `src1`.

Click **New**. A new section displays as below.

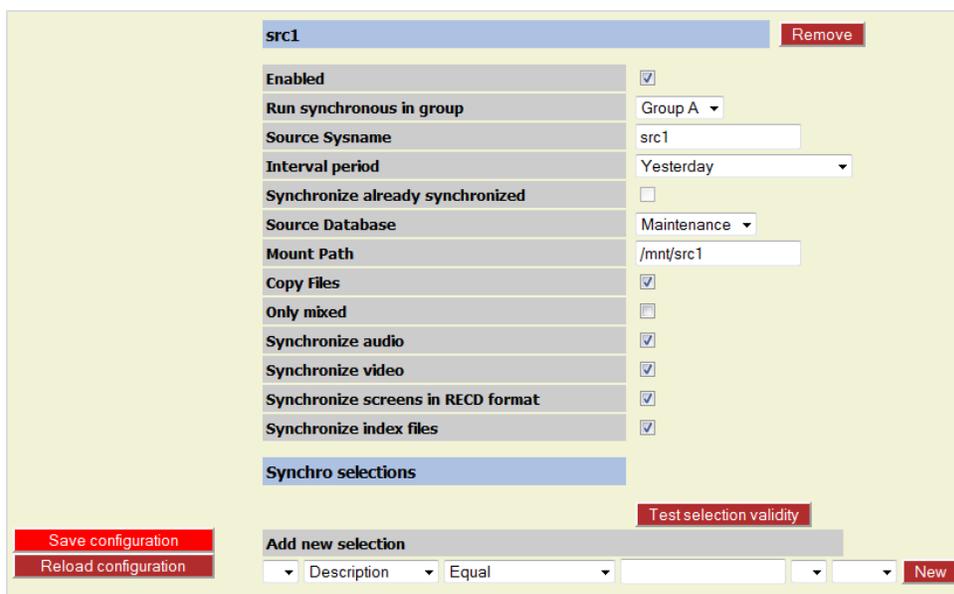


Figure 167: Synchro Source

To set the source parameters.

1. Select the **Enabled** checkbox to enable the source.
2. Select a group from the drop-down list **Run synchronous in group**.
3. Select one of the predefined intervals for synchronizing this recording server with the replay server from the **Interval Period** drop-down list. The options are: **Yesterday**, **Last Week**, **Last Month**, or **Use custom interval period**. If **Use custom interval period** was selected, then type the **Custom**

interval period in the field that displays. Use the standard Call Recording time specification format that is described in the section [Time Specification](#).

Synchronized already synchronized: By default this option is off. It is not recommended except for special situations where calls have been marked as erroneous. Contact <http://genesyslab.com/support/contact>.

4. Select the database pool of this source from the **Source Database** drop-down list (the database must be pre-defined in the **Settings > Call Recording Core > Database** part of the configuration interface).
5. Type the **Mount Path** for this source on the Replay server (each source must have a different, absolute mount path). This is the remote drive predefined in Linux that is used for additional archive storage for example.

Copy files default is enabled. When enabled, both files and database records are copied to the replay server. If disabled, only database entries are added to the master database, pointing to the original source files. This is only done exceptionally where large amounts of storage is available at the Recorder server. Disabling **Copy files** can add a significant delay when playing back, and for this reason normal practice is to leave this option enabled.

Only mixed: If enabled, this copies only Screen Capture video with accompanying audio tracks. If there is no audio, the Screen Capture video is ignored.

Synchronize audio: Enable audio synchronization.

Synchronize video: Enable video synchronization.

Synchronize screens in RECD format: enable RECD screens synchronization.

Click **Save Configuration**.

Setting up the Target

The target or replay server is where calls from all recorder servers are stored. There can only be one target. Navigate to **Settings > Configuration > Maintenance > Synchro**.

Figure 168: Target Setup

Target Parameters:

- **Target Sysname:** the name of the target server used by Call Recording for identification. Has to be unique.
- **Target Database:** the database pool of the target (must be defined in the **Settings > Configuration Call Recording Core > Database** part of the configuration interface).
- **Default Target Path :** where to store synchronized files.
- **Additional Paths:** designate alternative storage paths for files synchronized in this task.
 - Priority :** sets the priority for the target path.
 - Balance:** sets the load balancing for the restore task.
 - Watermark:** sets the capacity trigger for file storage.
- **Synchro video target paths (optional):** set default and additional video target paths for synchronization.
- **Synchro Source and Target Duplication:** the target database cannot be the same as a source database. Configuring the system in this way is not supported.

Restarting the Synchro Tool

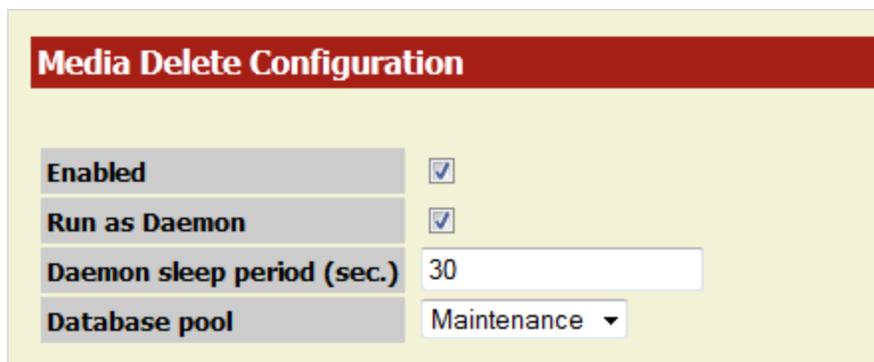
Use an SSH client. Log in as `admin`. Enter `su -` to log in as the root user.
Enter the password, the default is `zoomcallrec`.

To restart the Synchro tool use the following command:

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

Configuring Delete

Call Recording enables users to set deletion parameters for the system to free up storage space after calls have been archived. Navigate to **Settings > Configuration > Maintenance > Delete**.



The screenshot shows a web form titled "Media Delete Configuration" with a red header. The form contains four rows of configuration options:

Media Delete Configuration	
Enabled	<input checked="" type="checkbox"/>
Run as Daemon	<input checked="" type="checkbox"/>
Daemon sleep period (sec.)	<input type="text" value="30"/>
Database pool	<input type="text" value="Maintenance"/>

Figure 169: Deletion Parameters

1. Select the **Enabled** checkbox to activate the deletion function. If unselected, the delete tool is disabled.
2. **Run as Daemon**: if not selected to run as daemon, the script can be either run manually or it is run each day at midnight, according to `/etc/cron.d/callrec` cron configuration settings.
3. Enter the **Daemon period sleep time (sec.)**: defines the frequency for running the daemon in seconds.
4. Select the **Database pool** from the drop-down list. Choose database pool, that is used as the source for call related data, defined in **Settings > Configuration > Call Recording Core > Database tab**.

Configuring Delete Calls, Delete Recorded Screens, Delete Screens in Recd Format, and Delete Index Files

Navigate to **Settings > Configuration > Maintenance > Delete** and scroll down.

Delete Calls		Delete Screens in Recd Format	
Enabled	<input checked="" type="checkbox"/>	Enabled	<input type="checkbox"/>
Interval period	Use custom interval period ▾	Interval period	Use custom interval period ▾
Custom interval period	older than 12 months	Custom interval period	older than 6 months
Only if synchronized	<input type="checkbox"/>	Only if synchronized	<input type="checkbox"/>
Only if backed up	<input checked="" type="checkbox"/>	Only if backed up	<input checked="" type="checkbox"/>
Delete database link	<input type="checkbox"/>	Delete database link	<input type="checkbox"/>
Delete Recorded Screens		Delete index files	
Enabled	<input type="checkbox"/>	Enabled	<input type="checkbox"/>
Interval period	Use custom interval period ▾	Interval period	Use custom interval period ▾
Custom interval period	older than 6 months	Custom interval period	older than 12 months
Only if synchronized	<input type="checkbox"/>	Only if synchronized	<input type="checkbox"/>
Only if backed up	<input checked="" type="checkbox"/>	Only if backed up	<input checked="" type="checkbox"/>
Delete database link	<input type="checkbox"/>	Delete database link	<input type="checkbox"/>

Figure 170: Delete Calls

There are four blocks identifying parameters for deleting calls, recorded screens, indexes and database records.

1. **Enabled:** enables automatic deletion.
2. Select an **Interval period** between deletions from the drop down list or specify a custom period by selecting **Use custom interval period**.
3. If **Use custom interval period** is selected, define the interval in the Custom interval period field. Use the standard Call Recording time specification format, described in the section [Time Specification](#).
4. **Only if synchronized:** only deletes records that have already been synchronized, for example, copied to another mirror.
5. **Only if backed up:** enabled by default. Only deletes records that have already been backed up, for example, records stored in an archive created by the Backup tool.
6. **Delete database link:** deletes database references to deleted calls and screen video captures.

Delete Database Records

Navigate to **Settings > Configuration > Maintenance > Delete** and scroll down.

Figure 171: Delete Database Records

The first five parameters are the same as for Delete Calls, Recorded Screens, and Screens in Recd Format.

Additional parameters for **Delete Database Records**:

Delete selection, this applies to all enabled delete tasks.

1. To add a new selection criteria, click **New**. Select a **Description**, **File path**, **Length** (in seconds), **Calling number**, or **Called number** from the drop-down list.
2. To remove a selection, click **Remove**.
3. **Enable Source Watermarks**: enables the watermark feature if selected. The watermark sets the capacity trigger for file deletion.

4. To Add an alternative source path to the main source enter the following information:
 - Type the full path to the new source in **Additional paths** for files to be deleted in this task.
 - **Priority** between 1 (highest) and 10 (lowest) sets the priority for the target path.
 - **Balance** between 1 and 100 sets the load balancing for the restore task.
 - **Low Watermark** is the amount of remaining disk capacity, in MB, for file storage that triggers deletion. Set this as a percentage of the whole disk, for example, 14,000 MB is 10% of a 140 GB drive, and deletion is triggered when less than this amount of free disk space is available.

Click **New** and the application validates the entries. Any field that does not pass the validation appears with the text in red on a pink background. Click **Save configuration** and then **Reload configuration** to see the changes.
5. To remove a source path click **Remove**.

Starting the Delete Tool Manually One-shot

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

To start the delete tool one-shot enter the following command:

```
/opt/callrec/bin/deletetool
```

Restarting the Delete Tool to Run Continually

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

To restart the delete tool to run continually:

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

Configuring Media Relocation

Stored calls and screen captures can be periodically relocated elsewhere in the Call Recording system. This is to help with data storage optimization and ensure that there is always enough disk space available to continue recording calls and screen captures. Relocated calls can still be played through the Call Recording Web GUI interface. Navigate to **Settings > Configuration > Maintenance > Relocation**.

Media Relocation Configuration

Enabled

Run as Deamon

Daemon period sleep time (sec.)

Database pool Maintenance ▾

Calls Relocation Setting

Enabled

Interval period

Relocation source paths

Default source path

Additional paths **Priority** **Balance** **Low Watermark (MB)**

Add alternative source paths

Relocation target paths

Default target path

Additional paths **Priority** **Balance** **High Watermark (MB)**

Add alternative target paths

Figure 172: Maintenance - Relocation

- **Enabled:** activates relocation function. If unselected, the relocate tool is disabled.
- **Run as Deamon:** enables running relocation as a daemon.
- **Daemon period sleep time (sec.):** defines frequency for running the daemon in seconds.

- **Database pool:** choose the database pool to be used as a source for call related data, defined in the **Settings > Call Recording Core > Database tab**.

Parameters for Calls, Screens and Recd Relocation:

- **Enabled:** enables or disables relocation.
- **Interval period:** sets the time period for relocating records. All records that have been saved from this time to the present are relocated. The interval period can be selected from the drop-down list, or specify a custom period by selecting use custom interval period option and defining the interval in the Custom interval period field. Use the standard Call Recording time specification format, which is described in the section [Time Specification](#).
- **Default source path:** is the default source directory for saved calls and screens.
- **Additional paths:** designate alternative source paths for files relocated in this task.
 - Priority:** sets the priority for the target path.
 - Balance:** sets the load balancing for the restore task.
 - Watermark:** sets the capacity trigger for file storage.
- **Default target path:** a **Relocation target path** must be set to relocate data to, in each of the following: **Calls Relocating Setting, Screen Relocating Setting and Recd Relocating Setting**. The administrator must allocate volumes for long term storage of the calls, screens and recd files. The relocation target path must have permissions set that enables Call Recording to access files for media playback.
- **Additional paths:** enables the user to designate alternative target paths for files relocated in this task.
 - Priority :** sets the priority for the target path.
 - Balance:** sets the load balancing for the restore task.
 - Watermark:** sets the capacity trigger for file storage.

Restarting the Relocation Tool

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

To restart the Relocation tool use the following command:

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

Configuring the Disk Space Monitor

The Disk Space Monitor, displays the amount of free disk space for recording and can send warnings when disk space goes below a certain threshold of days capacity.

To configure the Disk Space Monitor:

Navigate to **Settings > Configuration > Maintenance > Disk Space Monitor**.

Figure 173: Disk Space Monitor Settings

- To send warnings:
 - by email select the **Notify by email** checkbox.
 - by SNMP select the **Notify by SNMP** checkbox.
- Type email addresses in the **Email addresses** field separated by commas.
- Type the number of days warning that the system gives before recording space runs out in the **Warn when space will last (days)**. The system sends warning messages when it predicts that there are only this number of days left of recording at present consumption of disk space. For example:

"Warning: Volume /dev/sda1 (/mnt/disk1) is running out of the space, estimated time remaining is 3.5 day(s)."

Volume /dev/sda1 (/mnt/disk1): 27.5 GB used, 4.5 GB free space."
- If **Notify by SNMP** is selected type a name for the **SNMP trap destination**.

5. If **Notify by SNMP** is selected, then select the **SNMP version** from the drop-down list.
6. Click **Save configuration**.

Viewing Disk Usage in the Disk Space Monitor

To view Disk Usage in the Disk space monitor:

Navigate to **Settings > Disk Usage**.

The Disk space monitor displays the disk usage if there are more than twenty four hours of data available.

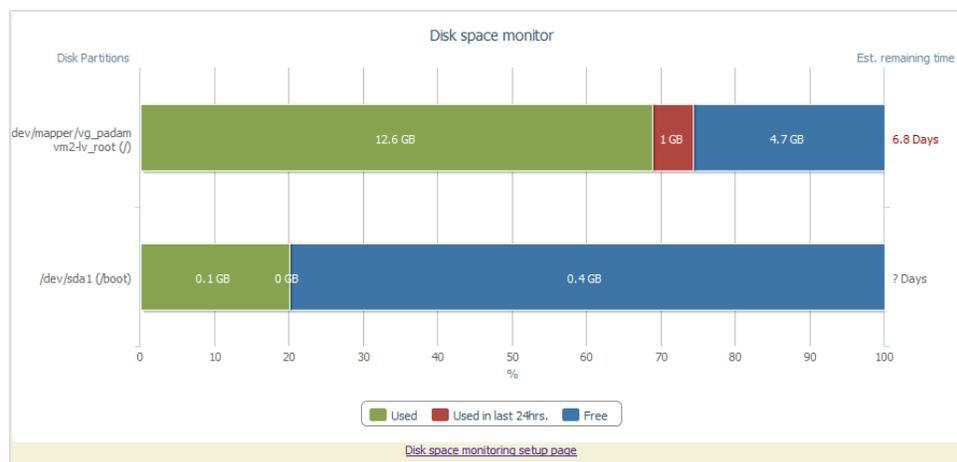


Figure 174: Viewing Disk Usage

The disk monitor displays any writable disk partitions and calculates the estimated remaining time in days, based on the average daily usage of the last seven days. If the disk monitor has a full week of data then the estimate is more accurate than if the disk monitor only has a little data.

Custom Triggers

Maintenance tools can be run based on custom event triggers defined by the administrator. Combine custom selection conditions for triggers with the Boolean operator “**AND**”. Available Call Detail Record (CDR) values for custom selection queries include:

- description
- call length (in seconds)
- file path
- called number
- calling number

This would make it possible, for example, to create a trigger to immediately archive all calls more than thirty minutes long upon call completion.

Available comparison expressions include:

- equals
- does not equal
- lesser than <
- lesser than or equal <=
- greater than >
- greater than or equal >=
- exists (for use with Calling number and Called number)
- does not exist (for use with Calling number and Called number)
- begins/ends with (for use with Calling number and Called number)
- contains (for use with Calling number and Called number)

Matching/Not matching regular expression (“regexp”)

Valid data types include:

- string
- num

Conditions may be combined using brackets and Boolean operators (AND/OR).

Alternative Source Paths

Generally, Call Recording conducts maintenance operations and Media Lifecycle Management tasks using the default source path defined during installation and configuration.

When Alternative Source Paths (ASPs) are specified, Call Recording ignores the default path, and instead applies the following rules:

- The highest priority ASP is searched first. (From 1-10, the lower the number, the higher the priority).
- Operations involving calls from multiple ASPs can be load balanced by assigning a balance coefficient to each ASP (from 1 to 100 percent).
- Watermarks can be defined to enable the user to set a capacity trigger. When a partition where calls are stored reaches the watermark level of used storage space, the calls are processed.

Alternative Target Paths

Generally, Call Recording conducts maintenance operations and Media Lifecycle Management tasks using the default target directory defined during installation and configuration.

When Alternative Target Paths (ATPs) are used, Call Recording ignores the default path, and instead applies the following rules:

- The highest priority ATP is used first for storing or moving calls. (From 1-10 the lower the number, the higher the priority.)
- Call storage can be load balanced by assigning a balance “weight” to each ATP (from 1 to 100 percent).
- Watermarks can be defined to set a capacity trigger. When a partition where calls are stored is below the watermark level of used storage space, Call Recording stores calls on that partition.

Time Specification

All dates must be in the format: DD.MM.YYYY. All times must be in the format: h:mm:ss. The hour must be in 24 hour format and may be one (0-9) or two digits (10-23). The **from** variable must be included first, then the **to** variable.

The time range for tools uses the following case sensitive parameters:

- `all`: all the time (without restriction)
- `today`: from today 0:00:00 to current time today
- `yesterday`: from yesterday 0:00:00 to today 0:00:00
- `tomorrow`: from tomorrow 0:00:00 to the day after tomorrow 0:00:00
- `this week`: from first day of current week 0:00:00 to current time today
- `last week`: from first day of last week 0:00:00 to first day of current week 0:00:00
- `this month`: from first day of current month 0:00:00 to current time today
- `last month`: from first day of last month 0:00:00 to first day of current month 0:00:00
- `this year`: from first day of current year 0:00:00 to current time today
- `last year`: from first day of last year 0:00:00 to first day of current year 0:00:00
- `daily`: from current time 1 day ago to current time today
- `weekly`: from current time 7 day ago to current time today
- `days=x`: from current time x days ago to current time today
- `start=s end=e`: from s to e
- `start=s days=x`: from s to s + x days
- `end=e days=x`: from e -x days to e
- `floatend=xMOD1 MOD2=y` - calls between now and (y MOD2 - x MOD1); MOD = minutes, hours, days
for example: `floatend=5minutes days=15` selects calls between current time today and (now + (15 days - 5 mins))
- `older than x MOD` - calls older than x MOD; MOD = minute, minutes, hour, hours, day, days, month, months)

Chapter

21 PCI DSS Compliance

This chapter describes PCI DSS Compliance and how each issue is addressed.

This chapter contains the following sections:

[PCI DSS Compliance Overview](#)

[GQM PCI Compliance Checklist](#)

[Vendor-supplied Default Passwords Are Not Used](#)

[Pause/Resume Functionality Is Enabled](#)

[Key Manager Is Active and Keys Are Valid for no Longer than 12 Months](#)

[Audio Files Are Encrypted](#)

[Video Files Are Encrypted](#)

[Web Access Is Encrypted](#)

[Audit Logs Are Collected](#)

[Password Management Is Enforced](#)

[Brute-force protection is enforced](#)

[Data Retention Policies Are Enforced](#)

[Encrypt Tool](#)

[Switching On Debug Logs](#)

[Password Storage in GQM](#)

PCI DSS Compliance Overview

PCI DSS (Payment Card Industry Data Security Standard) is a worldwide information security standard defined by the Payment Card Industry Security Standards Council, an organization founded by the key electronic payment providers including, American Express, Visa, Inc, and MasterCard Worldwide. The standard aims to reduce or prevent credit card fraud by requiring that organizations in the payment card industry implement increased controls around cardholder data, thereby minimizing its exposure to compromise.

Certification as “PCI DSS compliant” is mandatory for large numbers of organizations in the credit card payment industry; the standard applies to all organizations that hold, process, or exchange cardholder information from any card branded with the logo of one of the PCI SSC members.

Genesys GQM 8.1.5x introduces full compliancy with the following relevant PCI DSS directives:

Control Objectives	PCI DSS Requirements	GQM 8.1.5x
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data.	N/A
	2. Do not use vendor-supplied defaults for system passwords and other security parameters.	✓
Protect Cardholder Data	3. Protect stored cardholder data.	✓
	4. Encrypt transmission of cardholder data across open, public networks.	✓
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software on all systems commonly affected by malware.	N/A
	6. Develop and maintain secure systems and applications.	✓ (ongoing)
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know.	✓

Control Objectives	PCI DSS Requirements	GQM 8.1.5x
	8. Assign a unique ID to each person with computer access.	✓
	9. Restrict physical access to cardholder data.	N/A
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data.	✓
	11. Regularly test security systems and processes.	N/A
Maintain an Information Security Policy	12. Maintain a policy that addresses information security.	N/A

Table 12: PCI DSS Compliance

GQM PCI Compliance Checklist

The **PCI Compliance Status** screen is not visible in the Call Recording Web GUI until a valid license including the PCI Compliance feature is uploaded and Call Recording is restarted.

Navigate to **Settings > PCI Compliance** to view the PC Compliance Overall Status.

GENESYS
AN ALCATEL-LUCENT COMPANY

PCI Compliance Overall Status ❌

<https://www.pcisecuritystandards.org/>

Vendor-supplied default passwords are not used

- Vendor-supplied default passwords must be changed immediately upon first login

Pause/Resume functionality is enabled

- It should be possible to pause and resume the recording to protect sensitive data from being recorded

Key Manager is active and keys are valid for no longer than 12 months

- Key Manager must be up and running and its keys are to be valid for no longer than 12 months

Audio files are encrypted

- Encryption for audio files must be enabled

Video files are encrypted

- Encryption for video files must be enabled

Web access is encrypted

- Only HTTPS access can be used

Audit logs are collected

- Audit logs must be collected

Password management is enforced

- The system must ensure the minimum password strength. Each password must be at least 8 characters long, contain numbers or symbols. Passwords must be valid for no longer than 90 days. The new password must not be equal to at least 4 recent passwords.

Brute-force protection is enforced

- The number of unsuccessful login attempts before the account is locked must be no more than 6. The lockout period must not be less than 30 minutes.

Data retention policies are enforced

- Archive and delete tools must be enabled and configured

Figure 175: PCI DSS Compliance Status Screen

Sections marked with mean that this feature already complies with PCI DSS recommendations.

Sections marked with mean that this feature does not comply with PCI DSS recommendations and that further steps must be taken.

Ensure that the GQM license includes the **PCI Compliance** property, that enables the following features in GQM:

- **Key Manager**, for managing server and client encryption keys.
- The **PCI Compliance Status** page, in the Call Recording Web GUI at **Settings > PCI Compliance Status**, that displays if the GQM features influencing PCI Compliance are correctly configured within the GQM installation.

The following sub-topics cover how to achieve compliance for each requirement that displays on the **PCI Compliance Status** page.

Vendor-supplied Default Passwords Are Not Used

By default after installation, the first time the system administrator logs in to the Genesys Call Recording Web GUI using the default login credentials, the administrator is required to change the administrator password.

Resolution: none required.

Pause/Resume Functionality Is Enabled

This functionality is currently available via the Pause/Resume and RMI API for third party applications, see the Developer API Guide.

Resolution: none required.

Key Manager Is Active and Keys Are Valid for no Longer than 12 Months

PCI-DSS Compliance requires authenticated, encrypted transmission of data across networks (see Appendix A Encrypt Tool)– which includes between clients and servers in distributed systems like Genesys GQM. One of the functions of the Key Manager is to manage this secure transmission, including automatic transparent renewal of authentication certificates when they expire.

Resolution: install authentication and encryption certificates and activate Key Manager. See Activating Key Manager.

Self-Signed or Commercial Certificates

For standard production environments, use **commercially signed authentication certificates** with **Key Manager**. “Commercial certificates” are authentication certificates that are signed by a trusted commercial CA (Certificate Authority, such as, Thawte or Verisign).

Self-signed certificates are quick to create; they can be created during GQM setup by answering ‘yes’ to the query "Do you want to create a self-signed certificate and keys for Key Manager?" (see the Implementation Guide).

However, self-signed certificates are not as secure or trusted as commercial certificates, so they can provoke warnings and security errors, particularly when used with web technologies, see the SSL section in this Guide. Only use them for testing purposes.

Key Manager in Cluster Installations

To comply with PCI DSS recommendations, in cluster installations **Key Manager** must only be enabled on one server. Typically **Key Manager** is deployed on the server that runs Call Recording Core. The **Key Manager** service in the GQM is selected by default in the service list during setup so the **Key Manager** service must be deselected on all the other servers in the cluster.

The following security precautions must be taken:

- Remote access to the key store must not be possible.
- The directory where the keys are stored must be protected by file system permissions and should be only accessible for the **Key Manager** process and the **Key Manager** administrator.
- Keys for communication between **Key Manager** and **Key Manager** clients should be distributed using safe transport, for example, distributed physically on a USB stick or in protected SSH session.

There is a tool for importing and exporting certificates into and out of the key store.

Activating Key Manager

Activate **Key Manager** using the following procedure:

Either:

Opt to create **self-signed certificates and keys** during setup. These self-signed certificates are usually only used for test purposes during set up of the system. They are not recommended for use in a working environment.

Or:

Opt to use a **commercial certificate and keys**. In this case, do not create self-signed certificates and keys during setup, but after setup is complete, manually set up Key Manager with a commercial certificate and keys (see the [Installing Commercially Signed Certificates](#) section of this guide).

Enabling Encryption in Client Setup

Navigate to **Settings > Configuration > Key Manager > Client Setup**.

Client Setup	
Key Manager Server	
Server	keyManager
Encryption	
Enabled	<input checked="" type="checkbox"/>
Password file location	/opt/callrec/keys/enc/pwds.properties
Authentication keystore location	/opt/callrec/keys/enc/auth_keystore
Trust keystore location	/opt/callrec/keys/enc/trust_keystore
Algorithm	AES
Purpose	Audio
Minimum strength	0
Maximum strength	128

Figure 176: Activating Key Manager and Call Encryption

1. Select the **Enabled** checkbox in the Encryption section to enable Key Manager and call encryption.
2. Click **Save configuration**.

Important:

The **Key Manager** settings tab is not visible in the Call Recording Web GUI until a valid license including the PCI Compliance feature is uploaded, certificates, self-signed or commercial, installed and Call Recording restarted using the `service callrec restart` command.

In both cases, the key validation expiration dates are determined when generating the server keys, using the `keygen` command line tool. In the case of self-signed certificates created during GQM setup, an expiration date of 365 days is set (the maximum allowable period for PCI Compliance).

Installing Commercially Signed Certificates

Commercially signed certificates are created and installed using the following process. It is assumed that a Certification Authority (CA) such as Thawte or Verisign is available to process certificate signing requests:

- Generate server, encoder and decoder private keys and certificates.
- Generate certificate signing request (.csr) files for each certificate and send these for signing to the CA.
- Install a root (trust) certificate for the CA if required.
- Install the signed certificates from the CA in the server authorization store and encoder & decoder trust and authorization stores.
- Generate Key Manager encryption keys.

Installing Commercial Certificates for Key Manager

If self-signed certificates are installed, remove them before attempting to install commercial certificates as follows:

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

```
rm -rf /opt/callrec/keys
/opt/callrec/bin/rc.callrec_keymanager restart
Stopping CallREC Key Manager: ..... [ OK ]
Starting CallREC Key Manager: .... [ OK ]
```

Create keys directory, private keys and certificate request files.

1. Copy the following commands into a text file named `/home/admin/genkeys1.sh`, then modify the `CERTIFICATES_PASS` and `CERTIFICATES_PROPERTIES` information regarding password and organization details respectively.

```
#!/bin/sh
#
# Set up and create request files (.csr) for commercially signed
# certificates for Key Manager
# Genesys Labs, Inc. - GQM      8.1.5x
#
##### Modify as required #####
# Password for all certificate stores
CERTIFICATES_PASS=callrec
# Organizational details for certificates
# [first and last name, organizational unit, organization, city or
# locality,
# state or province, two-letter country code]
CERTIFICATES_PROPERTIES="CN=Administrator, OU=Dept, O=Company, L=City,
S=State, C=US"
#####
##### Standard CallREC defaults #####
CALLREC_HOME=/opt/callrec
ERR_FILE=/tmp/installcerts.err
KEYTOOL=/usr/java/default/bin/keytool
KEYS_DIR=$CALLREC_HOME/keys
ENC_DIR=$KEYS_DIR/enc
DEC_DIR=$KEYS_DIR/dec
PWDS_FILE=$KEYS_DIR/pwds.properties
#####
```

```

# Create CallREC keys directory if it doesn't exist
# Creating /opt/callrec/keys directory tree including pwds.properties
files
if [ ! -e $KEYS_DIR ] ; then
mkdir -p $KEYS_DIR
fi
if [ ! -e $ENC_DIR ] ; then
mkdir -p $ENC_DIR
fi
if [ ! -e $DEC_DIR ] ; then
mkdir -p $DEC_DIR
fi

# Generating content of PWDS file
echo "authpwd=$CERTIFICATES_PASS" > $PWDS_FILE
echo "trustpwd=$CERTIFICATES_PASS" >> $PWDS_FILE
echo "keystorepwd=$CERTIFICATES_PASS" >> $PWDS_FILE
echo "keyentriespwd=$CERTIFICATES_PASS" >> $PWDS_FILE
cp $PWDS_FILE $ENC_DIR
cp $PWDS_FILE $DEC_DIR

# Generating content of PWDS file
echo "authpwd=$CERTIFICATES_PASS" > $PWDS_FILE
echo "trustpwd=$CERTIFICATES_PASS" >> $PWDS_FILE
echo "keystorepwd=$CERTIFICATES_PASS" >> $PWDS_FILE
echo "keyentriespwd=$CERTIFICATES_PASS" >> $PWDS_FILE
cp $PWDS_FILE $ENC_DIR 2>&1 >> $ERR_FILE
cp $PWDS_FILE $DEC_DIR 2>&1 >> $ERR_FILE

# Create private certificates for server and encoder, decoder clients,
# then generate certificate signing request files (server.csr,
encoder.csr,
# decoder.csr) in the /home/admin directory
# NOTE: To export existing certificates instead, replace the '-certreq'
# parameter with '-exportcert', which will export a .cer type
# certificate file, e.g. server.cer.
# Server
$KEYTOOL -genkeypair -alias server -keyalg rsa -keysize 2048
-validity 365
-keypass $CERTIFICATES_PASS -keystore $KEYS_DIR/.auth_keystore -storetype
jks
-storepass $CERTIFICATES_PASS -dname "$CERTIFICATES_PROPERTIES"
2>&1 >> $ERR_FILE

$KEYTOOL -certreq -alias server -file /home/admin/server.csr
-keystore
$KEYS_DIR/.auth_keystore -storetype jks -storepass $CERTIFICATES_PASS

```

```

2>&1 >> $ERR_FILE

# Encoder
$KEYTOOL -genkeypair -alias encoder -keyalg rsa -keysize 2048 |
-Validity 365
-keypass $CERTIFICATES_PASS -keystore $ENC_DIR/.auth_keystore -storetype jks
-storepass $CERTIFICATES_PASS -dname "$CERTIFICATES_PROPERTIES"
2>&1 >> $ERR_FILE

$KEYTOOL -certreq -alias encoder -file /home/admin/encoder.csr
-keystore
$ENC_DIR/.auth_keystore -storetype jks -storepass $CERTIFICATES_PASS
2>&1 >> $ERR_FILE

# Decoder
$KEYTOOL -genkeypair -alias decoder -keyalg rsa -keysize 2048
-Validity 365
-keypass $CERTIFICATES_PASS -keystore $DEC_DIR/.auth_keystore -storetype jks
-storepass $CERTIFICATES_PASS -dname "$CERTIFICATES_PROPERTIES"
2>&1 >> $ERR_FILE

$KEYTOOL -certreq -alias decoder -file /home/admin/decoder.csr
-keystore
$DEC_DIR/.auth_keystore -storetype jks -storepass $CERTIFICATES_PASS
2>&1 >> $ERR_FILE

# Set permissions
# Changing key file ownership to callrec/callrec
chown -R callrec:callrec $KEYS_DIR 2>&1 >> $ERR_FILE

```

- Execute the following commands to run the file. Three '.csr' certificate signing request files (server.csr, encoder.csr, decoder.csr) are created in the /home/admin directory.

```

chmod 755 /home/admin/genkeys1.sh
/home/admin/genkeys1.sh

```

Obtain Signed Certificates

- Send the three certificate request files in the /home/admin directory to the chosen Certificate Authority (CA) and receive signed certificate files in return, upload them also to the /home/admin directory and rename them, if necessary, to server.cer, encoder.cer, decoder.cer.
- [OPTIONAL]** Install CA certificate file if CA is not include in the cacerts Java keystore.

5. Check for the existence of your CA in the `cacerts` keystore with the following command that lists all CA owner names (default password is `changeit`):

```
/usr/java/default/bin/keytool -list -v -keystore
/usr/java/default/jre/lib/security/cacerts | grep "Owner:"
```

6. To install a CA certificate, first modify the `-alias` and `-file` parameters in the following command to reflect a suitable reference name and location of certificate file before running it for certificate installation:

```
/usr/java/default/bin/keytool -importcert -alias myCA -file
/home/admin/myCA.cer
-keystore /usr/java/default/jre/lib/security/cacerts -storepass changeit
```

Install signed certificates and create encryption/decryption certificates

7. Copy the following commands into a second text file named `/home/admin/genkeys2.sh`, then modify the `CERTIFICATES_PASS` to match the value used for it in the earlier `genkeys1.sh` script.

```
#!/bin/sh
#
# Install signed certificates in Key Manager for encryption/decryption
# Genesys Labs, Inc. - GQM      8.1.5x
#
##### Modify as required #####
# Password for all certificate stores
CERTIFICATES_PASS=callrec
#####
##### Standard CallREC defaults #####
CALLREC_HOME=/opt/callrec
ERR_FILE=/tmp/installcerts.err
KEYTOOL=/usr/java/default/bin/keytool
KEYS_DIR=$CALLREC_HOME/keys
ENC_DIR=$KEYS_DIR/enc
DEC_DIR=$KEYS_DIR/dec
PWDS_FILE=$KEYS_DIR/pwds.properties
CACHED_CFG_SERVER_IP=localhost
DEFAULT_PORT="30400"
#####
# OPTIONAL: Import CA certificates (only required if CA is not included
# in java CACERTS keystore)
# View current CACERTS entries like this (default password: changeit)
#/usr/java/default/bin/keytool -list -v -keystore
#/usr/java/jdk1.6.0_35/jre/lib/security/cacerts | grep "Owner:"
```

```
#
# To install a CA certificate, uncomment the following line, and modify
# the -alias and -file parameters to reflect a suitable reference name and
# location of certificate file:
#/usr/java/default/bin/keytool -importcert -alias myCA -file
#/home/admin/myCA.cer -keystore /usr/java/jdk1.6.0_
35/jre/lib/security/cacerts
#-storepass changeit

# Import signed certificates received from your Certificate Authority (CA)
# Assumes that certificates are named server.cer, encoder.cer, decoder.cer
# in the /home/admin directory
# Server
$KEYTOOL -importcert -noprompt -trustcacerts -alias server -file
/home/admin/server.cer -keystore $KEYS_DIR/.trust_keystore -storepass
$CERTIFICATES_PASS 2>&1 >> $ERR_FILE

# Encoder (assumes CACERT certificate file is at $KEYS_DIR/.auth.cer)
$KEYTOOL -importcert -noprompt -trustcacerts -alias encoder -file
/home/admin/encoder.cer -keystore $KEYS_DIR/.trust_keystore -storepass
$CERTIFICATES_PASS 2>&1 >> $ERR_FILE

$KEYTOOL -importcert -noprompt -trustcacerts -alias server -file
/home/admin/server.cer -keystore $ENC_DIR/.trust_keystore -storepass
$CERTIFICATES_PASS 2>&1 >> $ERR_FILE

# Decoder (assumes CACERT certificate file is at $KEYS_DIR/.auth.cer)
$KEYTOOL -importcert -noprompt -trustcacerts -alias decoder -file
/home/admin/decoder.cer -keystore $KEYS_DIR/.trust_keystore -storepass
$CERTIFICATES_PASS 2>&1 >> $ERR_FILE

$KEYTOOL -importcert -noprompt -trustcacerts -alias server -file
/home/admin/server.cer -keystore $DEC_DIR/.trust_keystore -storepass
$CERTIFICATES_PASS 2>&1 >> $ERR_FILE

# Set permissions
# Changing key file ownership to callrec/callrec
chown -R callrec:callrec $KEYS_DIR 2>&1 >> $ERR_FILE

# Restart Key Manager
/opt/callrec/bin/rc.callrec_keymanager restart

# Create encryption/decryption keys using QM Suite genkeys utility
# Default activation date = today (or format: dd-mm-yyyy)
ACTIVATION_DATE=`date "+%d.%m.%Y"`
# Default expiration date = today + 365 days (or format: dd-mm-yyyy)
```

```
EXPIRATION_DATE=`date -d "+365 days" "+%d.%m.%Y"`
$CALLREC_HOME/bin/genkeys -activationDate $ACTIVATION_DATE
-algorithm AES
-expirationDate $EXPIRATION_DATE -purpose Audio -strength 128 -config
"//${CACHED_CFG_SERVER_IP}:${DEFAULT_PORT}/pci_compliance" 2>&1 >> $ERR_FILE
```

8. Execute the following two commands to run the file. Note the output below the commands.

```
chmod 755 /home/admin/genkeys2.sh
/home/admin/genkeys2.sh
```

If the certificate installation was successful the sample output should be similar to:

```
Certificate was added to keystore
0 [main] INFO cz.zoom.callrec.keyman.client.cmd.KeyGeneratorClient
- Fetched remote KeyVaultAdmin
287 [main] INFO cz.zoom.callrec.keyman.client.cmd.KeyGeneratorClient
- Generated key, uuid=87639aff-716f-41f3-a304-47594125edfe, algorithm=AES,
strength=128
287 [main] INFO cz.zoom.callrec.keyman.client.cmd.KeyGeneratorClient
- Key generation completed successfully
```

Otherwise check the default error file at `/tmp/installcerts.err`.

9. Switch on call encryption in the Call Recording Web GUI (see [Client Encryption](#)).

10. Restart Key Manager.

```
/opt/callrec/bin/rc.callrec_keymanager restart
Stopping CallREC Key Manager: ..... [ OK ]
Starting CallREC Key Manager: .. [ OK ]
```

More information on keys, certificates and the Java keytool utility: [Java SE keytool reference](#)

Troubleshooting Key Errors

- If call encryption has been enabled in the Call Recording Web GUI, but calls are represented by a warning icon with the message **Decoder error (IO failure)**, check the decoder error log at

```
/opt/callrec/logs/ds.error.log.
```

- If an exception containing text similar to:
cz.zoom.callrec.keyman.KeyVaultException: No key with these parameters can be found, there is an issue with the encryption keys, which is preventing the decoder working. They should be reinstalled as follows:

```
Remove the existing keys and certificates: rm -f  
/opt/callrec/keys
```

1. Stop Call Recording: `service callrec stop.`
2. Run GQM setup again, selecting options to create self-signed certificates if required:
`/opt/callrec/bin/callrec-setup.`
3. Follow the earlier instructions to install commercial certificates if required, and enable call encryption again.
4. If the same key errors occur repeatedly, contact:
<http://genesyslab.com/support/contact>

Configuring Key Manager

After **Key Manager** is activated through the installation of authentication keys and certificates, navigate to **Settings > Configuration > Key Manager > Server Setup**.

Server Setup

The screenshot shows the 'Server Setup' configuration page. On the left, there are tabs for 'Server Setup' (selected) and 'Client Setup'. The main content area is titled 'Server Setup' and is divided into three sections: 'Database', 'Key Management', and 'RMI'.
 - **Database**: 'Database pool' is set to 'callrec' with a dropdown arrow and a note 'Takes effect after reboot'.
 - **Key Management**:
 - 'Password file location': /opt/callrec/keys/pwds.properties
 - 'Keystore location': /opt/callrec/keys/keystore
 - 'Authentication keystore location': /opt/callrec/keys/auth_keystore
 - 'Authentication keystore type': JKS (dropdown)
 - 'Trust keystore location': /opt/callrec/keys/trust_keystore
 - 'Trust keystore type': JKS (dropdown)
 - 'Auto re-encryption enabled':
 - **RMI**: 'Port number' is 30401.
 At the bottom left, there are two buttons: 'Save configuration' and 'Reload configuration'.

Figure 177: Key Manager Configuration – Server Setup

The **Server Setup** section contains the following parameters:

Database

Database pool: the database pool used by **Key Manager**, usually `callrec` for a single server installation.

Key Management

Password file location: the **Key Manager** server's key/certificate password lookup file. Key Manager uses this to manage the key stores in the event of authentication/encryption key expiration & re-creation.

Keystore location: the server key store, containing media encryption keys.

Authentication keystore location: Key Manager's authentication key store, containing the K.M. server's own private authentication key(s).

Trust keystore location: Key Manager's trust key store, containing public authentication keys of trusted clients (for example, encryption & decryption clients).

Auto re-encryption enabled: encrypted files automatically re-encrypted when their certificates expire.

RMI

Port number: RMI port number used by Key Manager, typically 30401.

Client Setup

Navigate to **Settings > Configuration > Key Manager > Client Setup**.

The screenshot displays the 'Client Setup' configuration page for the Key Manager. It features a sidebar with 'Server Setup' and 'Client Setup' tabs. The main area is titled 'Server Setup' and is divided into three sections: 'Key Manager Server', 'Encryption', and 'Decryption'. In the 'Key Manager Server' section, the 'Server' dropdown is set to 'keyManager'. The 'Encryption' section has an 'Enabled' checkbox checked, and several fields for file locations and encryption parameters. The 'Decryption' section has a 'Password file location' field. At the bottom left, there are two buttons: 'Save configuration' and 'Reload configuration'.

Figure 178: Key Manager Configuration – Client Setup

Select the **Enabled** checkbox to enable call and screen capture encryption.

The **Client Setup** section contains the following parameters:

Key Manager Server

Server: the Key Manager server (defined in Call Recording Core settings).

Encryption

Enabled: enable call and screen capture encryption. This only functions after both the authentication keys and encryption keys are configured, as described earlier in this document.

Password file location: The encryption client key/certificate password lookup. The client uses this to manage the key stores, in the event authentication/encryption key expiry and re-creation.

Authentication keystore location: the encryption client authentication key store, containing the client's own private authentication keys.

Trust keystore location: the encryption client trust key store, containing public authentication keys of the trusted servers.

Algorithm: the type of cipher used for encryption and decryption. Genesys uses AES as standard.

Purpose: specify the key set to use for encryption and decryption. The key set's purpose is defined during key creation (audio is default).

Minimum strength: lowest strength cipher to use if the server does not support stronger algorithms.

Maximum strength: the preferred (default) strength, used if server and client both support it. On a single server default installation this should always be used.

Decryption

Password file location: the decryption client key/certificate password lookup. The client uses this to manage the key stores in the event of authentication/encryption key expiration and re-creation.

Authentication keystore location: the decryption client authentication key store, containing the client's own private authentication keys.

Audio Files Are Encrypted

Once **Key Manager** activates, audio encryption enables automatically.

Resolution: none required.

Video Files Are Encrypted

Once **Key Manager** activates, video (Screen Capture) encryption enables automatically.

Resolution: none required.

Web Access Is Encrypted

By default, the Tomcat web server installed and configured for the Call Recording Web GUI and Quality Manager applications, does not have secure-socket layer (SSL) encryption enabled. This is a requirement for PCI Compliance. Instructions are given in the section [Secure Web Access](#).

Resolution: Manual configuration of SSL security in the Tomcat web server.

Audit Logs Are Collected

By default, audit logs are collected in QGM Call Recording. Audit logs are available in the following directory: /opt/callrec/logs. They can also be viewed in the Call Recording Web GUI (see screenshot and the Call Recording Administration Guide). Similarly, the Quality Manager audit log can be viewed and exported in Excel format (see the Quality Manager User Guide CC Manager).

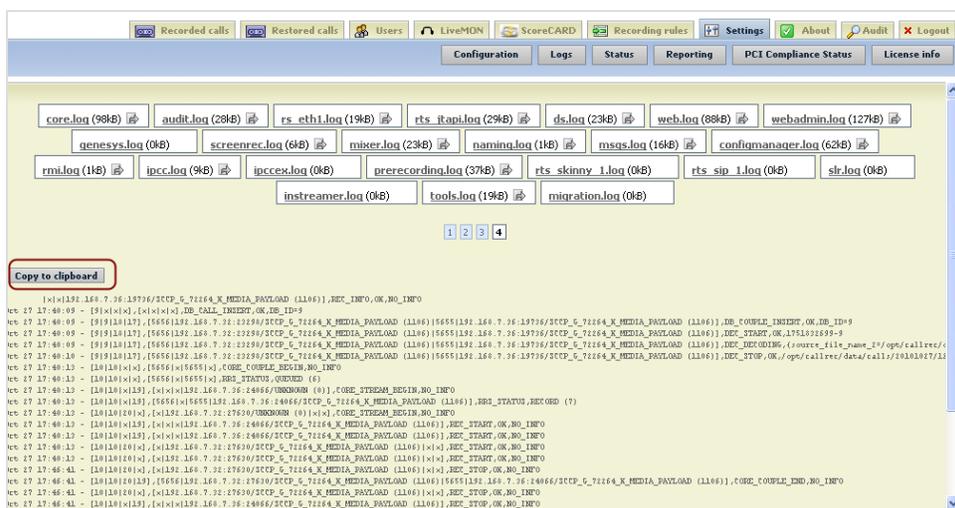


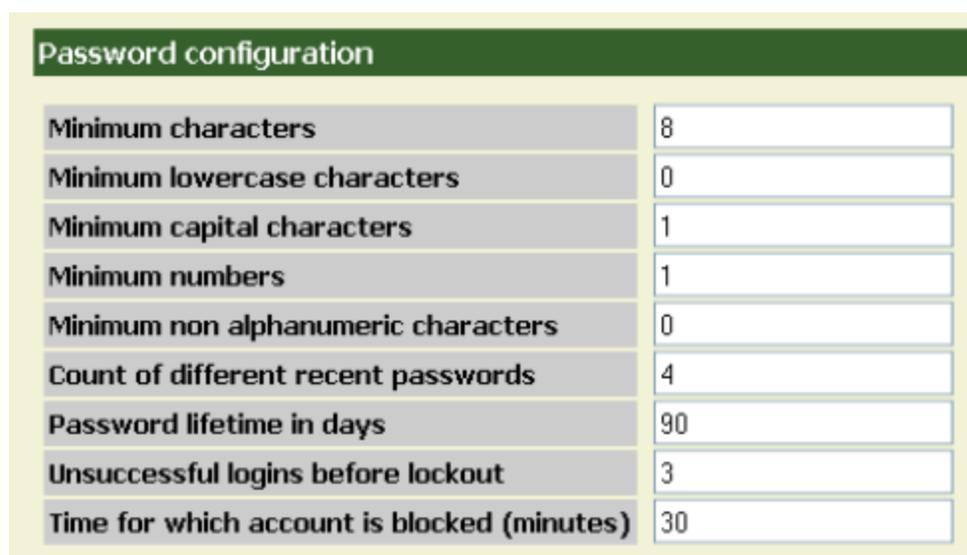
Figure 179: Copying Call Recording Audit Log Data to the Clipboard

Resolution: None required

Password Management Is Enforced

GQM includes advanced password management facilities, that are initially switched off by default, this enables weak passwords to be used. These settings also dictate the settings for Quality Manager. Where integration with external systems is used, the external system dictates password settings for external users.

The following settings are required to be modified from the default values in order for passwords to be marked as PCI Compliant. These are modified in the **Call Recording Web GUI > Settings > Configuration > Web UI > Web Interface > Password configuration** section.



Password configuration	
Minimum characters	8
Minimum lowercase characters	0
Minimum capital characters	1
Minimum numbers	1
Minimum non alphanumeric characters	0
Count of different recent passwords	4
Password lifetime in days	90
Unsuccessful logins before lockout	3
Time for which account is blocked (minutes)	30

Figure 180: Minimum password configuration for PCI Compliance

- **Minimum characters:** at least 8
- **Minimum capital characters:** at least 1
- **Minimum numbers:** at least 1

See the screenshot for more details:

For more information on password configuration settings, see the **User Interface Configuration** section.

Resolution: update the **Password configuration** settings in Call Recording Web UI.

Brute-force protection is enforced

In addition to the minimum password configuration settings above, **PCI Compliance** also requires protection against brute-force attacks, when a hacker makes use of automated password generation techniques to repeatedly attempt entry.

To safeguard against these attacks, the following two settings in the Password configuration section are required to be active (they are PCI Compliant by default):

- **Unsuccessful logins before logout:** 6 or under.
- **Time for which account is blocked (minutes):** 30 or more.

To change these settings, navigate to Call Recording **Web GUI > Settings > Configuration > Web UI > Web Interface > Password configuration**.

Resolution: None required if default settings are kept.

Data Retention Policies Are Enforced

For full **PCI Compliance**, both the **Archive** and **Delete** media lifecycle management (MLM) tools need to be configured and operational. Both of these can be enabled and configured in the **Maintenance** section of Call Recording Settings, **Call Recording Web GUI > Settings > Configuration > Maintenance**.

Sample settings for these tools are shown in the following screenshots. It is critical that settings are configured according to the MLM requirements.

Archive Tool

Media Archive Configuration	
Enabled	<input checked="" type="checkbox"/>
Run as Daemon	<input checked="" type="checkbox"/>
Daemon sleep period (sec.)	1000
Database pool	Maintenance
Subject	Call Recording Archive
Send to email	admin@company.com
Send success emails	<input type="checkbox"/>
Send failure emails	<input checked="" type="checkbox"/>
Temporary directory	/tmp
default	
Enable this task	<input checked="" type="checkbox"/>
Interval period	Last month
Archive filename prefix	archive
Archive max size (MB)	650
Archive not decoded streams	<input type="checkbox"/>
Exclude media type	NOTHING
Exclude RECD	<input type="checkbox"/>
Delete archived files	<input type="checkbox"/>

Figure 181: Maintenance Settings – Archive tool sample settings

Enable the **Archive** tool, including **Daemon sleep period (sec.)** and email settings, **Subject**, **Send to email**, **Send success mails**, or **Send failure emails**, then add an archive task, including the **Interval period**.

Delete Tool

The screenshot displays the 'Maintenance' settings for the 'Delete' tool. The interface includes a sidebar with navigation options: Global Configuration, Archive, Backup, Restore, Synchro, Delete (selected), and Relocation. At the bottom left, there are buttons for 'Save configuration' and 'Reload configuration'.

Media Delete Configuration

- Enabled:
- Run as Daemon:
- Daemon sleep period (sec.): 1212
- Database pool: Maintenance

Delete Calls

- Enabled:
- Interval period: Use custom interval period
- Custom interval period: older than 12 months
- Only if synchronized:
- Only if backed up:
- Delete database link:

Delete Recorded Screens

- Enabled:
- Interval period: Use custom interval period
- Custom interval period: older than 6 months
- Only if synchronized:
- Only if backed up:
- Delete database link:

Figure 182: Maintenance Settings – Delete Tool Sample Settings

Enable the **Delete** tool including **Daemon sleep period (sec.)**, set to a different value than for the **Archive** tool in this example, then add a delete task, and enable the type of media to delete and **Interval period** for each.

Resolution: Enable and configure the **Archive** and **Delete** MLM tools in Call Recording Maintenance settings.

Encrypt Tool

The encrypt tool, found at `/opt/callrec/bin/encrypt` on a default Call Recording server installation, is used to encrypt un-encrypted media files, or re-encrypt compromised media files (the encryption keys are no longer valid or safe).

There is an optional parameter `-r` that enables re-encryption of encrypted files. If run without this parameter, the tool only encrypts non-encrypted files.

Parameters

`-config pci_compliance`: mandatory parameter, that points to PCI compliance related parameters in the Configuration Service.

`-r`: optional re-encryption mode parameter. If specified, only encrypted (compromised) files are re-encrypted, otherwise only non-encrypted files are encrypted.

`-date`: optional parameter, that specifies a time window filter ('from' date and 'to' date) for files to encrypt. Date format: `hh/dd/mm/yyyy`. For example, `-date 23/04/05/2011 00/05/05/2011` would process all files created between 11pm of May 4th 2011 and midnight of May 5th 2011.

If no date is provided, the tool displays a message similar to the following:

```
WARNING! No time range has been specified. Processing
may take a while and can cause a significant load on the
server.
```

`-logger`: optional parameter, that is provided with the path to a log4j properties file, for a customized debug log. More information about setting up log4j property files is given in the [Switching On Debug Logs](#) section of this Appendix.

Examples:**1. Encrypt all non-encrypted files:**

```
/opt/callrec/bin/encrypt -config pci_compliance -logger  
</path/to/log4j/properties/file>
```

2. Encrypt all non-encrypted files within given 1-hour time window:

```
/opt/callrec/bin/encrypt -config pci_compliance -date 20/04/05/2011  
00/04/05/2011 -logger </path/to/log4j/properties/file>
```

3. Re-encrypt all encrypted files:

```
/opt/callrec/bin/encrypt -config pci_compliance -r -logger  
</path/to/log4j/properties/file>
```

4. Re-encrypt all encrypted files with compromised key in given time window:

```
/opt/callrec/bin/encrypt -config pci_compliance -r -date date1 date2 -logger  
</path/to/log4j/properties/file>
```

Switching On Debug Logs

If the default debug output of a Call Recording tool or script is not enough to pinpoint the cause of the error, switch on more granular error reporting. This process is similar for virtually any other component in the Genesys Quality Management product, since all use the same 'log4j' logging API.

1. Create a log configuration file with the following content using vi or other text editor and save it as:

`/opt/callrec/etc/mydebuglog.log4j.properties`, modify the `/var/log/callrec/mydebuglog.log` output log location as required:

```
log4j.rootLogger=TRACE, file
# file
log4j.appender.file=org.apache.log4j.RollingFileAppender
log4j.appender.file.MaxFileSize=2500MB
log4j.appender.file.MaxBackupIndex=0
log4j.appender.file.File=/var/log/callrec/mydebuglog.log
log4j.appender.file.layout=org.apache.log4j.PatternLayout
log4j.appender.file.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %-5p [%t]
%c - %m\n
```

2. Run the tool or script, using the `logger` parameter to specify the location of the configuration file created.

For example, the following is how the `encrypt` tool is given the `logger` parameter:

```
/opt/callrec/bin/encrypt -logger
/opt/callrec/etc/mydebuglog.log4j.properties
```

3. View the output log at the location specified and search for errors and exceptions in the detailed output:

```
less /var/log/callrec/mydebuglog.log
```

Password Storage in GQM

To meet PCI DSS requirements for password storage, from GQM version 8.0.47x onwards, passwords are stored in the Call Recording database as follows:

- A unique password salt is created for each user and stored in the database.
- The user's password is hashed with the salt using approx. 1000 passes of the SHA-1 encryption algorithm.

This procedure provides protection against brute force and rainbow table attacks. See the references below for more information.

References:

- Wikipedia entry for cryptographic salts: [http://en.wikipedia.org/wiki/Salt_\(cryptography\)](http://en.wikipedia.org/wiki/Salt_(cryptography))
- Wikipedia entry for the SHA-1 cryptographic hash function: <http://en.wikipedia.org/wiki/Sha-1>
- Wikipedia entry for Brute Force attacks: http://en.wikipedia.org/wiki/Brute-force_attack
- Wikipedia entry for Rainbow Tables: http://en.wikipedia.org/wiki/Rainbow_table

22 **Secure Web Access for PCI-DSS Compliance**

Genesys GQM installs a web server (Apache Tomcat 6.x) to run web-based applications such as Call Recording Web GUI and Quality Manager. By default, Tomcat is not configured to provide secure (HTTPS) access via a Secure Socket Layer (SSL) implementation, but this is required for PCI-DSS compliance.

This chapter contains the following sections:

[Component Compatibility](#)

[Configuration](#)

[Creating the Key and Certificate](#)

[Converting the Certificate](#)

[Configuring Tomcat](#)

[Restarting the Call Recording Web Service](#)

[Adding the Localhost Certificate to the Java CA Certificates](#)

[Adding the Port Redirect to the IP Tables](#)

[Configuring the Quality Manager Stream URL Setting](#)

[Secure LDAP](#)

[GQM Port Usage Guide](#)

Component Compatibility

Some GQM components require HTTP connectivity alongside secure HTTPS. Review the following before deciding whether to deploy only HTTPS, or both HTTPS and HTTP protocols in parallel.

- **CUCM-based Prerecording:** Requires HTTP as well as HTTPS due to a CUCM limitation.
- **Live Monitor:** Works with HTTPS with no additional configuration (HTTP not required).
- **Screen Capture:** Currently requires HTTP as well as HTTPS. Although the Screen Capture Client communicates via TLS to the Screen Capture Server (SRS), HTTP is required for communication from the Client to the Screen Capture Media Upload Server.

Configuration

Use a commercial CA Certificate Authority, such as Thawte or Verisign, to sign the SSL certificates. Using a commercial CA avoids browser warnings regarding 'untrustworthy' self-signed certificates.

The following steps cover the procedure to configure secure web access using both commercially signed and self-signed SSL certificates. Tomcat 6.0 contains the Tomcat Native APR library, recommended for production use. However, use of this library prevents the use of the `java keytool` utility for key and certificate generation; the OpenSSL utility must be used instead as covered here.

Creating the Key and Certificate

To generate an RSA private key, use an SSH Client. Log in as `admin`. Enter `su` - to log in as the root user. Enter the password, the default is `zoomcallrec`. Enter the following command:

```
$ openssl genrsa 1024 > localhost.key  
$ chmod 400 localhost.key
```

Obtain a commercially signed certificate or create a self-signed certificate.

Obtaining a Commercially Signed Certificate

To obtain a commercially signed certificate:

1. Create the certificate signing request file (`cert.csr` in PEM format); answer all questions, including the required challenge password for identification:

```
$ openssl req -new -nodes -sha1 -key localhost.key > cert.csr
```

2. Send the certificate signing request file `cert.csr` to the CA.
3. After receiving the signed certificate, save it as `localhost.crt` on the server in the same location as the private key.
4. Copy the key and certificate into place and change the file ownership using the following command:

```
$ cp localhost.key /opt/callrec/web/conf
$ cp localhost.crt /opt/callrec/web/conf
$ chown callrec.callrec /opt/callrec/web/conf/localhost.*
```

Creating a Self-signed Certificate

To create a self-signed certificate, answer all the questions for the certificate data as below.

Important:

The Common Name certificate parameter must contain the FQDN name of the server, for example, `callrec.mycompany.com`.

```
openssl req -new -x509 -nodes -sha1 -days 365 -key localhost.key >
localhost.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:California
Locality Name (eg, city) [Newbury]:San Francisco
Organization Name (eg, company) [My Company Ltd]:MyCompany, Inc.
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname)
[:callrec.mycompany.com
Email Address []:it-callrec@mycompany.com
```

Converting the Certificate

The signed certificate can be converted from an alternative format to PEM format (.crt, .cer filetypes) using openssl, for example, the following converts a DER encoded certificate file (cert.cer) into PEM format (localhost.crt):

```
openssl x509 -inform der -in cert.cer -out localhost.crt
```

For further information and conversion examples, see the OpenSSL documentation: <http://www.openssl.org/docs/apps/x509.html> and SSL Shopper site: <https://www.sslshopper.com/ssl-converter.html>.

Configuring Tomcat

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

1. Edit the config file at `/opt/callrec/web/conf/server.xml` to include the following `<Connector>` port node definition (paste within the `<Service name="Catalina">` node service definition):

```
<Connector port="8443" maxHttpHeaderSize="8192" maxThreads="150"
  enableLookups="false" disableUploadTimeout="true"
  acceptCount="100" scheme="https" secure="true"
  SSLEnabled="true"
  SSLCertificateFile="${catalina.base}/conf/localhost.crt"
  SSLCertificateKeyFile="${catalina.base}/conf/localhost.key" />
```

Important:

To specify the version of the SSL protocol used, add the following option into the Connector port configuration (see <http://tomcat.apache.org/tomcat-6.0-doc/apr.html#HTTPS> for details):

```
SSLProtocol="SSLv3"
```

To disable unsecured HTTP access, comment out the http connector pointing to port 8080 in the file `/opt/callrec/web/conf/server.xml`:

```
<!--
<Connector port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="8443" />
-->
```

Restarting the Call Recording Web Service

1. After completing configuration, restart the Call Recording web service:

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

2. Observe the web server log at `/var/log/callrec/web.log` for any errors.
3. If the web server restarts successfully, and no serious errors are apparent in the server log:
If the web server is not accessible, try to access using the original non-secure http URL; if necessary re-enabling non-secure access if it was disabled earlier. Troubleshoot the `/var/log/callrec/web.log` log file for further indication of any issues.

Adding the Localhost Certificate to the Java CA Certificates

Use the Java `keytool` utility to add the new `localhost.crt` certificate to the collection of trusted Certification Authorities (CA). Change the `-alias` parameter value (`callrecssl`) if required:

```
keytool -keystore /usr/java/jdk1.6.0_35/jre/lib/security/cacerts -alias  
callrecssl -importcert -file  
/opt/callrec/web/conf/localhost.crt
```

Enter the default keystore password `changeit`.

Ensure the displayed certificate information is correct and type `y` to trust the certificate.

For more information on the `keytool` utility, including how to change the keystore password, see:

<http://download.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html>.

Adding the Port Redirect to the IP Tables

At this point, SSL access is functional, but a port (:8443) is always required in the Call Recording server URL. Adding an SSL port redirect rule to the Linux IP Tables configuration via the following procedure removes this requirement:

1. Add redirect rule to existing IP Tables, replace 10.9.8.7 with the Call Recording server IP address:

```
iptables -t nat -A PREROUTING -d 10.9.8.7 -p tcp --dport 443 -j REDIRECT --to-ports 8443
```

2. List (and note) updated IP Tables:

```
iptables -t nat -L -v -n
```

3. Save updated IP Tables records:

```
/etc/init.d/iptables save
```

4. Restart IP Tables:

```
/etc/init.d/iptables restart
```

5. Check and compare updated IP Tables:

```
iptables -t nat -L -v -n
```

6. Restart the web server, and clean out the server cache:

```
/opt/callrec/bin/rc.callrec_web stop  
rm -rf /opt/callrec/web/work/Catalina/localhost/*  
/opt/callrec/bin/rc.callrec_web start
```

7. The Call Recording web server should now be accessible at the URL:
`https://<SERVER_IP>` without a port being specified; for example,
`https://10.9.8.7`

Configuring the Quality Manager Stream URL Setting

When secure access to the Call Recording Web GUI is finalized, the **Quality Manager URL to Call Recording stream** parameter must be updated in the **Settings > Configuration > Quality Manager > Basic Setup** section to enable Quality Manager to correctly play media over the secure connection.

The Call Recording stream parameter is the same URL used to access the Call Recording Web GUI over https, for example:

```
https://<FQDN>/callrec
```

At this point, SSL access should be working for all GQM Tomcat-based web applications.

More information on setting up SSL in Apache Tomcat:

<http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html#Troubleshooting>.

Secure LDAP

The LDAPS (secure LDAP) protocol is the LDAP protocol running over an SSL connection. The application establishes an SSL connection with the LDAP server first, and then starts the LDAP bind/login attempt. This prevents attacks by sniffing for a password sent in plain text and "man in the middle" attacks by ensuring that the LDAP server is trusted.

Genesys GQM supports LDAPS, but this needs to be configured manually, principally by the installation of appropriate SSL certificates. In this way, secure directory access contributes to fulfilling [PCI-DSS directive #6](#).

If possible, it is helpful to configure and test a standard LDAP connection first before switching on LDAPS. Refer to the LDAP Configuration section in the Call Recording Administration Guide for more information.

The following steps are required in order to set up secure LDAP within Call Recording.

Install SSL Certificates

The java keytool supports X.509 certificates, so a commercial SSL certificate in this format is required. See the section on [Secure Web Access](#) for more information about certificates and format conversion.

To import the certificate using the keytool utility:

1. Upload the certificate file to the Call Recording server using scp, WinSCP or similar.
2. Run the command below, ensure it is entered on one line, and replace the following placeholders with their correct values:
 - [path_to_certificate]: the full path to the certificate file uploaded to the server.
 - [store_pass]: the keystore password; the default is: changeit.
 - [certificate_alias]: a reference name for the certificate.

```
/usr/java/default/bin/keytool -importcert -file [path_to_certificate] -
keystore
/usr/java/default/jre/lib/security/cacerts -storepass [store_pass] -alias
[certificate_alias]
```

If there is a problem with the certificate, for example if it is not trusted, view the errors in the Call Recording UI log file, similar to the following sample:

```
javax.naming.CommunicationException: simple bind failed: ldap.server.com:636
[Root exception is javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException:
PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to
find valid certification path to requested target]
```

Refer to the Logs section in the Call Recording Administration Guide for more information about viewing logs.

Enable LDAPS in the Call Recording Web GUI

Log in to the Call Recording Web GUI as an administrator, and navigate to **Settings > Configuration > Web UI > LDAP**.

Figure 183: Enabling LDAPS in the CallREC Web GUI

1. Select the **Use LDAPS protocol** checkbox to enable LDAPS.
2. Ensure that the correct SSL IP port is entered into the **Port** field. The default LDAPS port is 636.
 - Ensure the values for the remaining fields are correct. Refer to the LDAP Configuration section in the Call Recording Administration Guide for more information.
 - Save the modifications, then restart the web server :

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

- If the configuration is correct, import Call Recording users from the LDAP directory. Refer to the Adding Users from LDAP section in the Call Recording User Guide.

GQM Port Usage Guide

The single server installation uses the following ports:

Port Number	TCP	UDP	Use
22	✓		SSH – distant access
80	✓		GUI – http (internally redirected to port 8080)
111	✓	✓	NFS (for replay synchro)
389	✓		LDAP
443	✓		GUI – https (internally redirected to port 8443)
2049	✓	✓	NFS (for replay synchro)
4001 – 4004	✓	✓	NFS (for replay synchro)
5060	✓	✓	SLR default SIP port
5432	✓		PostgreSQL (for replay synchro)
7003	✓		Screen Capture Server (also TLS)
8080	✓		GUI – http (see port 80)
8443	✓		GUI – https (see port 443)
16384 - 17183.		✓	RTP streams to SLR
30100	✓		Skinny sniffer
30200	✓		SIP sniffer
30300	✓		JTAPI sniffer
30350	✓		MSR SLR sniffer

Port Number	TCP	UDP	Use
30400	✓		Default RMI port
30401	✓		Key Manager
30500	✓		Configuration service (allow it for Live Monitor)
30501	✓		Configuration service (allow it for Live Monitor)
30600	✓		Core (allow it for Live Monitor)
30601	✓		Core (allow it for Live Monitor)
37000 - 37100		✓	Datagrams ports (allow it for Live Monitor)

Table 13: Single Server Port Usage Guide

Genesys default ports for MSR/EPR/GIM

Port Number	TCP	UDP	Use
2020	✓		Genesys Configuration Service
3000	✓		T-Server communication

Table 14: Genesys Default Ports for MSR/EPR/GIM

RMI communications between modules uses random ports from range: 1024 – 65535 (TCP).

Important:

Do not change **Port** settings directly in configurations files without consulting Genesys Support. Change these settings through the Admin User Interface. Ensure that there is a backup of all configuration files before changing port numbers.

Chapter

23 **Activating Quality Manager**

This section gives a step-by-step guide to the licensing and activation of Quality Manager.

This chapter contains the following sections:

[Activating Quality Manager](#)

[Log Out, Refresh Page, Log In as CC Manager](#)

[Logged In as ccmanager](#)

[Default Quality Manager Users](#)

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

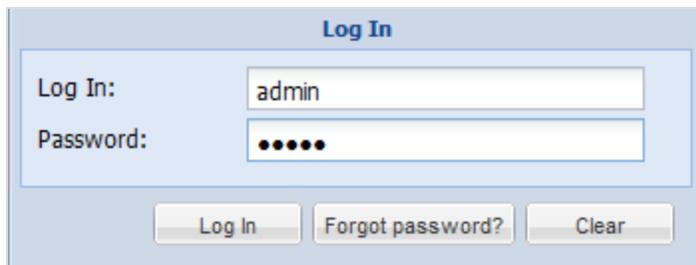


Figure 184: Log in as Administrator

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.

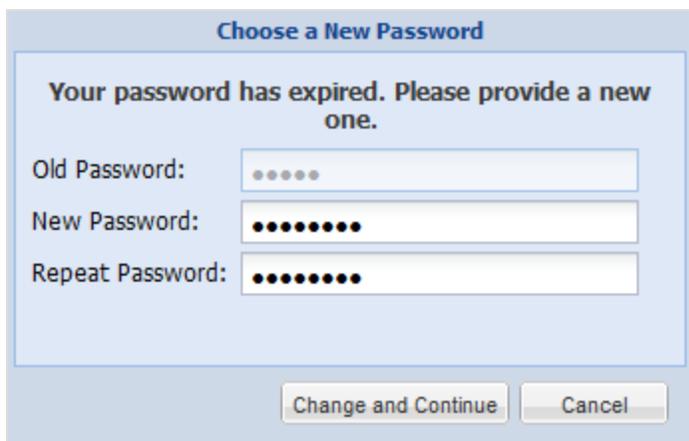


Figure 185: Choosing a New Password

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.

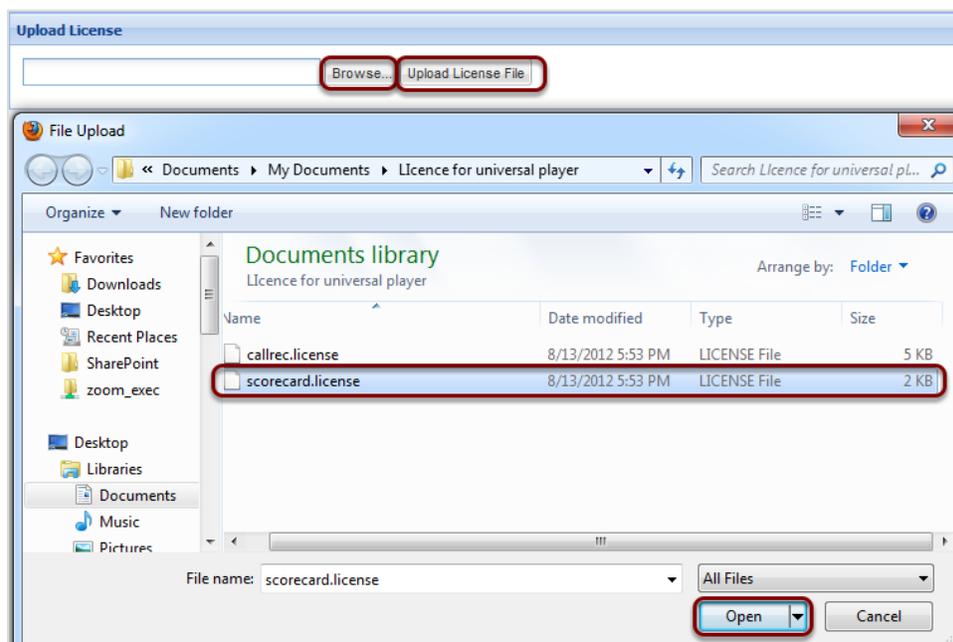


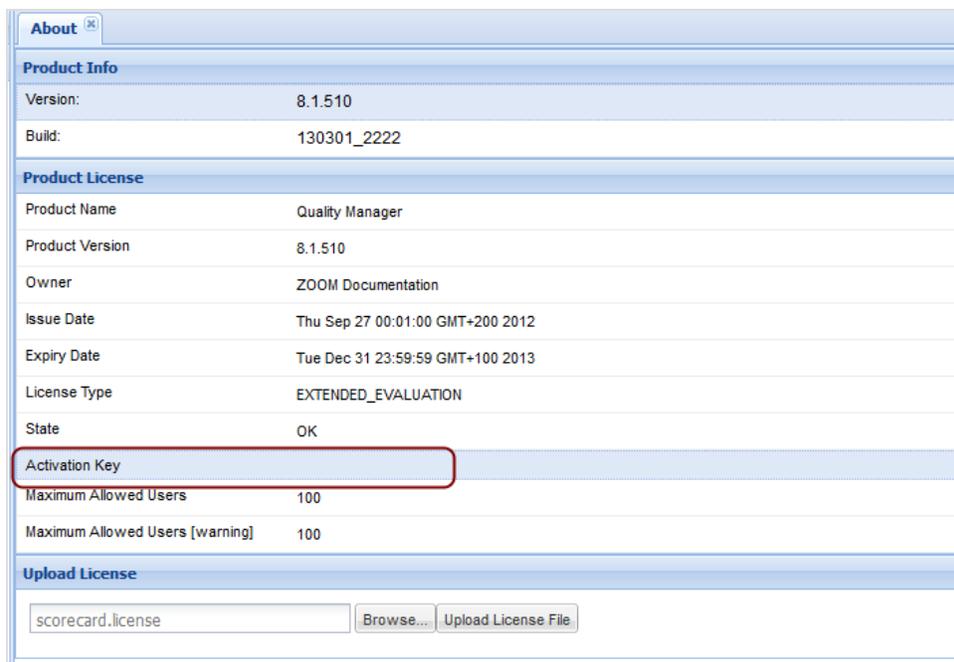
Figure 186: Browse to the License File

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



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	
<input type="text" value="scorecard.license"/>	<input type="button" value="Browse..."/> <input type="button" value="Upload License File"/>

Figure 187: 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

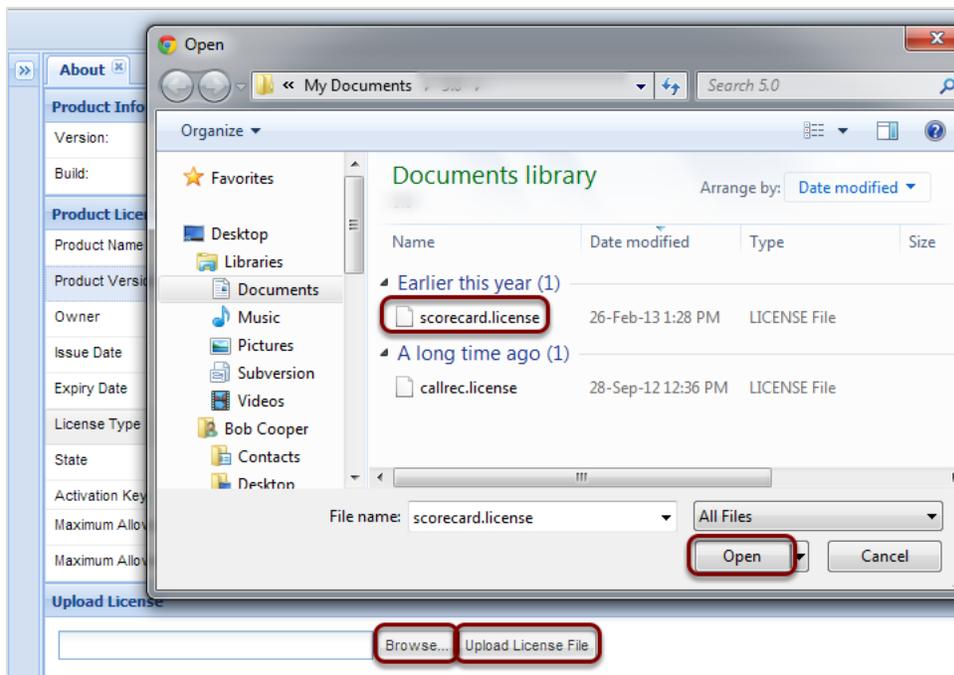


Figure 188: Browse to the License File

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
```

Log Out, Refresh Page, Log In as CC Manager

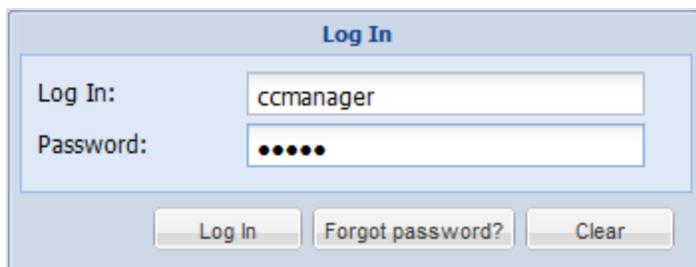
A dialog box titled "Log In" with a light blue background. It contains two input fields: "Log In:" with the text "ccmanager" and "Password:" with five black dots. Below the fields are three buttons: "Log In", "Forgot password?", and "Clear".

Figure 189: Log Out, Refresh the Page and Log In as CC Manager

Log in as call center manager (ccmanager) in order to set up Quality Manager. Log out of the application and refresh the page (click F5 or equivalent in the browser).

Log in as ccmanger with the default password admin.

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

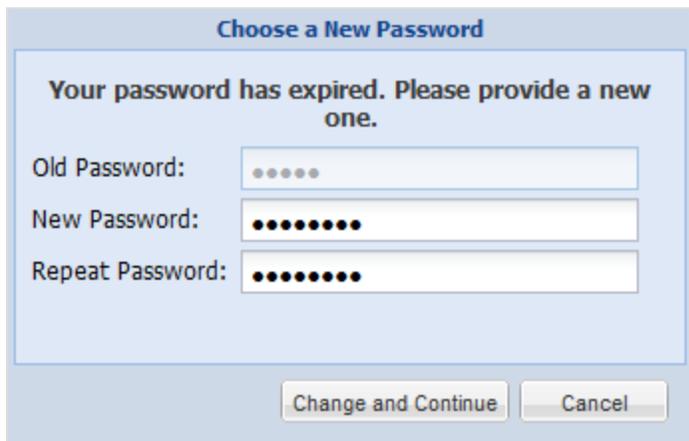
A dialog box titled "Choose a New Password" with a light blue background. It contains a message: "Your password has expired. Please provide a new one." Below the message are three input fields: "Old Password:" with five black dots, "New Password:" with eight black dots, and "Repeat Password:" with eight black dots. At the bottom are two buttons: "Change and Continue" and "Cancel".

Figure 190: Choosing a New Password

New passwords must have:

- at least 8 characters
- with at least one character a number (0-9)
- at least one character a lowercase letter (a-z)
- one character an upper case letter (A-Z)

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".

Logged In as ccmanager

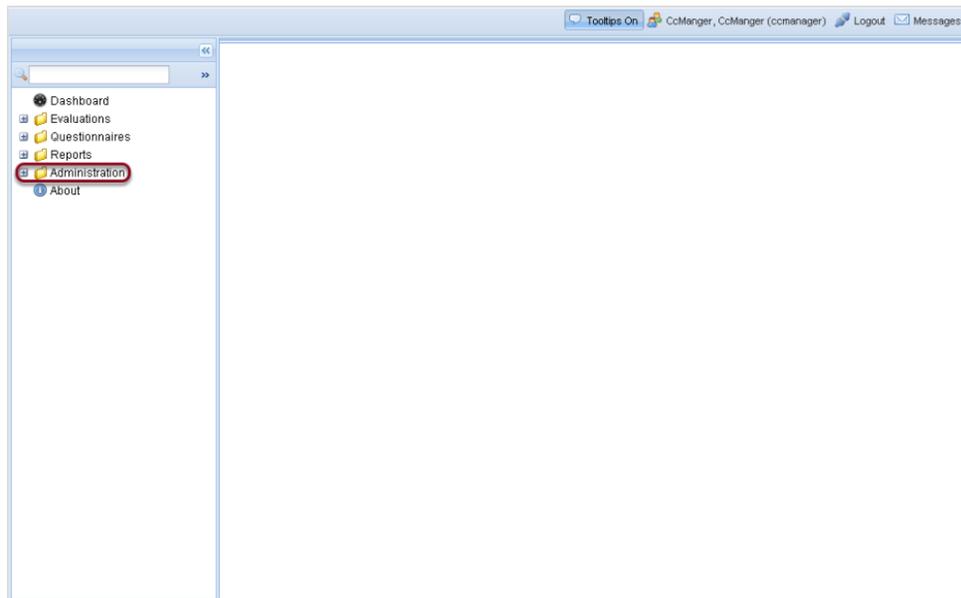
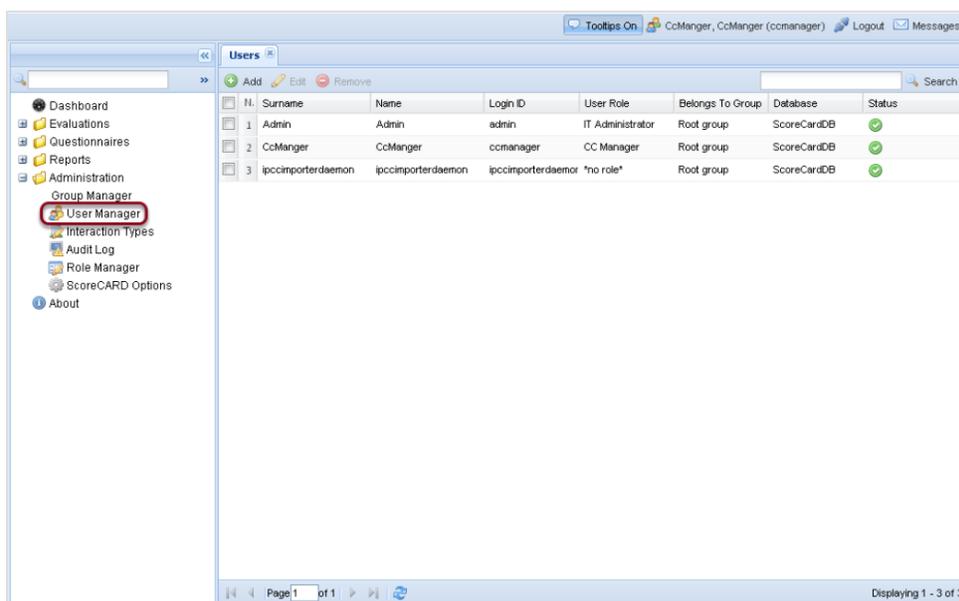


Figure 191: Logged in as CC Manager

Once logged in as `ccmanager`, users and groups can be configured (see the Quality Manager User Guide for more information).

Default Quality Manager Users



The screenshot shows the 'Users' management interface. On the left is a navigation menu with 'User Manager' highlighted. The main area displays a table of users with the following data:

N.	Surname	Name	Login ID	User Role	Belongs To Group	Database	Status
1	Admin	Admin	admin	IT Administrator	Root group	ScoreCardDB	✓
2	CcManger	CcManger	ccmanager	CC Manager	Root group	ScoreCardDB	✓
3	ipccimporterdaemon	ipccimporterdaemon	ipccimporterdaemor	*no role*	Root group	ScoreCardDB	✓

Figure 192: Default Quality Manager Users

Click **Administration > User Manager** to display the default users that Quality Manager installs.

The Quality Manager user 'ipccimporterdaemon' is added in to the database schema during the initial installation.

It is used only for synchronization with or Genesys CIM (if used), and has no other use.

If required, an administrator can create a different user with synchronization privileges, and delete this default one. In this case the `wbscimporter` script must be provided with proper user access (permission) credentials.

Important:

Note that importing users from or Genesys CIM must be performed with an empty Quality Manager database (i.e. after Quality Manager installation but before adding any other users within Quality Manager).

Chapter

24 **Configuring Quality Manager**

The Quality Manager tab is only visible if the Quality Manager service is selected during setup and the correct license is installed. The Quality Manager module contains the configuration settings for the server components of the Quality Manager.

This chapter contains the following sections:

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

[Scheduled Actions](#)

[Quality Manager Integrations](#)

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 193: 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:

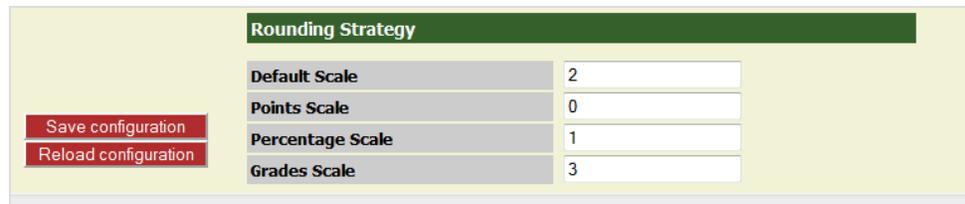
```
/opt/callrec/web/webapps/scorecard-webui/cz.zoom.scorecard.webui.Scorecard/
```

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 194: Rounding Strategy

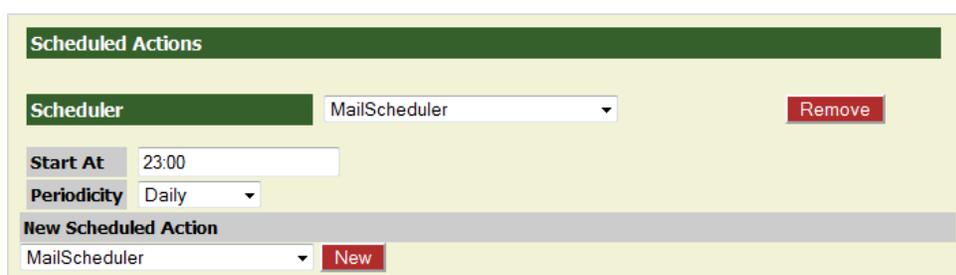
It is possible to set separate settings for:

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

Scheduled Actions

Scheduled Actions refers to regularly repeated actions, typically for user synchronization when using an integration module, or mail delivery.

To create a new mailer scheduled action for scheduling email delivery from ScoreCARD, navigate to **Settings > Configuration > Quality Manager Setup**.



The screenshot displays the 'Scheduled Actions' configuration page. At the top, there is a green header bar with the text 'Scheduled Actions'. Below this, there is a section for the current scheduler, labeled 'Scheduler', with a dropdown menu showing 'MailScheduler' and a red 'Remove' button. Underneath, there are two input fields: 'Start At' with the value '23:00' and 'Periodicity' with a dropdown menu showing 'Daily'. A grey bar separates this from the 'New Scheduled Action' section, which contains a dropdown menu with 'MailScheduler' selected and a red 'New' button.

Figure 195: Quality Manager Configuration - Mailer Scheduled Actions

1. Select **MailScheduler** in the **New Scheduled Action** field.
2. Select values for the following settings:
 - **Start At**: start the mail delivery daemon at this time (hh:mm using 24 hour clock; for example: 23:00).
 - **Periodicity**: run the mail daemon at these intervals: **Every hour** (the **Start At** value is not used), **Daily**, **Weekly**.

Scheduled Actions for integration module functionality are described in the appropriate integration configuration section of this guide:

- [Genesys integration scheduled actions](#)

Quality Manager Integrations

Quality Manager Integrations is the main section where Quality Manager-specific settings are configured for integration modules (Genesys).

More information can be found in the appropriate integration configuration section of this guide:

- [Genesys integration configuration](#)

25 Synchronizing Quality Manager with a Genesys Configuration Server

The Quality Manager Genesys Importer can import and synchronize user and group information from a Genesys Configuration Server. The synchronization is only one-way (from the Genesys Configuration Server to Quality Manager), and you can configure whether local changes made to Genesys users and groups in Quality Manager are retained or overwritten during a synchronization operation.

Genesys users imported into Quality Manager can be authenticated directly against Genesys Configuration Server or a third party authentication service such as Microsoft Active Directory. In this scenario, no local user passwords are stored within Quality Manager.

This chapter contains the following sections:

[Genesys Importer Features](#)

[Quality Manager Genesys Configuration](#)

[User Synchronization Option](#)

[Scheduling Genesys Synchronization](#)

[Integration Data Definition](#)

Genesys Importer Features

The following actions can be performed by the Genesys synchronization tool to data in Quality Manager based on updated data from Genesys Configuration Manager:

- add or remove agents
- add or remove team lists
- add or remove agent to and from team lists
- move agents between team lists
- make an agent a supervisor and vice-versa
- delete non-empty team list
- supervisor logs in as a normal user

The Genesys Importer for Quality Manager enables Genesys user data to be mapped to the Quality Manager user data structures in an entirely configurable manner, even if Virtual Agent Groups (VAGs) are used in the Configuration Server. Further, by using the Annex configuration feature in Genesys Configuration Manager, imported user groups may be structured as a multi-tier group hierarchy within Quality Manager.

Important:

The Importer is run at regular intervals, defined by the settings in the **Scheduler** section of Quality Manager Genesys Configuration. This overwrites any local role settings for users that are configured in Quality Manager.

Preparation for Importing

Genesys Configuration Manager does not currently support agent group hierarchy. It is possible to create many subordinate folders and put various agent groups into them, but it is not possible to place an agent group below another agent group.

To be able to import the agents and supervisors successfully and enable supervisors to evaluate their staff, first create a group for the supervisors in Configuration Manager. Then create groups for the agents in Configuration Manager and link each group to particular supervisors.

1. Create a Virtual Agent Group (VAG) for the supervisors to be imported for example with the name `GQM_Supervisors` in Configuration Manager.
2. Add the usernames of the supervisors to be imported to the VAG `GQM_Supervisors`.
3. Create an annex to the VAG `GQM_Supervisors` with an annex name = `import` and a value = 2.

Default key name:	<code>import</code>
Possible values:	0,1,2
Description:	0 = Do not import group and agents 1 = Import group only (no agents) 2 = Import group and agents

Table 15: Annex Import Parameter

4. Create a VAG for each group of agents to be imported each with a unique group name in Configuration Manager, for example `GQM_Team_A` for the first group, `GQM_Team_B` for the second group, `GQM_Team_C` for the third group, `GQM_Team_D` for the fourth group, and so on. Each VAG must have a different **SkillNumber** defined in Configuration Manager.
5. Add the usernames of the agents for each group to their appropriate VAG.
6. Create an annex to each agent VAG with an annex parameter = `import` and a value = 2.

To specify a multi-tier hierarchy when importing into Quality Manager, each agent group can have a link to a parent group defined in its Annex property. In this case, the Importer creates a multi-tier hierarchy of groups.

7. Create an annex to each agent VAG with an annex parameter = `Supervisor` and value = `x`, where `x` is one or more user names of the supervisor (evaluator) for that group contained in the VAG `GQM_Supervisors`. If there is more than one supervisor that can evaluate the group, the extra values can be entered, separated by commas. This sets which supervisors are able to evaluate this group.

The following figure shows the `supervisor` parameter added to an agent group's **Annex** property in Genesys Configuration Manager.

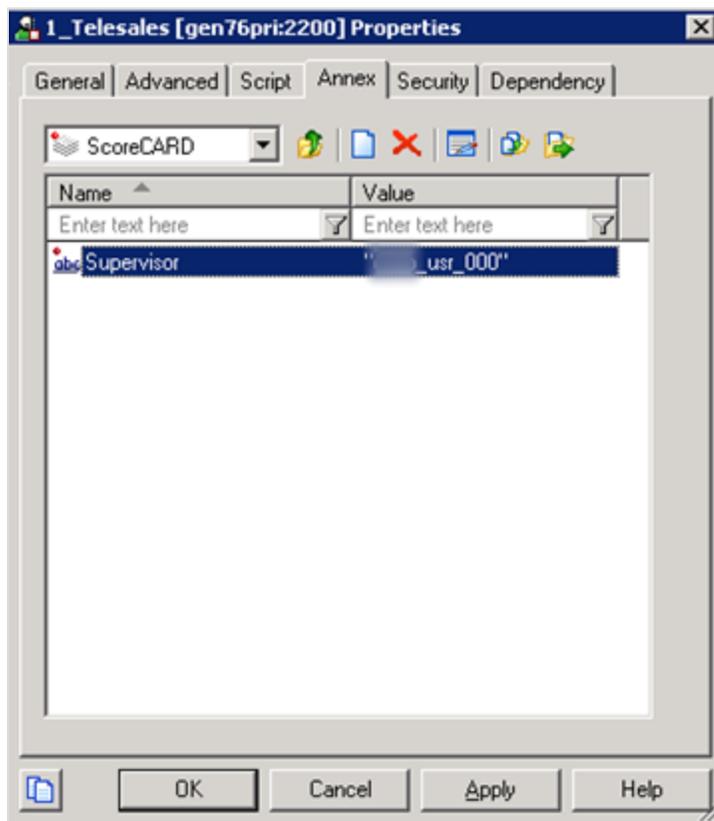


Figure 196: Genesys Annex Supervisor Parameter - Single Value

8. Create an annex to the Virtual Agent Group agents with an annex name = `parent-group` and a value = `GQM_Supervisors`.

To specify a parent group for an agent or agent group, add the following parameter to its **Annex** tab in the properties dialog, Quality Manager section:

Default key name:	parent-group
Possible values:	[string]
Description:	string refers to the name of the super-ordinate group or folder

Table 16: Annex Parent-Group Parameter

9. Ensure that Quality Manager includes the supervisor role in the Role Manager in the **Administration** section of Quality Manager. If the supervisor role is deleted or missing, the **Supervisor role equivalent** option in Quality Manager Options must be set to a different existing role name, not supervisor, otherwise the Importer fails.

Importing Agent Groups and Related Users

During an import operation, the Genesys Importer crawls the agent group structure created in the Configuration Server and, based on filtering values, imports and then re-constructs the group structure within Quality Manager. Only users that are members of selected groups are imported. Selected groups may further be filtered at group or user level using the Annex value.

By default, all groups under the top **agent groups** folder in Configuration Manager are imported. If a **Root Folder** is specified in the **Advanced Options** section of [Quality Manager Genesys Configuration](#), all users and groups under this folder are imported instead.

During an import synchronization, if an imported agent is disabled or removed from the Customer Interaction Management Platform (or CIM), the Importer sets the user's status in Quality Manager to **de-activated**. Agent records are not deleted from Quality Manager automatically, since evaluations may be associated with that agent.

Important:

Agents marked as disabled in Configuration Manager are imported but marked as inactive by the Importer and are not visible in Quality Manager. However, agent groups marked as disabled in Configuration Manager are imported but not marked inactive by the importer. Therefore, disabled agent groups are currently visible in Quality Manager.

Importing Virtual Agent Groups

Virtual Agent Groups (VAGs) contain agents with a specific skill, as defined in the script section of the respective VAG. The Importer treats VAGs in the same way as regular agent groups or folders and filtering can also be applied to them.

Advanced Filtering by Annex Value

By adding further parameters in the **Annex** tab of an agent or agent group's properties in Configuration Manager, advanced filtering and user import management can be specified.

For each of the following parameters, it is assumed that an Annex section named (by default) Quality Manager has been defined in the agent or group's properties dialog. Each parameter is added as a key/value pair in that section.

The section name and key names can be changed in the **Annex Options** section of [Quality Manager Genesys Configuration](#), but it is recommended to leave them unchanged.

Filtering imported groups by specific Annex value

Filtering imported agent groups can be necessary for the following reasons:

- The user may not want to import certain agents or agent groups within the target agent group structure.
- The structure of VAGs may contain duplicate records, so not all members of certain agent groups should be imported.

To add a filter for an agent or agent group, add the following parameter to its **Annex** tab in the properties dialog, Quality Manager section:

Default key name:	import
Possible values:	0,1,2
Description:	0 = Do not import group and agents 1 = Import group only (no agents) 2 = Import group and agents

Table 17: Annex import parameter

The default behavior of the Importer is to import all agent groups and their member agents, unless both, Annex processing is enabled and these keys are present.

Specify Agent Group Supervisors by specific Annex value

Although the supervisor or manager for an agent group can be specified in the **Supervisor** field (in the **Advanced** tab of the agent group properties dialog), this is often not flexible enough for organizations using Genesys CIM; for example, more than one manager for a group cannot be specified this way.

In order to accommodate other different methods of specifying supervisors (such as via specific skills), the Genesys Importer can be explicitly given the usernames of supervisors for a particular agent group.

To specify one or more supervisors or managers for an agent group, add the following parameter to its **Annex** tab in the properties dialog, Quality Manager section:

Default key name:	<code>supervisor</code>
Possible values:	<code>[string], [string], ...</code>
Description:	<code>string</code> refers to the username of a user who is assigned a manager role for this agent group in Quality Manager. Further usernames can be added, separated by commas.

Table 18: Annex supervisor parameter

The following figure shows multiple supervisors added to an agent group for import.

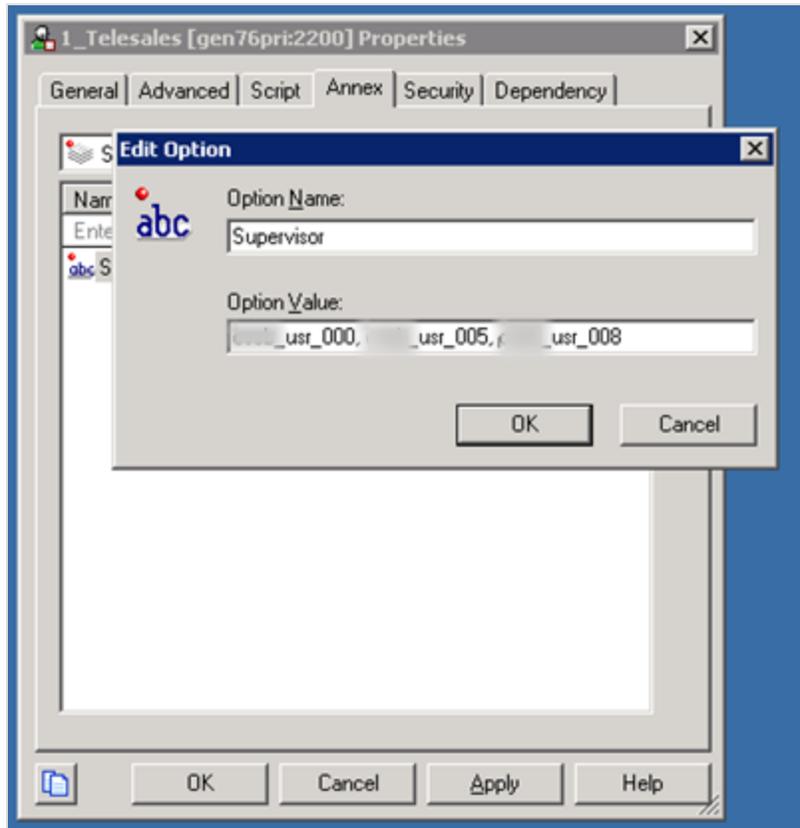


Figure 197: Genesys Annex supervisor parameter - multiple values

Authentication against Genesys Configuration Manager

Imported users are authenticated against the Genesys Configuration Manager. If a specified user is not (or no longer) present in Configuration Manager, access is declined and the event noted in the Quality Manager event log.

If the Configuration Server uses a secure (TLS) connection, ensure that the **Use Secure Connection** parameter is checked in the Genesys Configuration Server section of [Quality Manager Genesys Configuration](#).

Quality Manager Genesys Configuration

The Genesys integration configuration for Quality Manager can be viewed and modified in the Call Recording Web UI by navigating to **Settings > Configuration > Quality Manager > Integrations** section.

When Genesys GIM or Genesys Driver is selected during GQM setup, a Genesys integration setting group is automatically added in the **Integrations** section. However, integration setting groups can be added and removed manually by using the appropriate **New** and **Remove** buttons in the **Integrations** section.

ScoreCARD Integrations

Genesys ScoreCARD Integration

Genesys Configuration Server

Genesys Config Server Primary Address	<input type="text" value="//gen76pri:2200"/>
Genesys Config Server Secondary Address	<input type="text" value="//gen76sec:2200"/>
User Name	<input type="text" value="default"/>
Password	<input type="password" value="••••••••"/>
Application Name	<input type="text" value="CallREC GIM"/>
Use Secure Connection	<input type="checkbox"/>
Request Time	<input type="text" value="1000"/>
Connection Character Set	<input type="text" value="Local Encoding"/>

Advanced Options

Tenant Name	<input type="text"/>
Root Folder	<input type="text"/>
Enable Annex Based Filtering	<input type="checkbox"/>

Annex Options

Section Name	<input type="text" value="ScoreCARD"/>
Option name for "Import"	<input type="text" value="import"/>
Option name for "Parent Group"	<input type="text" value="parent-group"/>
Option name for "Supervisor"	<input type="text" value="supervisor"/>

Remove

Figure 198: Quality Manager Configuration - Genesys Integration

The Genesys integration setting group contains the following settings:

1. Genesys Configuration Server

The following settings should be pre-configured in the Configuration Server before entering them here, and is usually populated by the values specified during GQM setup.

- **Genesys Config Server Primary Address, Genesys Config Server Secondary Address:** The main and secondary IP address or Fully Qualified

Domain Name (FQDN) for the Genesys Configuration Server.

- **User Name, Password:** The username and password that enable the application to have access to the Configuration Server.
- **Application Name:** The Application Name for the integration module.
- **Use Secure Connection:** Check this setting if the Configuration Server requires a secure (TLS, or Transport Level Security) connection. This is not related to (and independent of) Key Manager settings in QQM.
- **Request Time:** The maximum length of time (in seconds) for the integration module to wait before terminating the connection to the Configuration Server.
- **Connection Character Set:** The character set used for the connection to the Configuration Server. Default is **Local Encoding**, which uses the character set specified for the Call Recording server. The remaining character sets enable a custom character set to be specified if the Configuration Server requires it.

2. Advanced Options

The Advanced Options concern the method of agent filtering during synchronization between integration module and Configuration Server.

- **Tenant Name:** The name of the **Tenant** in Configuration Manager when Configuration Server is configured for multiple tenants. If this field is left blank in a multi-tenant scenario, the Importer processes the parent tenant (**Environment**), losing tenant agent group hierarchy and causing inconsistencies if different tenants use the same agent or agent group name.
- **Root Folder:** The name of a folder in Configuration Manager under which all folders and agent groups are to be imported. If this is left blank, all folders and groups under the top agent groups folder are imported.
- **Enable Annex Based Filtering:** Filtering and exclusion of agents and agent groups is possible using Annex filtering, which is enabled by selecting this box. If enabled, the Annex of the agent or agent group in Configuration Manager must contain the required import key, otherwise the importer imports the whole group and associated agents by default. See [Genesys Importer Features](#) for more information on Annex configuration.

3. Annex Options

If the **Enable Annex Based Filtering** option in **Advanced Options** is selected, the following settings enable customization of the key values used for Annex configuration in Configuration Manager. However, the default settings should be used.

- **Section Name:** The name of the Quality Manager configuration section in the Annex (default: `ScoreCARD`).
- **Option Name for "Import":** (default: `import`).

- **Option Name for "Parent Group":** (default: `parent-group`).
- **Option Name for "Supervisor":** (default: `supervisor`).

User Synchronization Option

Quality Manager user profiles that are imported from Genesys can be configured to either discard all modifications made to them within Quality Manager during synchronization (synchronization 'on'), or to retain all locally-modified settings (synchronization 'off'). In the latter case, the user profile is effectively skipped during synchronization, including the user password, which is always authorized against the user's Genesys password.

By default, all imported users have synchronization switched on. To switch on/off synchronization for a Genesys-imported user profile, select the user in the **User Manager** or within the **Group Manager** and click **Edit**. A check mark in the **Synchronized** checkbox indicates synchronization is activated.

The screenshot shows a dialog box titled "Add or Edit User" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Database: GENESYS
- Synchronized:
- Status: Active (dropdown menu)
- User Role: Agent (dropdown menu)
- Language: Český (dropdown menu)
- Login ID: Agent00
- First Name: Argente
- Surname: Passel
- Email: replace@this.email
- Phone:
- Agent ID:
- None:
- Agent Group: All Agents (dropdown menu)
- Synchronize Now:
- Save:
- Cancel:

Figure 199: User Profile Synchronize Setting for a Genesys Imported User in Quality Manager

Scheduling Genesys Synchronization

Genesys synchronization can be scheduled either in the Call Recording Web GUI, or at the command line as a cron job. The web-based interface is more accessible, but scheduling and running synchronization at the command line can be preferable for fine tuning during the implementation phase.

Before running Genesys synchronization for the first time, ensure that a valid license is uploaded to Quality Manager and Quality Manager has been logged into as `ccmanager` at least once, due to the PCI DSS requirement to change passwords on first access.

Web-based Configuration

Navigate to: **Settings > Configuration > Quality Manager > Quality Manager Setup** and scroll down to **Scheduled Actions**.

The Scheduler section of Genesys Quality Manager Configuration is used to configure when and how often the Genesys importer daemon is run. After initial installation, no scheduling is defined, so by default no import synchronization takes place without this section being updated.

To schedule the running of the Genesys Importer:

The screenshot shows a web interface titled "Scheduled Actions". Below the title bar, there is a "New Scheduled Action" button, a dropdown menu currently showing "Genesys User Import Scheduler", and a red "New" button.

Figure 200: New Scheduled Action

1. Select the **GenesysUser Import Scheduler** option in the **New Scheduled Action** field and click **New**.

The screenshot shows the "Scheduled Actions" configuration page. It features a table with the following fields and values:

Scheduler	Genesys User Import Scheduler	Remove
Start At	23:00	
Periodicity	Daily	
Default Language (Country Code)	US	
Source	GENESYS	
Scorecard Authorized User Login	ccmanager	
Scorecard Authorized User Password	admin	
Agent property to match the AgentID in recorded calls	Agent Login	
New Scheduled Action	Genesys User Import Scheduler	New

Figure 201: Quality Manager Configuration - Genesys Scheduled Actions

2. The following options display:
 - **Start At:** Start the mail delivery daemon at this time (hh : mm using 24 hour clock; for example: 23 : 00).
 - **Periodicity:** Run the mail daemon at these intervals: **Every hour** (the **Start At** value is not used), **Daily**, **Weekly**.

- **Default Language (Country Code):** The country code indicating the language settings for import. This should match the language settings for the Genesys Customer Interaction Management Platform.
- **Source:** Normally GENESYS (this should not be changed).
- **Quality Manager Authorized User Login, Password:** A Quality Manager login user account and password for the importer. Create a dedicated importer user account in Quality Manager with administrative privileges.

Assigning the agent Identification for Genesys Importer Using the "Agent property to match the AgentID in recorded calls" Field

Navigate to: **Settings > Configuration > Quality Manager > Quality Manager Setup** and scroll down to **Scheduled Actions**.

Scheduled Actions	
Scheduler	Genesys User Import Scheduler Remove
Start At	23:00
Periodicity	Daily
Default Language (Country Code)	US
Source	GENESYS
Scorecard Authorized User Login	ccmanager
Scorecard Authorized User Password	admin
Agent property to match the AgentID in recorded calls	Agent Login
New Scheduled Action	Genesys User Import Scheduler New

Figure 202: Quality Manager Configuration - Genesys Scheduled Actions

Each agent imported from Genesys Configuration Manager into Quality Manager has multiple identification fields that identify the agent and person within the Genesys configuration.

Each recorded call holds the AgentID field, as provided by Genesys TServer during recording. This AgentID field can match various agent person identifiers from the Configuration Manager depending on the setup. Which field or property the system uses to match recorded calls with the imported agents must be configured correctly .

Agent property to match the AgentID in recorded calls. Select between:

- **Agent Login:** This uses `[CfgAgentLogin.loginCode]` to identify the agent, this is the default value.
- **User Name:** This uses `[CfgPerson.userName]` to identify the agent.
- **Employee ID:** This uses `[CfgPerson.employeeID]` to identify the agent.

The selected property must match the value that gets saved as agent id in couples. This value is provided by TServer during the recording. There may be multiple Agent Logins associated with each person. Currently Quality Manager can only use one Agent Login per person.

Configuration at the Command Line

The importer script can be set to run at pre-defined intervals (such as daily at midnight) using the Unix [Cron](#) scheduling tool. During Call Recording installation, a Call Recording cron job list is defined, so it is recommended that the Quality Manager Genesys Importer is added to this list, rather than configuring it elsewhere.

To add the Genesys Importer to the list of Call Recording cron jobs, root user permissions are required.

Edit the file at `/etc/cron.d/callrec` and add the following command as a single line (modifying the `wbscimporter` tool parameters as necessary):

```
# Web Scorecard Genesys importer
0 1 * * * root [ -x /opt/callrec/bin/wbscimporter ] &&
/opt/callrec/bin/wbscimporter -c localhost -C US -u ccmanger -p admin -t
GENESYS
```

The above example schedules Quality Manager every night at 01:00 (1:00 am) local time. More information about cron syntax can be found on the Internet, such as on the [Ubuntu Linux community pages](#).

The `wbscimporter` tool parameters can be viewed using the `--help` option, as follows:

```
# /opt/callrec/bin/wbscimporter --help
usage: Ipcc/Genesys to Scorecard user importer
-c,--configurationIP <arg>    URL to configuration manager
-C,--country <arg>           default country that will be assigned to
                              users US, CZ, RU ...
-h,--help                     this help
-l,--logger <arg>            log4j properties
-p,--password <arg>         password of user
-t,--targetdatabase <arg>   Name of database in scorecard table database
                              that will be associated with imported users
                              for authorization.
-u,--username <arg>        username of user, under his rights import
                              will be started
```

Important:

After running a synchronization operation, restart the Web Server in order to see any immediate changes within Quality Manager:

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

Integration Data Definition

Quality Manager synchronization only receives data from Genesys - it never writes or updates the Genesys Configuration Server XML in any way.

During synchronization, Genesys XML data is mapped to the Quality Manager database according to the following table:

Key in Genesys XML file	Table in Quality Manager	Column in Quality Manager
CfgPerson/firstName	sc_users	Name
CfgPerson/lastName	sc_users	Surname
CfgPerson/userName	sc_users	Login
CfgAgentGroup/CfgGroup/managerDBIDs/DBID	sc_users	Role - Supervisor, or Agent
CfgAgentGroup/agentDBIDs/DBID	sc_users	User group belongs
CfgPerson/employeeID	sc_users	AgentId
CfgPerson/state	sc_users	Status
CfgAgentGroup/CfgGroup/name	ccgroups	ccgroupName

Table 19: XML Data Mapping

The Primary Key in the Quality Manager database is the column `ExternalId`.

26 **Setting Up Data Export from Quality Manager**

Quality Manager data exports can be customized at two levels:

- Exported spreadsheet reports obtained by pressing the Export button on the report screen, can be customized by modifying the Report Export Template spreadsheet.
- Excel can be connected directly to the Quality Manager database tables to provide direct read-only connection to virtually all Quality Manager data.

This chapter contains the following sections:

[Customizing the Report Template Spreadsheet](#)

[Integrating the Quality Manager Database with Excel](#)

Customizing the Report Template Spreadsheet

The appearance of the data in the exported Excel report files can be customized by updating the Report Export Template. This spreadsheet file controls the visual formatting of headings and data cells.

Skills of Otis Andrews, login otis.andrews							
Questionnaire: Better Call (2.0)							
Date	Question Group						
	Opening call	Merchant's skills	Call control	žluťoučký kůň	Closing the call	Overall	Overall with weight
7/8/2010	90.00%	80.00%	100.00%	20.00%	60.00%	70.00%	76.00%
7/27/2010	90.00%	50.00%	100.00%	20.00%	15.50%	55.10%	61.10%
8/17/2010	30.00%	60.00%	100.00%	20.00%	5.50%	43.10%	37.10%
10/21/2010	100.00%	70.00%	100.00%	20.00%	5.50%	59.10%	67.10%

Figure 203: Exported Spreadsheet, Showing Default Formatting

The template file simply contains labeled cells for each type of visual format used on report data exports. The following types of Excel cell formats can be modified:

- alignment (excluding merge cells)
- font
- borders
- fill (background color)

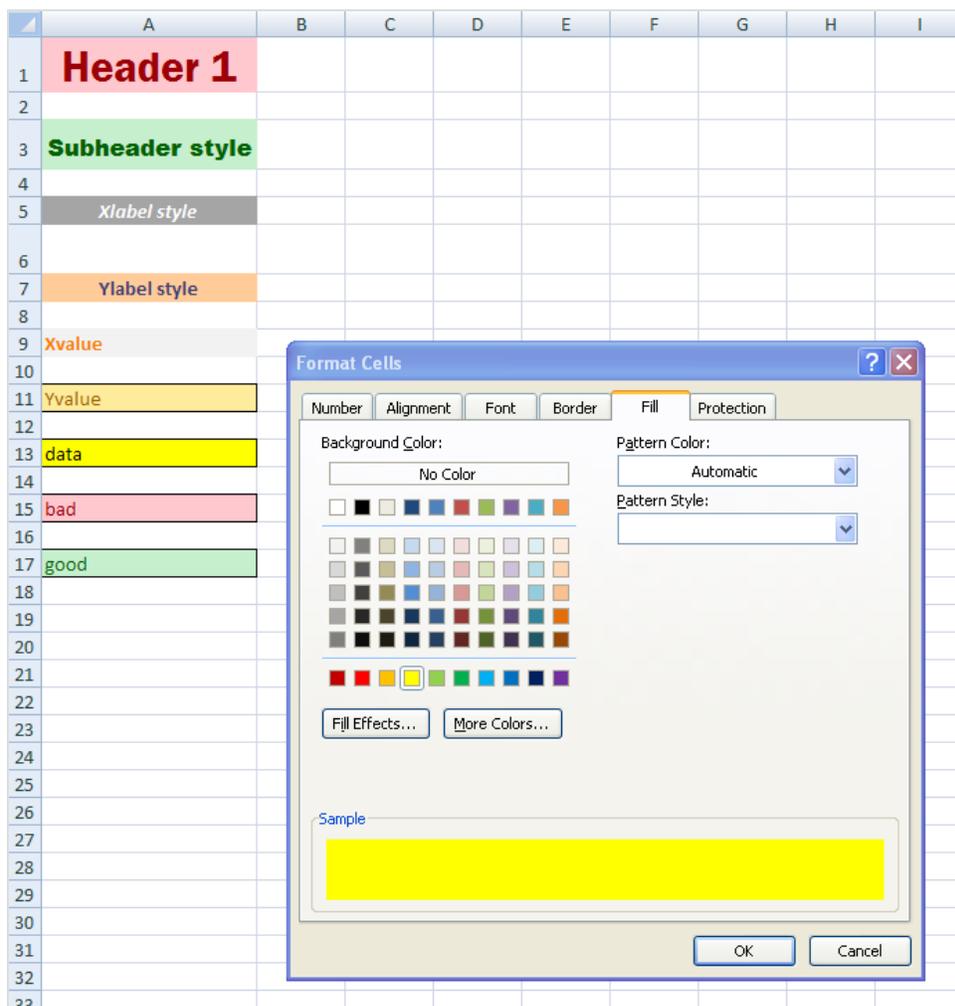


Figure 204: Customizing the Export Template Spreadsheet

The Report Export Template file (`styles.xlsx`) is located in the Quality Manager application's web root directory on the server. Updating this template file therefore requires server administrator permissions.

On a default Call Recording server installation, the location of this file is in the following directory:

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

After updating the template file, it may be necessary to restart the web server at the command line:

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

Exported report data should now reflect the updated formats in the `styles.xlsx` spreadsheet file.

Downloading files from and uploading files to the Call Recording Linux server can be achieved using a program such as [WinSCP](#). If the server is using default settings, the user is only able to log in using the non-root `admin` account (same default password as for root), which has a default starting directory of `/home/admin`

Integrating the Quality Manager Database with Excel

Analyze Quality Manager data on a Windows PC by connecting the Quality Manager database to Microsoft Excel. The procedure described below requires the following:

- Quality Manager is licensed, functional, and using the default PostgreSQL database for data storage.
- Administrator permissions to the GQM installation including root SSH permissions.
- At least installation permissions on the Windows XP, Vista, or Windows 7 client PC running Microsoft Excel.
- The client PC is connected via an IP network to the Quality Manager database server, typically the GQM server for standalone installations.
- Experience of Linux file editing commands, relational database structures, and SQL syntax.

Setup Instructions

Setup consists of three stages:

- Create a read-only user on the Quality Manager database server.
- Set up the ODBC source on the client PC running Excel.
- Import the ODC query files for use with Excel.

Create a Read-only Database User

To create a read only database user:

Connect to the main GQM server via an SSH Client. Log in as `admin`. Enter `su -` to log in as the root user. Enter the password, the default is `zoomcallrec`.

1. Open the file at `/opt/callrec/data/psql/pg_hba.conf` and add a line like the following to enable access from the client PC, where the PC's IP address and range are very narrowly defined, ideally an individual static IP address. The following example allows connection from IP addresses in the range 192.168.10.0 - 192.168.10.255:

```
host all all 192.168.10.0/24 md5
```

2. Save the file, then run the following command to apply this configuration change to the database:

```
/etc/init.d/postgresql reload
```

3. Start up the PSQL tool, logging in to the database as the postgres user:

```
psql -U postgres callrec
```

The following commands in this step are all database commands in SQL format. For best results, type or paste in each individual line, then press ENTER.

4. Create the database user. Replace the sample username: `excel` and password: `excel1234` with preferences, but ensure the remaining commands are updated appropriately:

```
CREATE ROLE excel WITH PASSWORD 'excel1234';
```

5. Enable this user to log in:

```
ALTER ROLE excel LOGIN;
```

6. Enable this user to view the callrec and wbsc schemas, for Call Recording and Quality Manager respectively:

```
GRANT USAGE ON SCHEMA callrec TO excel;  
GRANT USAGE ON SCHEMA wbsc TO excel;
```

7. Grant select (read permission) on the tables from the schema:

```
GRANT SELECT ON wbsc.answers TO excel;  
GRANT SELECT ON wbsc.companies TO excel;  
GRANT SELECT ON wbsc.criteria TO excel;  
GRANT SELECT ON wbsc.evalanswers TO excel;  
GRANT SELECT ON wbsc.evalcalls TO excel;  
GRANT SELECT ON wbsc.evaluations TO excel;  
GRANT SELECT ON wbsc.questforms TO excel;  
GRANT SELECT ON wbsc.questiongroups TO excel;  
GRANT SELECT ON wbsc.questions TO excel;  
GRANT SELECT ON wbsc.sc_users TO excel;  
GRANT SELECT ON wbsc.subevaluation TO excel;  
GRANT SELECT ON wbsc.user_belongsto_ccgroup TO excel;  
GRANT SELECT ON wbsc.ccgroups TO excel;  
GRANT SELECT ON wbsc.callwrapups TO excel;  
GRANT SELECT ON wbsc.interaction_types TO excel;  
GRANT SELECT ON wbsc.categories TO excel;  
GRANT SELECT ON wbsc.database TO excel;  
GRANT SELECT ON wbsc.languages TO excel;  
GRANT SELECT ON wbsc.user_role TO excel;  
GRANT SELECT ON wbsc.roles TO excel;
```

8. Exit the PSQL utility (type \q and press ENTER) and end the SSH session.

Set up the ODBC Source

The following procedure is performed on a Windows PC with administrative permissions. Read the following information before starting:

- The type of Operating System (32-bit or 64-bit). This can be determined using the following Microsoft Support page:
<http://windows.microsoft.com/en-us/windows7/find-out-32-or-64-bit>.
- The type of Microsoft Excel installation (32-bit or 64-bit). This can be seen in Excel 2007 by viewing the **File > Help > About Microsoft Excel** section.

Depending on the type of Excel installation, proceed as follows:

Excel 64-bit

1. Unzip and install the PostgreSQL ODBC driver after downloading the latest zipped MSI installation package from the following URL:

<http://www.postgresql.org/ftp/odbc/versions/msi/>. The 64-bit drivers are named with the suffix `-x64.zip`.

2. Open the following Windows dialog panel: **Administrative Tools > Set up data sources (ODBC)**, or paste the following at a Windows command prompt:
`%systemdrive%\Windows\system32\odbcad32.exe`
3. On the **Drivers** tab, ensure that the PostgreSQL drivers are listed, then click **Add** on the **User DSN** tab.

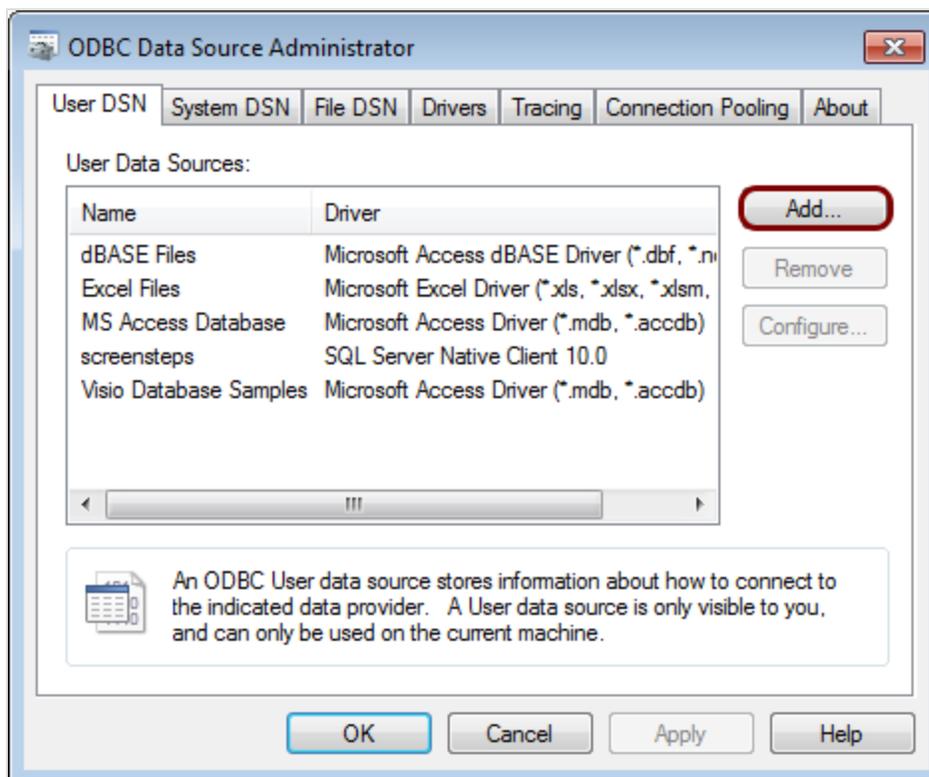


Figure 205: Add an ODBC User DSN

4. Select the **PostgreSQL Unicode(x64)** driver.

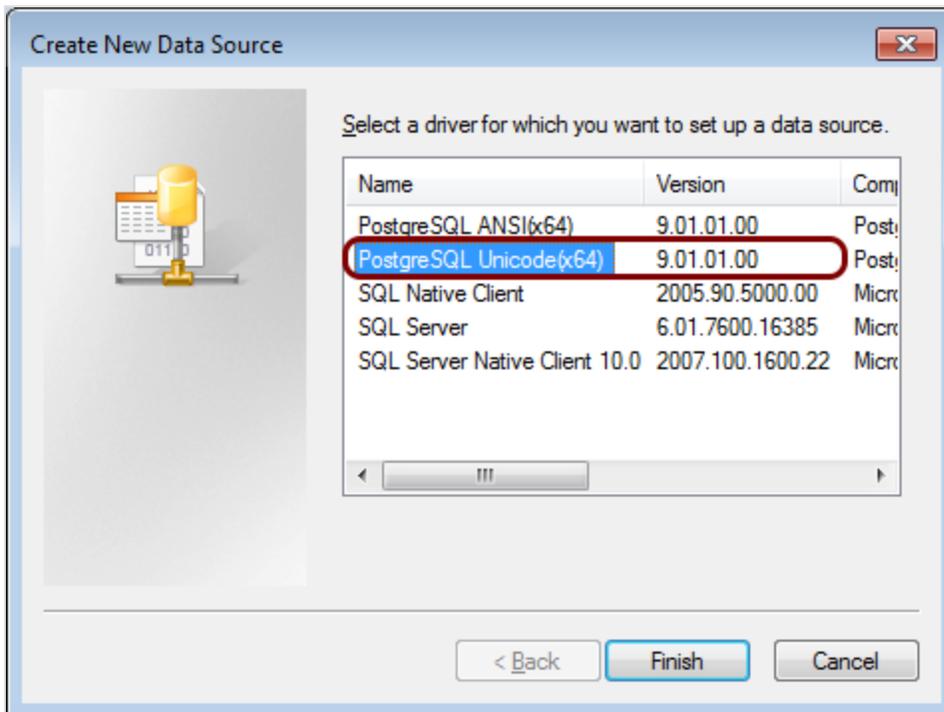


Figure 206: Select the Postgres ODBC Unicode Driver

5. Configure the database server access credentials for the database user created earlier.

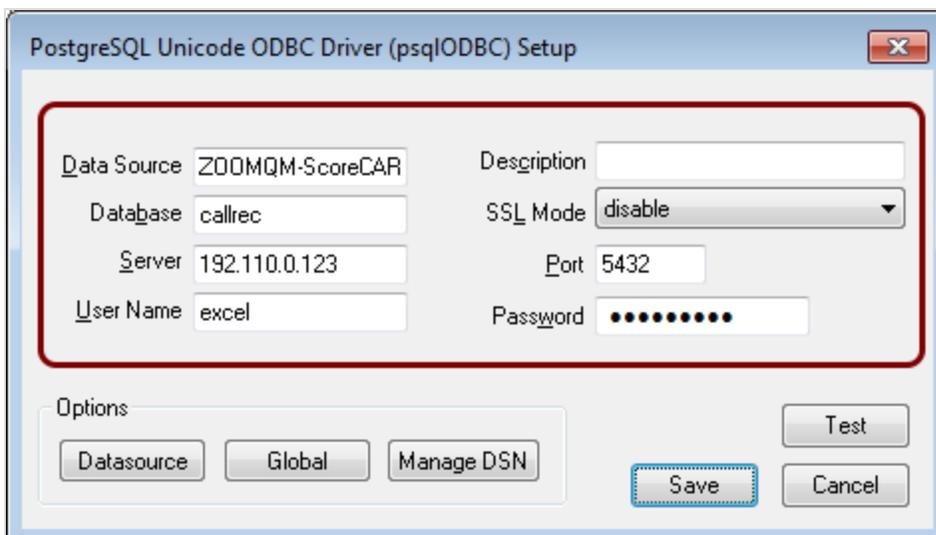


Figure 207: Configure the ODBC Server Parameters

Use the following parameters, modifying the **Server**, **Port**, **Username**, and **Password** fields as required. The **Data Source** field must be set to the value shown to run the sample ODC database queries unmodified.

- **Data Source:** ZOOMQM-ScoreCARD
- **Description:** leave blank.
- **Database:** callrec
- **Server:** (GQM server IP address or fully qualified domain name).
- **Port:** 5432
- **Username:** excel
- **Password:** excel1234

6. Click **Test** to check the connection, then **Save**.

Excel 32-bit

Follow steps 1-6 above (the screens vary), with the following differences:

- **Step 1:** Download a 32-bit MSI installation file (without the `x-64.zip` suffix), then unzip and install it.
- **Step 2:** On a 64-bit Windows system, run the 32-bit ODBC Administrator dialog box to see the 32-bit PostgreSQL ODBC drivers. Paste the following at a Windows command prompt:
`%systemdrive%\Windows\SysWoW64\odbcad32.exe`
- **Step 4:** Select the **PostgreSQL Unicode** driver.

Import the ODC Files

Sample database queries have been provided in ODC (Office Database Connection) format. The samples can be imported into the Office Data Connections list to display data, such as the list of Quality Manager evaluations and details of individual questionnaires, evaluations and users.

To test the sample queries, download and unzip the ODC files to a temporary folder on the client PC. Then do the following:

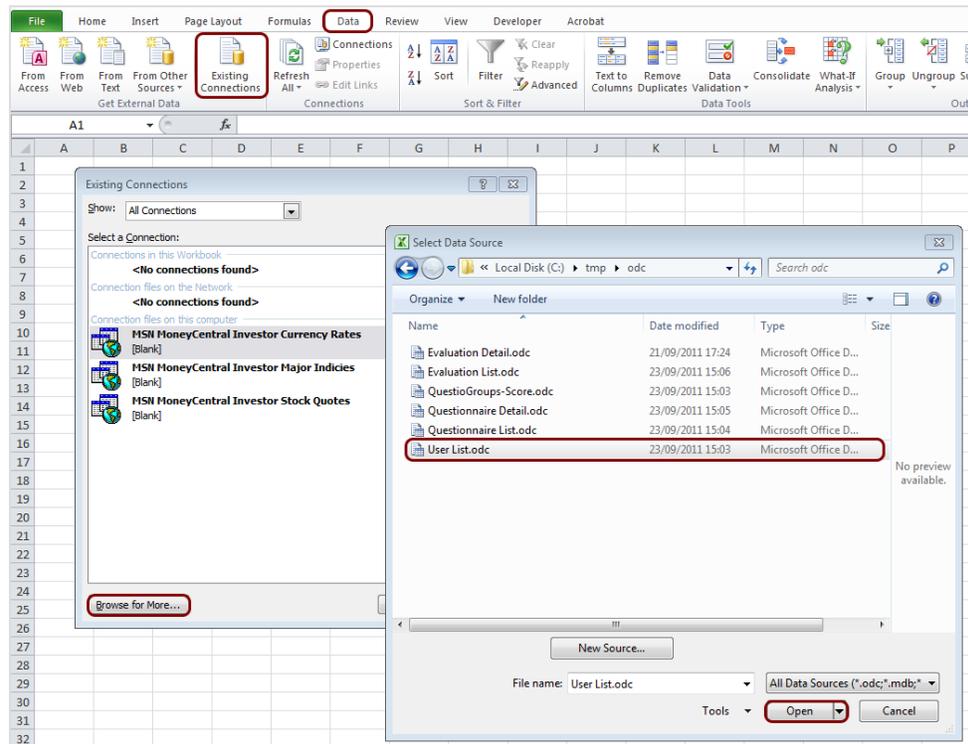


Figure 208: Importing an ODC Query to Excel

1. Open Excel and click the **Data** menu.
2. Click **Existing Connections**.
3. In the **Existing Connections** dialog, click **Browse for More...**
4. Navigate to the location of the unzipped ODC files in the **Select Data Source** dialog and select a file.
5. Click **Open**. If the ODBC data connection, set up earlier is correctly configured, the **Import Data** dialog opens.

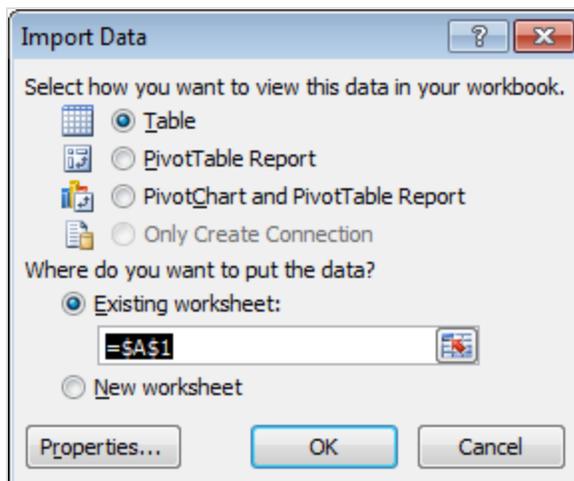


Figure 209: Excel Import Data Dialog

6. In the **Import Data** dialog, decide where and in what format to place the data and click **OK**.

Note: Start with the **Table** format until familiar with the data structure.

userid	name	login	database	sync	status	phone	agentid	identifier_used
1	Admin Admin	admin		1 0	ACTIVE	12345	123	PHONE
2	CcManager CcManager	ccmanager		1 1	ACTIVE	12345	123	PHONE
3	ipccimporterdaemon ipccimporterdaemon	ipccimporterdaemon		1 0	ACTIVE	12345	123	PHONE

Figure 210: User Data Imported into Excel

7. The data is imported. Data is refreshed both when the saved workbook is re-opened and when clicking **Refresh**.

There is no 'remove' option in the Excel **Existing Connections** dialog. However, to remove unnecessary external data connections from this dialog, simply delete the appropriate ODC files or their shortcuts in the My Data Sources directory. The following example opens this location on a Windows 7 PC:

```
%UserProfile%\Documents\My Data Sources.
```

Modifying ODC SQL Queries

Although SQL queries in individual ODC files can be edited in any text editor, there is the danger of errors creeping in due to the character-escaped SQL syntax that is used. A more robust method is to modify the SQL query in Excel after import. This does require that the ODC connection has been successfully imported into Excel using the setup procedure above:

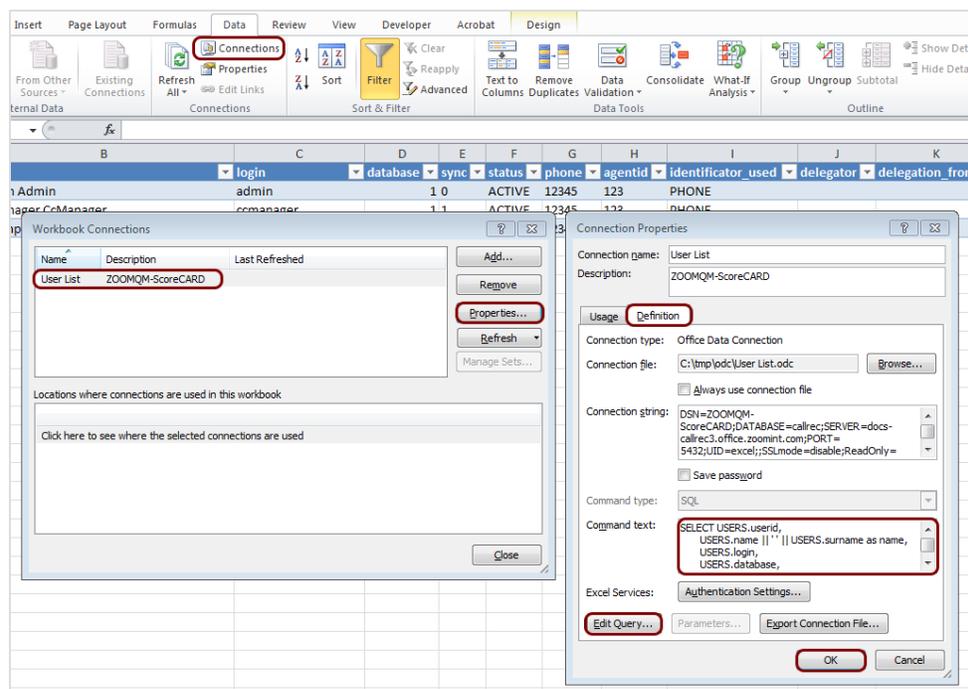


Figure 211: Modifying an ODC Connection Query in Excel

1. In the Excel **Data** menu, click **Connections** to open the **Workbook Connections** dialog.
2. Ensure the ODC connection is displayed and select it.
3. Click **Properties...** to open the **Connection Properties** dialog.
4. Click the **Definition** tab.
 - **EITHER:** View and modify the SQL query directly.
 - **OR:** Edit the query in Microsoft Query. If an error states that: "This query cannot be edited in the Query Wizard", edit the SQL directly by clicking **SQL** in Microsoft Query after acknowledging the error. Close the Wizard to return to the **Connection Properties** dialog.

5. Click **OK** to commit the changes, then accept any ODC file modification requests, after which the data is refreshed from the database according to the updated SQL query.

Chapter

27 Live Monitor

Genesys Live Monitor (previously known as LiveMonitor) enables supervisors to listen to calls and add information as they happen. Live Monitor is a Java application that is launched by clicking on the Live Monitor tab in CallREC.

Live Monitor is normally installed along with Call Recording.

If using Network Address Translation (NAT), additional steps are necessary to enable Live Monitor.

Live Monitor localization is based on the regional settings for the computer that Live Monitor is run on. For example, to reach the settings in Windows 7, navigate to **Control Panel > Region and Language > Keyboards and Languages**.

This chapter contains the following sections:

[Configuring Live Monitor in Call Recording](#)

[Adding External Data Fields](#)

[Restricting Calls in Live Monitor](#)

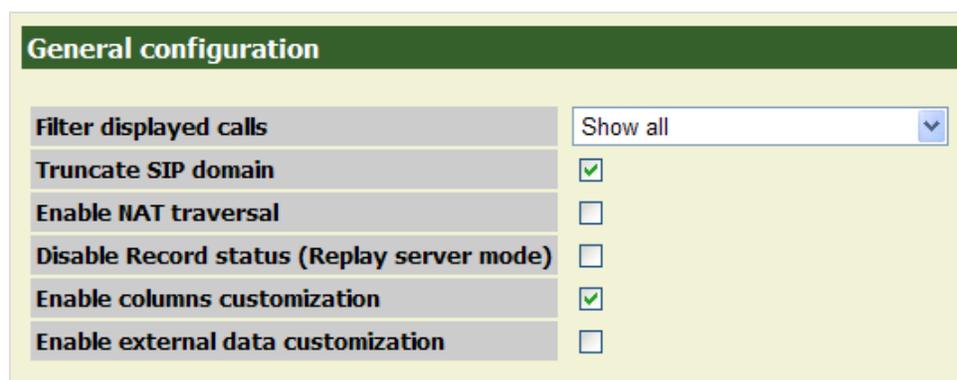
[NAT and Firewall Settings with Live Monitor](#)

Configuring Live Monitor in Call Recording

To configure Live Monitor, log in to Call Recording with administrator privileges. Navigate to **Settings > Extras > Live Monitor**.

Important:

Live Monitor must be run at least once (by running the java file downloaded when clicking on the main page's Live Monitor tab) before this configuration page is displayed.



The screenshot shows the 'General configuration' section of the Live Monitor settings. It includes a dropdown menu for 'Filter displayed calls' set to 'Show all', and several checkboxes: 'Truncate SIP domain' (checked), 'Enable NAT traversal' (unchecked), 'Disable Record status (Replay server mode)' (unchecked), 'Enable columns customization' (checked), and 'Enable external data customization' (unchecked).

General configuration	
Filter displayed calls	Show all
Truncate SIP domain	<input checked="" type="checkbox"/>
Enable NAT traversal	<input type="checkbox"/>
Disable Record status (Replay server mode)	<input type="checkbox"/>
Enable columns customization	<input checked="" type="checkbox"/>
Enable external data customization	<input type="checkbox"/>

Figure 212: LiveMON Configuration

The following options are available:

Filter displayed calls: Enables the selection of what type of calls are displayed. The options are as follows:

- **Show all** (default): All calls registered by Call Recording Core are displayed, regardless of whether they are being recorded or not.
- **Recorded calls only:** Displays only the calls that are actually being recorded.
- **Recorded and prerecorded calls:** Displays all the calls that are either being recorded or that are being prerecorded and may be saved.

Truncate SIP domain: If enabled, SIP extension numbers are displayed without SIP domain suffix. Disable to see full SIP address (this may be useful for debugging purposes).

Enable NAT traversal: Limits number of ports used for communication with Recording Core. See details and recommended firewall settings in the chapter below.

Disable Record status (Replay server mode) : Disables displaying of call status icons and associated actions. This is useful when Live Monitor runs on the replay server. The replay server is not recording calls, so the status icon would report that no calls are being recorded. It may confuse users and thus it is recommended to hide the record status in this case.

Enable columns customization: Enable users to choose which columns are displayed in Live Monitor. The columns are defined by the administrator for both recorded call view and for Live Monitor. Users can adjust the view in the **User Setup > Column Setup** panel.

Enable external data customization: Enables displaying and modification of customized External data fields. The procedure of creating customized external data is described in the following section.

Adding External Data Fields

Add external data options that enable supervisors to add information to Live Monitor. Also restrict the types of calls that display in the Live Monitor interface.

Change the order of the external data fields in Live Monitor with the **Up** and **Down** buttons.

Delete external data fields in Live Monitor with the **Remove** button.

There are three data types that can be added to Live Monitor:

- **Text**: For supervisors comments.
- **List** : For choosing predefined options.
- **Checkbox**: For labeling calls with True or False value.

To add a new data row to Live Monitor, navigate to **Settings > Extras > Live Monitor** and scroll down to **External data customizations**.

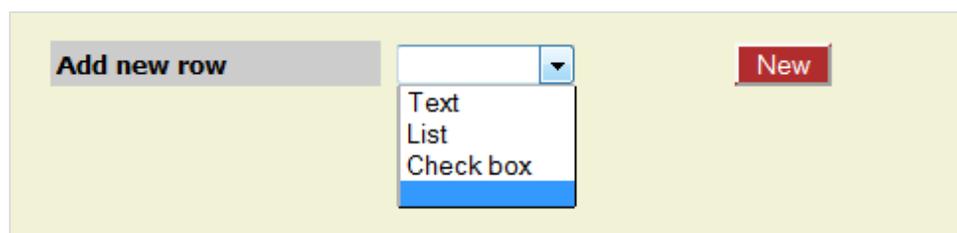


Figure 213: Adding a new row

1. Select a data type from the **Add new row** drop-down list.
2. Click **New**.

For a new Text row:

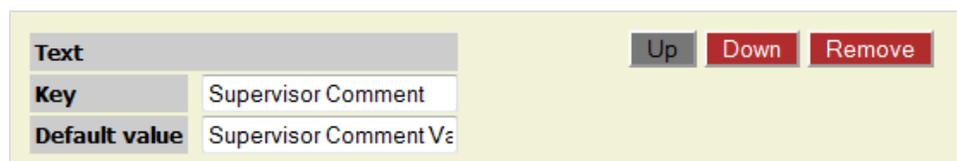


Figure 214: Adding a text field

- **Key**: Type the name of the text field to display.
- **Default value**: Type text that appears in the field by default. This can be overwritten by users.

- Click **Save** configuration to save the new Live Monitor text box.

For a new List row:

List		Up	Down	Remove
Key	Agent Rating			
Default value	Good			Remove
	Average			Remove
	Bad			Remove
New item	some value			New

Figure 215: Adding a Selection List

- **Key:** Type the name of the list.
- **New item:** Type the value of an item then click **New**.
- **Items:** Displays the item values entered. To delete an item from the list, click **Remove**.

3. Click **Save configuration** to save the new Live Monitor list.

For a new Check box row:

Check box		Up	Down	Remove
Key	Trained			
Default value	<input type="checkbox"/>			

Figure 216: Adding a checkbox

- **Key:** Type the name of the checkbox.
- **Default value:** Select this box to make the key a default value. If blank, the box is unselected in Live Monitor.

4. Click **Save configuration** to save the new Live Monitor checkbox.

Restricting Calls in Live Monitor

Live Monitor only displays calls in progress that are within the number range. The number range is specified by the filters for that user in Call Recording. To edit the filters navigate to Call Recording > **Users**, select the user, click **Edit**, and modify the properties in the **Edit User** dialog field **Phone number**. Set a range of phone number using ? as a wild card. For example 20?? sets the range from 2000 to 2099.

NAT and Firewall Settings with Live Monitor

The standard installation of Live Monitor does not include Network Address Translation (NAT) and Firewall access. To enable NAT and Firewall access, change the NAT settings and the open ports in the firewall for Live Monitor.

If a strict firewall is used, open these ports in the firewall to enable Live Monitor to pass through:

TCP:

30400: used by RMI service

30500, 30501: for configuration service, these ports can be changed in `config_manager.xml`

30600, 30601: for core, these ports can be changed in `core.xml`

UDP:

37000-37100: for RTP streams, these ports can be changed via the Call Recording **Web interface under Settings > Recorders > API – Datagrams ports start/end**

28 Viewing and Sending Call Recording Logs

Log files summarize the behavior of the system. Logs record all messages and exceptions generated by Genesys Call Recording components and related applications. All log files use the standard Apache service “log4j” for standardized text only outputs.

This chapter contains the following sections:

[Viewing Logs](#)

[Important Log Files](#)

[Sending Logs to Genesys](#)

[DEBUG Mode](#)

[Logs advanced modifications](#)

Viewing Logs

Logs are located in the following directory:

```
/var/log/callrec
```

The logs are automatically created while Call Recording is running, and log files are rotated each day. The system saves log files for 30 days, and then they are deleted.

To access log files from the Call Recording web interface:

1. Log in as **admin**.
2. Navigate to **Settings > Logs**.
3. Open individual log pages, copy them to the clipboard, or export them for further analysis.

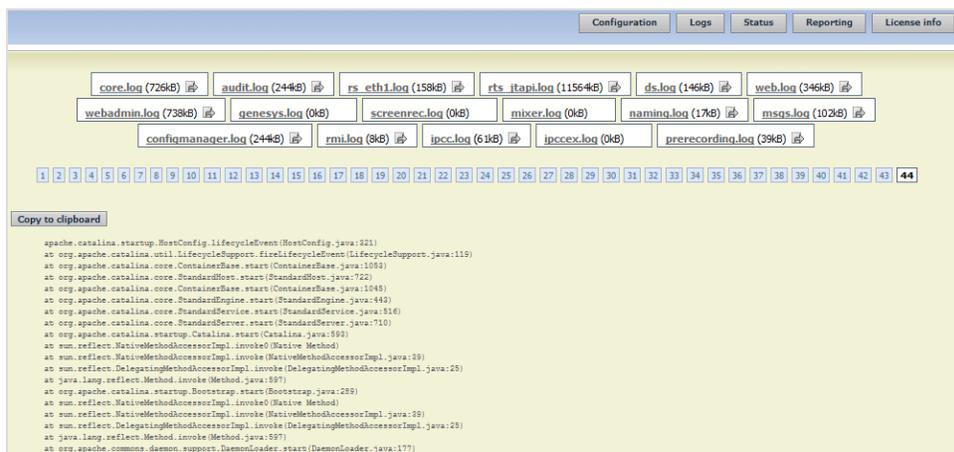


Figure 217: Working with the Call Recording Log Files

To browse through log files:

1. Click the number icons to open log pages.
2. Use the **Copy to clipboard** command to copy the current page to the clipboard.

Important Log Files

There are many log and report files generated by Call Recording, but most important are the following six files:

- `audit.log`: Logs all actions taken during the recording of a call. Also contains information about the codec used for a call.
- `core.log`: Contains information about the core module. Check for errors and exceptions, if an error occurred during recording it should be logged here.
- `rts_jtapi.log`: Contains information about JTAPI connectivity to Cisco CallManager. During CallREC start-up all observed phones are reported here. If there is trouble connecting to the CallManager, check for correct login and JTAPI library version, all this information is reported during module start up.
- `ds.log`: Logs the activity of the Decoder Server. If there is any issue with the call processing (decoding) it is reported here.
- `webadmin.log`: Logs the activity of the Web Administration user interface.
- `webadmin-audit.log`: Records all user actions performed through the web user interface and logs them here. Contains information about which users performed which action.

Sending Logs to Genesys

Log files are particularly helpful for diagnosing problems with the system.

Either:

Send the log files as an email attachment to the Support team (<http://genesyslab.com/support/contact>).

Or:

Send the logs directly using the `bugreport` script. SMTP must be enabled and have internet access.

Sending the Logs as an Email Attachment

To send the logs as an email attachment:

1. Log in as 'admin' then type `su - root`.
2. Tar the `/var/log` folder and enter the following command:

```
tar -pczvf /home/admin/log.tar.gz /var/log/callrec/*
```

3. Connect to Call Recording server by WinSCP.
4. Copy the `log.tar` file from `/home/admin/` folder to the computer.
5. Send the `log.tar` file as an email attachment to <http://genesyslab.com/support/contact>

Sending the Logs with the `bugreport` Script :

To send the logs with the `bugreport` script :

1. Log in with administrator privileges, then type `su - root`.
2. Enter the following command:

```
/opt/callrec/bin/bugreport
```

DEBUG Mode

All Call Recording components use log4j to create logs. This standard Apache service creates comprehensive logs at runtime without modifying the application binary. In most cases there is no need to change logger settings or working mode.

To provide additional debug change from log4j to debug mode.

Every component has its own configuration file for logging. These configuration log files are located in `/etc/callrec/`.

Switching Between log4j and Debug Modes

To switch between log4j and debug logging modes increase the logging activity level:

1. Locate the configuration file that belongs to chosen component and open it. The first line sets the logging activity level:

```
log4j.rootLogger=INFO, file, onlyError
```

Levels of Logging Activity:

- **INFO:** lowest log level, minimal logging
 - **WARNING:** second level, writes into log file the same information as INFO plus any warning messages
 - **ERROR:** stores all text messages generated by the component
 - **DEBUG:** logs everything and stores all operations, exceptions
2. Replace **INFO** with **WARNING**, **ERROR**, or **DEBUG**.
 3. Save the file.
 4. Restart the component to enable the higher logging activity level.

Logs advanced modifications

Genesys Call Recording displays logs on the Status page of the web interface. This enables changes in how much information is contained on a single log page, and which logs are available by editing the web interface configuration file.

The configuration file is located here:

```
/opt/callrec/etc/webadmin.xml
```

Changing the Log Page Size

To change the number of log records displayed on a single page, adjust the number of kilobytes in the value of the `viewSizeLog` item. The default is 8 kilobytes, about 8,000 characters.

1. Find the element with `viewSizeLog`.

```
<ItemLong name="viewSizeLog" value="8"/>
```

2. Change the value.
3. Save the changes.

Adding Logs to the User Interface

The element `SpecifiedConfiguration` `name="externalTools"` identifies the logs to be displayed in the user interface.

- To remove a log from the user interface, delete the line with the log file, or comment the `ItemString` so it is ignored.

To add a log to the user interface:

1. Open the web interface configuration file.
2. Consult the list of log file names (below).
3. Add an `ItemString` to identify the new log filename and the `.log` extension.

```
<ItemString name="log" value="/var/log/callrec/MODULE_NAME.log"/>
```

4. Save the configuration file:

Filename	Comment
Log filename	Logged module or service
audit.log	Call Recording modules audit
callmonitor.log	Call Recording CallMonitor
core.log	Call Recording Core
ds.log	Call Recording Decoder server
error.log	Global errors
genesys.log	Genesys integration
instreamer.log	Instreamer integration
ipcc.log	UCCE integration
ipccex.log	UCCX integration
move.log	Move tool
msgs.log	Recorded calls initiation message
naming.log	Naming service
prerecording.log	Call Recording Prerecording

Filename	Comment
repair.log	Repaircalls tool
rmi.log	Call Recording RMI
rs_ethX.log	Ethernet adapter X (1, 2, 3...)
rts_jtapi.log	JTAPI adapter
rts_sip.log	SIP adapter
rts_skinny.log	Skinny adapter
synchro.log	Synchronization tool
tools.log	All other Tools
webadmin.log	Call Recording Webadmin functionality
webadmin-audit.log	Call Recording Webadmin audit

Table 20: Log File Names

Log File Output Example

```
<SpecifiedConfiguration name="externalTools">
<ItemLong name="viewSizeLog" value="8" description="Page size in kB"/>
<EqualGroup name="logs">
<ItemString name="log" value="/var/log/callrec/core.log"/>
</EqualGroup>
<EqualGroup name="logs">
<ItemString name="log" value="/var/log/callrec/audit.log"/>
</EqualGroup>
<EqualGroup name="logs">
<ItemString name="log" value="/var/log/callrec/rs_eth1.log"/>
<ItemString name="log" value="/var/log/callrec/rs_eth2.log"/>
<ItemString name="log" value="/var/log/callrec/rs_eth3.log"/>
</EqualGroup>
<EqualGroup name="logs">
<ItemString name="log" value="/var/log/callrec/rts_jtapi20.log"/>
<ItemString name="log" value="/var/log/callrec/rts_jtapi.log"/>
<ItemString name="log" value="/var/log/callrec/rts_skinny.log"/>
<ItemString name="log" value="/var/log/callrec/rts_sip.log"/>
</EqualGroup>
<EqualGroup name="logs">
<ItemString name="log" value="/var/log/callrec/ds.log"/>
</EqualGroup>
</SpecifiedConfiguration>
```


Generating and Using Call Recording Reports

Genesys Call Recording generates a variety of reports for administrators and supervisors. These reports can be displayed in a web browser, or exported to email as an attachment.

This chapter contains the following sections:

[Generating a Report](#)

[Report Type](#)

[Report Results Setting](#)

[Setting Up Periodical Reports with Quick Filter](#)

[Report Results](#)

[Time Range Setup for Selected Parameters](#)

[Bad Calls Report](#)

[Not Decoded Calls Report](#)

[Transfers](#)

Generating a Report

To generate a report, log in with administrator privileges and navigate to **Settings > Reporting**.

Name of report: Report Short errors length(seconds):

Reported period Alltime

Total Calls	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Call Recording Quotient (CRQ)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Error Calls	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Averages	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Transfers In	<input type="checkbox"/>	<input type="checkbox"/>	
Transfers Out	<input type="checkbox"/>	<input type="checkbox"/>	
Files Summary	<input type="checkbox"/>	<input type="checkbox"/>	
Busy Hour Call Records (BHCR)	<input type="checkbox"/>	<input type="checkbox"/>	Limit

Report: Show on HTML
 Send by e-mail

Enter email address where you want to send daily reports from CallREC. You can add more addresses separated by a semicolon.

Quick filter option: no filter

From:

July
2011

Wk	Su	Mo	Tu	We	Th	Fr	Sa
26						1	2
27	3	4	5	6	7	8	9
28	10	11	12	13	14	15	16
29	17	18	19	20	21	22	23
30	24	25	26	27	28	29	30
31	31						

To:

July
2011

Wk	Su	Mo	Tu	We	Th	Fr	Sa
26						1	2
27	3	4	5	6	7	8	9
28	10	11	12	13	14	15	16
29	17	18	19	20	21	22	23
30	24	25	26	27	28	29	30
31	31						

Clear filters
 Save filters
 Process

Scheduled tasks overview

Name of report: Quick filter option

Figure 218: Reporting – Parameters

Name of report: changes the options available for the report:

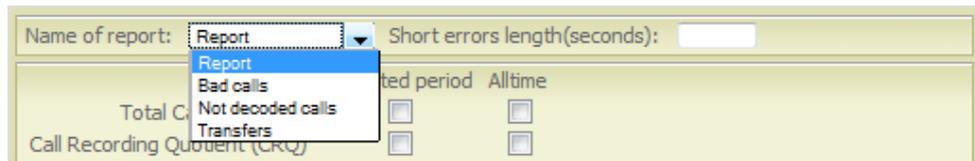


Figure 219: Reports Selection

1. **Report:** All reporting options are available. **Bad calls** limit the report to only calls that are incorrectly recorded or missing information in the database.
Not decoded calls: Limits the report to only calls that have been recorded but not yet decoded and saved. This is useful for analyzing the load levels in the system that may be causing delays.
Transfers: Limits the report to only calls that have been recorded, decoded, and moved to the replay server. This is useful for checking synchronization between the system core server and replay servers.
2. **Short errors length (seconds):** This value sets the minimum call length, in seconds, before a call is included in the report. This enables very short calls to be discarded, and does not include them in the report.

Report Type

Select two types of reports:

	Reported period	Alltime	
Total Calls	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Call Recording Quotient (CRQ)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Error Calls	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Averages	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Transfers In	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Transfers Out	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Files Summary	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Busy Hour Call Records (BHCR)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Limit <input type="text" value="10"/>

Figure 220: Report Parameters Selection

- **Reported period:** Includes records for only the selected time period.
- **Alltime:** Includes all matching records in the database, regardless of time period.

When both types are selected, a matching tables shows the results for the selected time period and for the entire database. This is useful for comparing a selected period with normal system values.

Important:

If there are too many calls that fall outside of the selected time range, this could indicate a high load on the system.

Report Results Setting

Reports are displayed in the web browser, select **Show on HTML**, or sent to an email address, select **Send by e-mail**.



The screenshot shows a light yellow rectangular form with a thin border. Inside the form, the text "Report:" is followed by two radio button options. The first option is "Show on HTML" with a blue radio button that is selected. The second option is "Send by e-mail" with an unselected radio button, followed by a white rectangular input field for an email address.

Figure 221: Report Results Setting

Setting Up Periodical Reports with Quick Filter

To create an automatic periodical report based on a time range, use a Quick filter option. The Quick filter options pre-define a period for the report to be sent to the email recipients.

The image shows a screenshot of a web form for setting up daily reports. It consists of two main input areas. The top area is a text box with a light green background and a thin border. Inside, it contains the text: "Enter email address where you want to send daily reports from CallREC. You can add more addresses separated by a semicolon." To the right of this text is a small input field containing the placeholder text "name@domain.com". The bottom area is another text box with a light green background and a thin border. It contains the text "Quick filter option:" followed by a dropdown menu. The dropdown menu is currently set to "yesterday" and has a small downward-pointing arrow to its right.

Figure 222: Daily Reporting

1. Select a time period from the drop-down list. The best options are yesterday or last week.
2. Enter an email address. To enter multiple recipients of email notifications, use a semicolon “;” to separate email addresses.
3. Click **Save filters**.

The Quick filter report is added to the Scheduled tasks list.

- To remove a task from this list, click **Stop**.
- To remove all tasks from the list, click **Clear filters**.

Report Results

Total Calls: Displays the total number of calls captured by Call Recording. The example below shows not decoded calls, correct calls and error calls.

Total Calls	
Total calls	27254
Short calls	281
Calls to record	26973
Not decoded calls	0
Correct calls	26800
Correct calls length	78:11:49
Error calls	173
Error calls length	02:38:26

Figure 223: Total Calls Captured by Call Recording

Call Recording Quotient (CRQ): Shows the percentage of total calls that have been recorded.

Call Recording Quotient (CRQ)	
Call Recording Quotient (CRQ)	99.358

Figure 224: Percent of Calls Recorded

Error Calls: Generates a table of all error calls, listed by the type of error.

Error calls	
NO_STREAMS	173

Figure 225: Error Calls

Averages: Shows the average number of daily calls and their average length in seconds.

Average count	
Average count per day	21
Average length of calls	53

Figure 226: Average Count

Transfers-in, Transfers-out: Shows the total number of calls synchronized within Call Recording.

Transfers In	
Location	Count
LOCAL	27249
archive-2010.04.13-home-admin-0000.zip	3
archive-2010.04.16-home-admin-0000.zip	1
archive-2010.04.17-home-admin-0000.zip	1

Transfers-out	
Synchronised	0
Duplicated	0
Non synchronised	27254

Figure 227: Synchronized Calls

- Transfers-in includes all call events within the system.
- Transfers-out is the total number of calls that have been decoded, synchronized, and stored for replay.

Files Summary: Shows the number of saved files in the system as processed recordings (MP3 format) and recordings not yet decoded (PCAP).

Files Summary	
.avi	49
.mp3	26789

Figure 228: Total Number of Saved Files in Listed Formats

Busy Hour Call Records(BHCR): Shows recording activity for selected periods.

Busy Hour Call Records (BHCR)	
Hour	Count
2010-02-21 04:00:00+01	328
2010-02-18 18:00:00+01	325
2010-02-19 15:00:00+01	325
2010-02-19 22:00:00+01	325
2010-02-20 06:00:00+01	325
2010-02-20 11:00:00+01	325
2010-02-20 16:00:00+01	325
2010-02-20 21:00:00+01	325
2010-02-21 08:00:00+01	325
2010-02-21 16:00:00+01	325

Figure 229: Recording Levels

Limit: Enables the number of events set to be displayed in the report.

	Reported period	Alltime
Total Calls	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Call Recording Quotient (CRQ)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Error Calls	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Averages	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Transfers In	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Transfers Out	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Files Summary	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Busy Hour Call Records (BHCR)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Limit

Figure 230: Recording Limit Selection

Time Range Setup for Selected Parameters

The time range for reporting parameters can be set by using the Quick filter option, or by selecting the time period using standard calendar controls. If a reporting period is not specified, the whole database of calls is processed for reporting.

The screenshot shows a web interface for setting a time range. It features two calendar grids, one for 'From' and one for 'To', both set to September 2012. Below the calendars are three buttons: 'Clear filters', 'Save filters', and 'Process'. At the bottom, there is a section titled 'Scheduled tasks overview' with a placeholder for 'Name of report Quick filter option'.

From:							
	September						
	2012						
Wk	Su	Mo	Tu	We	Th	Fr	Sa
35							1
36	2	3	4	5	6	7	8
37	9	10	11	12	13	14	15
38	16	17	18	19	20	21	22
39	23	24	25	26	27	28	29
40	30						

To:							
	September						
	2012						
Wk	Su	Mo	Tu	We	Th	Fr	Sa
35							1
36	2	3	4	5	6	7	8
37	9	10	11	12	13	14	15
38	16	17	18	19	20	21	22
39	23	24	25	26	27	28	29
40	30						

Clear filters Save filters Process

Scheduled tasks overview
Name of report Quick filter option

Figure 231: Selecting Time Period

To run a report, click **Process**.

Saved filters should only be set by the administrator.

Bad Calls Report

Figure 232: Error Report Setting

When **Bad Calls** is selected from the Report drop-down list, check the **With external data** box. This includes data from external databases in the **Bad Calls** report.

Couple id	Problem	Start	Duration	Source IP	Destination IP	Caller	Callees	Key	Value
1	RECORDER_LICENSE_PROBLEM	2008-11-04 11:29:18.433+01	10	192.168.7.22	192.168.10.106	3018	3242	CallRecCalledURL TERMINAL_SEP CallRecCallingURL CiscoCallManagerID CiscoGlobalCallID CiscoID TERMINAL_SEP	192.168.10.106:24576(1104) SEP003094C35F57 192.168.7.22:26842(1104) 1 598257 17375473 SEP001AA0886555
2	RECORDER_LICENSE_PROBLEM	2008-11-04 11:50:46.964+01	11	192.168.6.55	192.168.7.31	2017	3030	CallRecCallingURL CallRecCalledURL CiscoCallManagerID CiscoGlobalCallID CiscoID TERMINAL_SEP	192.168.6.55:16384(1115) 192.168.7.31:23704(1115) 1 599437 17376653 SEP0018896D8F5A
3	RECORDER_LICENSE_PROBLEM	2008-11-04 11:50:58.469+01	41	192.168.6.55	192.168.7.31	2017	3030	CallRecCallingURL CallRecCalledURL CiscoCallManagerID CiscoGlobalCallID CiscoID TERMINAL_SEP	192.168.6.55:16384(1115) 192.168.7.31:24846(1115) 1 599437 17376653 SEP0018896D8F5A

Figure 233: Bad Call Report with External Information

When **With external data** is selected, additional information like **Key** and **Value** is displayed.

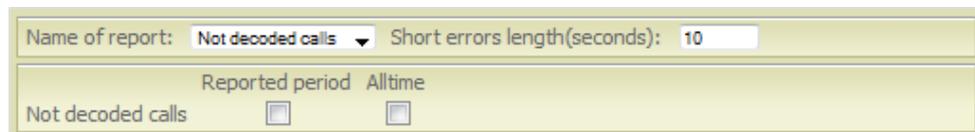
Couple id	Problem	Start	Duration	Source IP	Destination IP	Caller	Callees
1	RECORDER_LICENSE_PROBLEM	2008-11-04 11:29:18.433+01	10	192.168.7.22	192.168.10.106	3018	3242
2	RECORDER_LICENSE_PROBLEM	2008-11-04 11:50:46.964+01	11	192.168.6.55	192.168.7.31	2017	3030
3	RECORDER_LICENSE_PROBLEM	2008-11-04 11:50:58.469+01	41	192.168.6.55	192.168.7.31	2017	3030
4	RECORDER_LICENSE_PROBLEM	2008-11-04 11:53:45.921+01	3	192.168.6.55	192.168.7.31	2017	3030
5	RECORDER_LICENSE_PROBLEM	2008-11-04 12:07:09.265+01	60	192.168.7.44	192.168.7.31	3001	3030
6	RECORDER_LICENSE_PROBLEM	2008-11-04 12:08:11.538+01	27	192.168.7.44	192.168.7.31	3001	3030
7	RECORDER_LICENSE_PROBLEM	2008-11-04 12:08:40.336+01	766	192.168.7.44	192.168.7.31	3001	3030
8	RECORDER_LICENSE_PROBLEM	2008-11-04 12:21:50.125+01	4	192.168.7.44	192.168.7.31	3001	3030
9	RECORDER_LICENSE_PROBLEM	2008-11-04 12:22:09.266+01	9	192.168.7.44	192.168.7.31	3001	3030
10	RECORDER_LICENSE_PROBLEM	2008-11-04 12:22:54.572+01	8	192.168.10.124	192.168.7.31	3259	3030
11	RECORDER_LICENSE_PROBLEM	2008-11-04 12:23:44.426+01	30	192.168.10.124	192.168.7.31	3259	3030

Figure 234: Bad Calls Report without External Information

When **With external data** is not selected, the **Bad calls** report includes only standard data.

Not Decoded Calls Report

The **Not decoded calls** report displays Couple IDs for calls that are in the system, but have not yet been decoded. This is useful for analyzing system performance, as it enables visibility to potential overloads, creating queues before decoding.



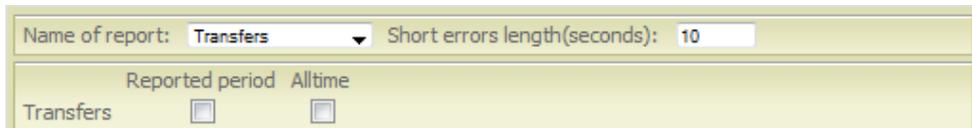
The screenshot shows a form with two rows. The first row contains a dropdown menu labeled 'Name of report:' with 'Not decoded calls' selected, and a text input field labeled 'Short errors length(seconds):' with the value '10'. The second row contains a label 'Not decoded calls' followed by two radio buttons. Above the radio buttons is the text 'Reported period Alltime'.

Figure 235: Not Decoded Call - Parameters

Example: If the Call Center recordings finish at 6pm, it may take several minutes before the system decodes all recordings and saves them. The **Not decoded calls** report shows those calls.

Transfers

When Call Recording is run on a distributed network, the **Transfers** report shows the performance of the system by analyzing whether calls are transferred within the system in the selected time range.



The screenshot shows a form with two rows. The first row contains a dropdown menu set to 'Transfers' and a text input field set to '10'. The second row contains a label 'Reported period' followed by 'Alltime' and two checkboxes, both of which are unchecked.

Figure 236: Transferred Recordings – Parameters

There are two parameters:

- **Outside:** Recordings that are recorded before the specified time range, but are processed in the selected time period.
- **Within:** Recordings that are processed in the selected time period.

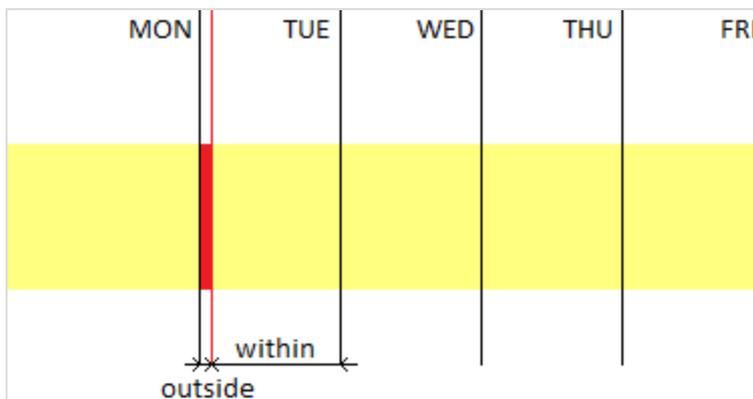


Figure 237: Transfers within and Outside the Specified Time Range

30 SNMP

The Simple Network Management Protocol (SNMP) enables the parameters and functions of servers and applications to be monitored remotely.

Call Recording uses SNMP v2 messaging with an installed agent module, that supports SNMP GET (SNMP SET is not supported). This module is installed during GQM installation in a default configuration, that can be modified via the `/etc/snmp/snmpd.conf` configuration file.

The Call Recording Message Information Block (MIB) defines the variables that are available to SNMP clients. The following data is available from the Call Recording SNMP Agent:

- **Decoder:** number of registered decoders, decoder communicator status, pending requests in decoder queue
- **Recorder:** number of registered recorders, recorder communicator status, SPAN port check (port-up/port-down)

This chapter contains the following sections:

[Structure of the Call Recording SNMP MIB](#)

[Configuring the SNMP Agent for Oracle](#)

[Testing SNMP Functionality](#)

Structure of the Call Recording SNMP MIB

Call Recording defines the SNMP Management Information Base (MIB) as follows:

Node Object ID (OID) Pattern	Explanation
.1.3.6.1.4.1.16321	This root node is used by Genesys Labs, Inc.
.1.3.6.1.4.1.16321.1	The next node is reserved for Genesys software
.1.3.6.1.4.1.16321.1.10	This OID identifies Call Recording modules
.1.3.6.1.4.1.16321.1.10.1	This covers variables with versions of modules
.1.3.6.1.4.1.16321.1.10.1.0	The value of the Master (0) module version
.1.3.6.1.4.1.16321.1.10.1.1	The value of the Core reporter (1) module

Table 21: Table: MIB Structure

The following table contains a summary of the main Call Recording nodes (all Object IDs are prefixed by .1.3.6.1.4.1.16321.):

Node OID	Module Name
1.10.1	Core
1.10.2	Redlines
1.10.4	Observable Naming
1.10.5	Prerecording Server
1.10.6	Decoder Master Communicator
1.10.7	Config Manager Communicator
1.10.8	SRS Communicator
1.10.9	Remote NS
1.10.10	User Interface
1.10.11	Remote JTAPI
1.10.13	Mixer
1.10.15	Genesys Adapter

Table 22: Table: Major MIB Nodes

To display specific Object IDs and values within the Call Recording system MIB, use the Linux command `snmpwalk`, as described in the next section. For a complete list of defined OIDs, please contact <http://genesyslab.com/support/contact>.

Configuring the SNMP Agent for Oracle

Navigate to **Settings > Configuration > Call Recording Core > Database** and scroll down to the oracle pool settings.

The screenshot shows a configuration panel for an Oracle pool. The panel has a green header with the text "oracle". Below the header is a table of configuration fields:

Pool name (for CallREC set "callrec")	oracle
Pool type	lbatis pool
SQL map	Callstorage (Oracle)
Host	oracle.mydomain.com
Port	1521
Database	callrec
Login name	callrec
Password	callrec
Maximum connections	20
Connections on init	1
Timeout	5

At the bottom of the configuration table is a red button labeled "Remove".

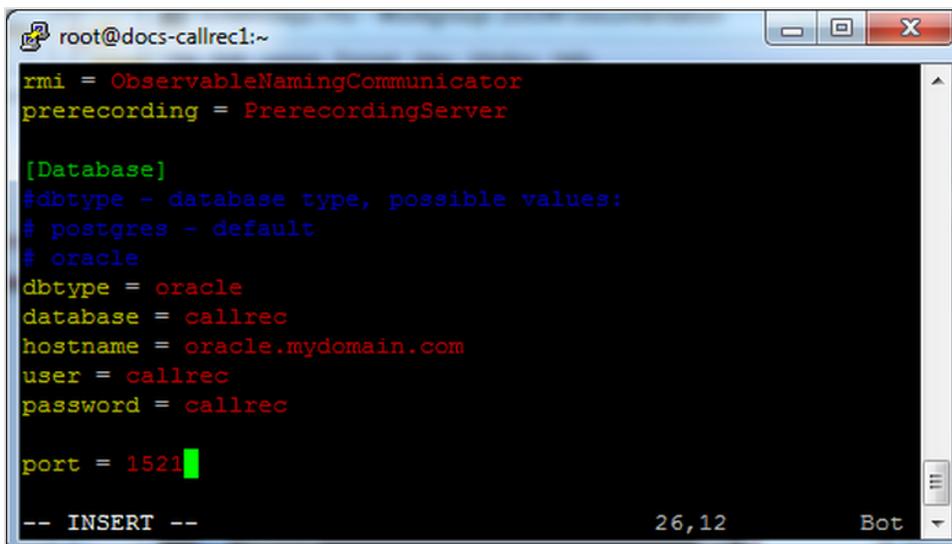
Oracle Pool settings

Read the parameters from the pool configuration for oracle, in the example the pool name is **oracle** where the SQL map is **Callstorage (Oracle)**.

Using an SSH Client such as PuTTY log in to the Call Recording server. Log in as `admin`. Enter `su -` to log in as the root user. Enter the password, the default is `zoomcallrec`.

Using vim or a similar editor modify the SNMP configuration file for example:

```
vim /opt/callrec/SNMP/src/deployment.cfg
```

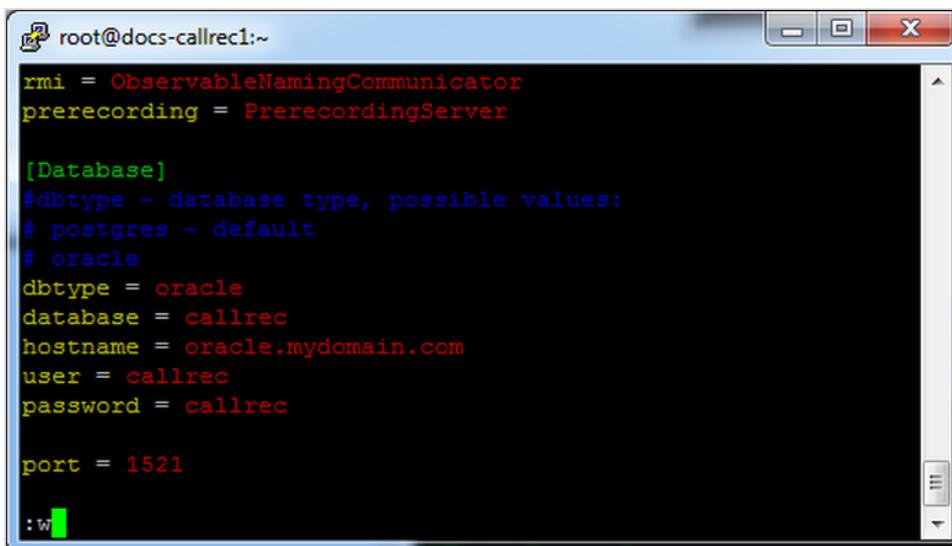


```
root@docs-callrec1:~  
rmi = ObservableNamingCommunicator  
prerecording = PrerecordingServer  
  
[Database]  
#dbtype - database type, possible values:  
# postgres - default  
# oracle  
dbtype = oracle  
database = callrec  
hostname = oracle.mydomain.com  
user = callrec  
password = callrec  
  
port = 1521  
  
-- INSERT --
```

Figure 238: Database Settings in Config

Press the **i** key to go into **--INSERT--** mode. Use the cursor keys to position the cursor over the values.

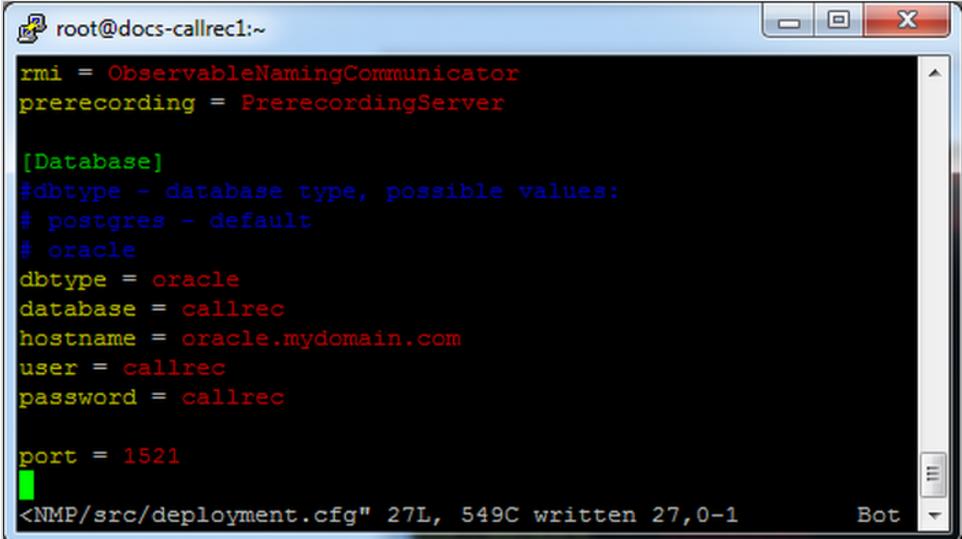
1. Change **dbtype** value to `oracle`.
2. Change the parameters `database`, `hostname`, `user` (login name), `password` and `port` to values found on the configuration page.
3. Note that the editor is in **--INSERT --** mode.



```
root@docs-callrec1:~  
rmi = ObservableNamingCommunicator  
prerecording = PrerecordingServer  
  
[Database]  
#dbtype - database type, possible values:  
# postgres - default  
# oracle  
dbtype = oracle  
database = callrec  
hostname = oracle.mydomain.com  
user = callrec  
password = callrec  
  
port = 1521  
  
:w
```

Figure 239: Image Caption

Press **Esc** to go into command mode. The **-- INSERT --** message at the bottom of the screen disappears indicating the exit of editing mode. Enter the command **:w** to save the configuration. A message displays to confirm that the config is written, for example:



```
root@docs-callrec1:~  
rmi = ObservableNamingCommunicator  
prerecording = PrerecordingServer  
  
[Database]  
#dbtype - database type, possible values:  
# postgres - default  
# oracle  
dbtype = oracle  
database = callrec  
hostname = oracle.mydomain.com  
user = callrec  
password = callrec  
  
port = 1521  
  
<NMP/src/deployment.cfg" 27L, 549C written 27,0-1
```

Figure 240: Confirmation Message

To exit from vim type **:q!**.

It should not be necessary to restart Call Recording.

Testing SNMP Functionality

The following test procedures assume the default configuration.

To test the functionality of SNMP from the command line, when logged in with `root` level permissions, use the Linux shell command `snmpwalk` with the following syntax:

```
snmpwalk -v 1 -c public localhost .1.3.6.1.4.1.16321.1
```

If SNMP is functioning properly, the following confirmation appears:

```
SNMPv2-SMI::enterprises.16321.1.10.0.1.0 = STRING: "ZOOM CallREC - Master
module, Copyright (C) 2002-2011 ZOOM International, All Rights Reserved"
SNMPv2-SMI::enterprises.16321.1.10.0.2.0 = INTEGER: 1
SNMPv2-SMI::enterprises.16321.1.10.0.3.0 = STRING: "WARNING"
SNMPv2-SMI::enterprises.16321.1.10.0.6.1.0 = INTEGER: 10
    <-- More Output Lines -->
End of MIB
```

Important:

Before testing a new installation and configuration of SNMP, wait 5-7 minutes to enable SNMP to gather information.

Each object in the system listed in the Management Information Base (MIB) has its own error and information codes, to track the status of the system. Consult the SNMP documentation for further information.

Chapter

31

Backing Up Call Recording

This chapter describes recommendations on how to integrate a Call Recording server into the overall company disaster recovery plan.

Please note that deployment of these scripts requires at least basic knowledge of Linux systems.

This chapter contains the following sections:

Compatible Backup Agents

Genesys Quality Management solutions are built on Red Hat Linux operating systems. When choosing a third party backup agent, make sure it is compatible with the currently installed version of RedHat on the Call Recording server.

This can be verified in the system by issuing the command

```
cat /etc/redhat_release
```

We do not provide system backup solutions.

Target components

- Calls
- Database
- Configuration

Back up calls

Recommended period: Daily

Days to keep: Depending on data retention policy and storage capability

Recommended tool: Call Recording Archive

Use the Call Recording Archive Tool for backing up calls. Archived calls can be easily restored with all of the information about the calls, (refer to the Call Recording admin guide).

Back up the database

Recommended period: Daily

Days to keep: 14 days history

Recommended tool: Genesys database backup script.

Back up Call Recording configuration

Recommended period: Weekly

Days to keep: 21 days history

Recommended tool: Genesys configuration backup script

Genesys Backup Scripts

Download

Both Configuration and Database backup scripts can be found in the archive under the following link:

http://download.zoomint.com/CallREC/Backup/ZOOM_CFG_DB_Backup_Scripts.zip

This archive always contains the latest version of the backup scripts.

Configuration

There are a few important variables to configure in the scripts.

TARGETDIR: This is the target directory where the backups are saved. If this directory does not exist, the script attempts to create it.

ROTATES : This is the number of previous backups to be kept, for example, if ROTATES is set to 5, it keeps 5 previous backups + the current one.

NOTIFY: Enables or disables e-mail notification. 0 = OFF / 1 = ON.

EMAIL: If e-mail notifications are enabled, configure the recipients here. Use a space or a semicolon between recipients as a separator to configure more than 1 recipient.

For the database backup script, there is also the **DATABASENAME** variable, that specifies the name of the Call Recording database.

Other variables do not need to be changed.

Please note that the **LOGFILE** and **LOCKFILE** directories need to exist. These directories are created by default during Call Recording installation, so they should not have to be created manually. Check that the directories exist prior to running the script for the first time.

Implementation

The use of cron task scheduler is recommended. To implement these scripts on the server:

1. Copy the scripts to the server. We recommend placing the scripts into the directory `/opt/callrec/bin/` in order to maintain a reasonable logical structure of data placement.
2. Make sure that the scripts are executable by issuing the following commands.

```
chmod +x backup_database.sh
chmod +x backup_configuration.sh
```

3. Create a new job for cron. Open up `/etc/cron.d/callrec` in a text editor, for example vim.

```
vim /etc/cron.d/callrec
```

4. Add the following entries (if deploying both scripts):

```
0 0 * * 0 root /opt/callrec/bin/backup_configuration.sh
30 0 * * * root /opt/callrec/bin/backup_database.sh
```

These entries make cron run the configuration backup run every Sunday at 00:00, and run the database backup every day at 00:30.

For more information about cron job scheduling, please refer to cron man pages, or search the Internet for a guide. For example, <http://www.cyberciti.biz/faq/how-do-i-add-jobs-to-cron-under-linux-or-unix-oses/>.

5. Finish editing the file, save it and restart cron daemon to apply the changes.

```
/etc/init.d/crond restart
```

6. The backup scripts are now successfully deployed.

Using Oracle

This chapter describes how to use Oracle databases with GQM.

This chapter contains the following sections:

[Overview](#)

[Pre-install Tasks](#)

[Installation and Setup](#)

Overview

Since version 8.0.48x of Genesys Quality Management, Oracle databases have been supported in addition to (or instead of) the embedded PostgreSQL database supplied as part of the GQM installation. Oracle databases are more suitable for GQM installations requiring high throughput and performance (such as for large numbers of call center agents and simultaneous calls), and often is a part of an enterprise database strategy, enabling more efficient corporate maintenance and backup procedures to be used.

An Oracle database can be used as the only configured database (storing all system and call data), or it can be used in addition to the embedded PostgreSQL database for specific data, such as call information. These database mappings can be modified after GQM installation, although a system restart is required after each change.

A typical use case for mixed database deployments is a larger cluster scenario, where multiple smaller distributed recorder installations (using embedded PostgreSQL databases) provide call data to a central Oracle-powered Replay Server.

This Guide covers two main operations: deploying GQM 8.1.5x with Oracle database support, and migrating existing data between PostgreSQL and Oracle.

All Oracle-specific operations such as database installation, setup and maintenance are the responsibility of the customer; Genesys does not provide direct support for maintaining Oracle databases as we do for the embedded PostgreSQL database.

Supported Oracle Versions

GQM 8.1.5x supports Oracle database version 11g and above.

Pre-install Tasks

Before beginning the GQM installation, complete the following tasks:

1. Set up access and credentials, **administrative database username & password** and optional tablespace for GQM, in a running Oracle database instance. The administrative username and password is needed during installation for the `create_schema.sh` script.

The Oracle database instance used for GQM must have its `NLS_LANG` setting set to the following:

```
AMERICAN_AMERICA.AL32UTF8
```

This setting can be checked by running the following database query:

```
Select * from nls_database_parameters;
PARAMETER                                VALUE
-----
NLS_LANGUAGE                             AMERICAN
NLS_TERRITORY                             AMERICA
NLS_CURRENCY                              $
NLS_ISO_CURRENCY                          AMERICA
NLS_NUMERIC_CHARACTERS                    .,
NLS_CHARACTERSET                          AL32UTF8
NLS_CALENDAR                              GREGORIAN
NLS_DATE_FORMAT                           DD-MON-RR
NLS_DATE_LANGUAGE                         AMERICAN
NLS_SORT                                   BINARY
NLS_TIME_FORMAT                           HH.MI.SSXFF AM
NLS_TIMESTAMP_FORMAT                      DD-MON-RR HH.MI.SSXFF AM
NLS_TIME_TZ_FORMAT                        HH.MI.SSXFF AM TZR
NLS_TIMESTAMP_TZ_FORMAT                   DD-MON-RR HH.MI.SSXFF AM TZR
NLS_DUAL_CURRENCY                         $
NLS_COMP                                   BINARY
NLS_LENGTH_SEMANTICS                      BYTE
NLS_NCHAR_CONV_EXCP                       FALSE
NLS_NCHAR_CHARACTERSET                    AL16UTF16
NLS_RDBMS_VERSION                         11.2.0.1.0
```

2. For any Oracle clients (for example Oracle SQL Developer) used with the GQM database schema, ensure that their host OS also has the `NLS_LANG` property set to `AL32UTF8`, which can be achieved as follows:

- On a **Unix-based host OS**, ensure the following system variable is defined:

```
NLS_LANG= AMERICAN_AMERICA.AL32UTF8
```

See Installation and Setup for an example of how to achieve this in RedHat Linux.

- On a **Windows-based host OS**, ensure the following registry key is set:

```
"NLS_LANG"=" AMERICAN_AMERICA.AL32UTF8"
```

This registry key is in the Oracle HOME registry branch, which can be found at the following locations for Oracle 11g:

either:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\KEY_OraClient11g_home1
```

or:

```
HKEY_LOCAL_MACHINE\SOFTWARE Wow6432Node\ORACLE\KEY_OraClient11g_home1
```

Installation and Setup

This guide assumes a new installation of GQM 8.1.5x. Earlier versions of GQM must be upgraded to at least version 8.0.48x using the upgrade wizard or manual upgrade methods before the following steps can be attempted (see the Upgrade Guide).

A basic overview of installation and setup is included here, refer to the Implementation Guide for details of the standard installation procedure.

Run Standard Installer and Setup

- Start the installer from the DVD / ISO and install the required Operating System (RHEL) as normal.
- After OS installation and a system restart, log in as root administrator and start GQM setup (/opt/callrec/bin/callrec-setup).

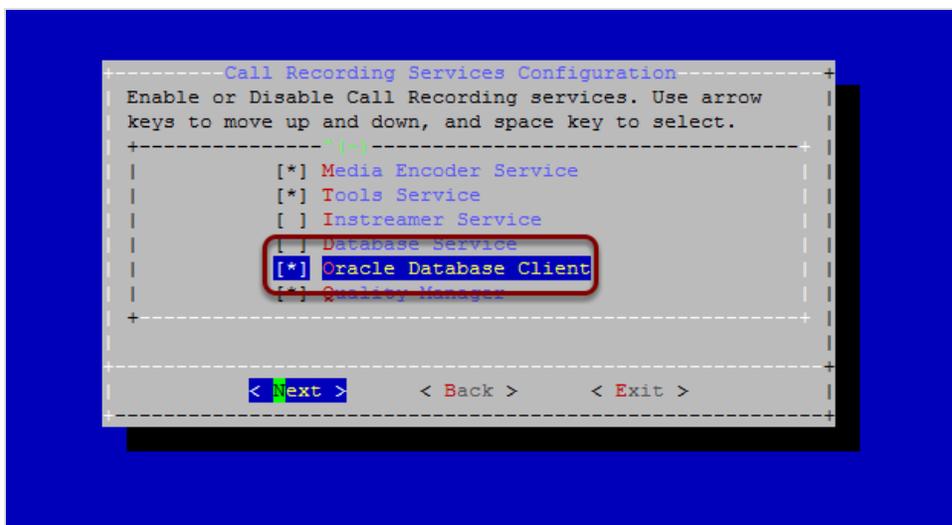


Figure 241: Selecting the Oracle Database Client

- On the services screen, select **Oracle Database Client** and unselect **Database Service** (the embedded PostgreSQL database).

Important:

To install and set up the embedded PostgreSQL database in addition to Oracle, run GQM setup twice; the first time selecting Database Service, and the second time selecting Oracle Database Client as described here.

After installation is complete, database pools, such as call data and Quality Manager data, can then be assigned to the different databases as appropriate – see [Database Pool Mapping](#).

```
Genesys Quality Management 8.1.402 Configuration
| Enter your Oracle configuration.
| +-----+
| |Oracle IP Address :   oracle.mycompany.com|
| |Oracle Port :       1521                 |
| |Oracle Database :   zoomdb              |
| |Oracle User :       callrec             |
| |Oracle Password :   *****            |
| |Retype Password :   *****            |
| |Oracle WBSC Database : zoomdb          |
| |Oracle WBSC User :   wbsc              |
| |Oracle WBSC Password : ****           |
| |Retype Password :   ****              |
| +-----+
|
| < Next >   < Back >   < Exit >
| +-----+
```

Figure 242: Oracle Database Configuration

- Enter the Oracle database credentials as follows:
 1. **Oracle IP Address** (or hostname): for example `oracle.mycompany.com`
 2. **Oracle Port**: default is `1521`
 3. **Oracle Database** (or service name for Call Recording schema): for example `zoomdb`
 4. **Oracle User** (Call Recording database user): for example `callrec`
 5. **Oracle Password** (Call Recording user password): default is `callrec`
 6. **Oracle WBSC Database** (or service name for Quality Manager schema): for example `zoomdb`
 7. **Oracle WBSC User** (Quality Manager database user): for example `wbsc`
 8. **Oracle WBSC Password** (Quality Manager user password): default is `wbsc`

Tip:

Within the Call Recording product, the term 'callrec' is often seen, which is synonymous with this product.

Similarly, the terms 'scorecard' and 'wbsc' are synonymous with the Quality Manager product, and 'screenrec' is synonymous with the Screen Capture product.

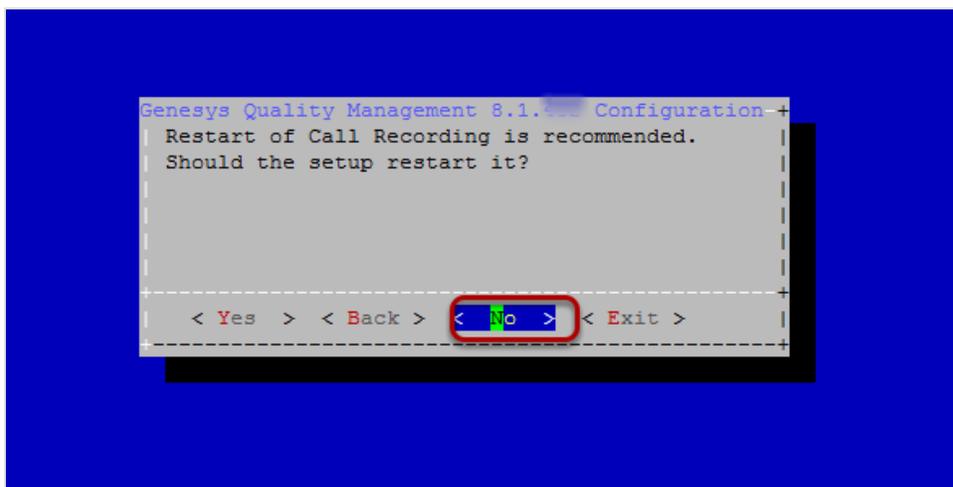


Figure 243: Do Not Restart Call Recording

- On the screen confirming a restart of Call Recording after completing Call Recording setup, select **No**.
- Complete the GQM setup.

Set System Variables

- After GQM setup is complete, **you must set the system variable NLS_LANG** to the following value for correct Oracle Client character set selection:
AMERICAN_AMERICA.AL32UTF8
1. To check the current setting, ensure that you are logged in as the root user and run the following command:

```
env | grep NLS_LANG
[output:]
                NLS_LANG=AMERICAN_AMERICA.AL32UTF8
```

2. If the command output is not the same as the above, run the following commands to set the NLS_LANG system variable:

```
echo >> ~/.bash_profile "NLS_LANG=\"AMERICAN_AMERICA.AL32UTF8\""
echo >> ~/.bash_profile "export NLS_LANG"
source ~/.bash_profile
```

Install the Database Schema

When configuring an Oracle connection for the first time, create the Call Recording and Quality Manager user schema (database tables, triggers, etc.) in the Oracle database. This is achieved in one operation by running a schema creation script in the `/opt/callrec/db_oracle_scripts/scripts` directory.

To remove the existing Call Recording and Quality Manager schema from the Oracle database, see [Removing the Database Schema](#).

The script is available in two versions; the `create_schemas.sh` script is a Linux shell script, while the `create_schemas.bat` script is a Windows DOS script. In either case, the script must be run on a host server that has the Oracle 11g database client installed. This Oracle client software is automatically included as part of the GQM installation process, so the `create_schemas.sh` Linux script can be run directly on the GQM server, as described here. An additional benefit of running the schema creation script on the GQM server, is to also ensure that there is correct connectivity between the server and Oracle database.

The Linux version of the script must be run by the root user. The script's usage and parameters are as follows:

```
sh create_schemas.sh [system_user] [system_password] [database_name]
[callrec_schema_name] [wbsc_schema_name] [options]
```

The DOS version is similar to the Linux version, but `create_schemas.bat` is run without the `sh` command preceding it.

The following parameters are required:

- `system_user`: Username of database administrator account (see [Pre-install Tasks](#)).
- `system_password`: Password of database administrator account.
- `database_name`: Database name, in the form:
`//hostname.domain.com:port/servicename`
for example: `//oracle.mycompany.com:1521/zoomdb`.
- `callrec_schema_name`: Call Recording schema user entered as **Oracle User** earlier during GQM setup.
- `wbsc_schema_name`: Quality Manager schema user entered as **Oracle WBS User** earlier during GQM setup.

Type: `sh create_schemas.sh` [without parameters] to view this parameter list.

The following options can also be specified (not required in a standard installation):

`--tbscallrec` value: name of tablespace used for Call Recording (default: `USERS`).

`--tbswbsc` value: name of tablespace used for Quality Manager (default: `USERS`).

`--temptbs` value: name of tablespace for temporary files (default: `TEMP`).

`--data Y [or] N`: create default data: user admin, roles, etc. (default: `Y`). This should normally be set to `Y` for new installations – the only case where the data is not required is when preparing a new database for migration of existing data.

`--create_admin Y [or] N`: create the user `callrec_wbsc_admin` with administrative rights for the Call Recording and Quality Manager schema (default: `N`).

This user has the following default credentials:

username: `callrec_wbsc_admin`

password: `adm`

See the following Linux example:

```
cd /opt/callrec/db_oracle_scripts/scripts
sh create_schemas.sh system sys //oracle.mycompany.com:1521/zoomdb callrec
wbsc --tbscallrec USERS --tbswbsc USERS --temptbs TEMP --data Y --create_
admin Y
```

Update Oracle Schema

After the `create_schema.sh` script is run, the new Call Recording and Quality Manager schema users have their passwords set to the **default** password values on the **Oracle configuration** screen in GQM setup. See the **Oracle User Password** and **Oracle WBSC User Password** properties in the chapter: [Run Standard Installer and Setup](#) for more details. If the default values were used, no updates are required.

- If different password values were used, reset the passwords for these Call Recording and Quality Manager schema users within Oracle. Consult the Oracle documentation for how to reset database user passwords.

Start Call Recording

- After schema installation is complete, start Call Recording at the command line, ensuring that the Call Recording Core service starts (indicating correct database connection):

```
service callrec start
```

Note that some other services may not start since they are not fully configured or await license activation, see the Implementation Guide for more details.

Installation and basic setup are now complete. Configure Call Recording and Quality Manager via their respective web interfaces (see the Call Recording Administration Guide and Quality Manager Administration Guide).

Troubleshooting Database Parameters

If there are any issues in starting up, check the database parameters in `/opt/callrec/etc/core.xml`, and the error log at `/opt/callrec/logs/error.log`.

After completing GQM setup with the Oracle Database Client service activated, the `core.xml` file should contain database pool configuration entries similar to the following (here with the default entries used earlier):

```

    <Pool name="callrec"
poolType="cz.zoom.util.db.pool.ibatis.IbatisPool">
    <Url dbName="zoomdb" host="oracle.mycompany.com" port="1521"/>
    <Login password="callrec" userName="callrec"/>
    <Connections init="1" max="20" timeOut="5"/>
    <SpecificSetting>
    <Value name="sqlMapClass">
cz.zoom.callrec.core.callstorage.pojo.oracle.SqlMap</Value>
</SpecificSetting>
    </Pool>
    <Pool name="Maintenance"
poolType="cz.zoom.util.db.pool.ibatis.IbatisPool">
    <Url dbName="zoomdb" host="oracle.mycompany.com" port="1521"/>
    <Login password="callrec" userName="callrec"/>
    <Connections init="1" max="20" timeOut="5"/>
    <SpecificSetting>
    <Value name="sqlMapClass">
cz.zoom.callrec.tools.bean.oracle.SqlMap</Value>
</SpecificSetting>
    </Pool>
    <Pool name="keymanager"
poolType="cz.zoom.util.db.pool.ibatis.IbatisPool">
    <Url dbName="zoomdb" host="oracle.mycompany.com" port="1521"/>
    <Login password="callrec" userName="callrec"/>
    <Connections init="1" max="20" timeOut="5"/>
    <SpecificSetting>
    <Value name="sqlMapClass">
cz.zoom.callrec.keyman.impl.pojo.oracle.SqlMap</Value>
</SpecificSetting>
    </Pool>
    <Pool name="scorecard"
poolType="cz.zoom.util.db.pool.ibatis.IbatisPool">
    <Url dbName="zoomdb" host="oracle.mycompany.com" port="1521"/>
    <Login password="wbsc" userName="wbsc"/>
    <Connections init="1" max="20" timeOut="5"/>
    <SpecificSetting>

```

```
<Value name="sqlMapClass">  
cz.zoom.scorecard.business.data.xmlOracle.SqlMap</Value>  
</SpecificSetting>  
</Pool>
```

Modify the dbName, host, password, and username properties (for all occurrences) if required, then restart Call Recording:

```
service callrec restart
```

If there are issues with connections between Call Recording or Quality Manager to the Oracle database instance, contact Genesys Support.

33 Database Migration to Oracle

This section covers the scripts and procedures necessary to migrate Call Recording and Quality Manager database data between the embedded PostgreSQL database and an external Oracle database; both PostgreSQL to Oracle and Oracle to PostgreSQL migration can be performed.

For customers with existing GQM deployments using PostgreSQL, the pattern of deployment and migration depends on the current version and products installed. See the Deployment and Migration Scenarios section.

This chapter contains the following sections:

[Deployment and Migration Scenarios](#)

[Migration Requirements](#)

[Call Recording Migration](#)

[Quality Manager Migration](#)

Deployment and Migration Scenarios

The following scenarios illustrate the basic tasks necessary to accomplish a successful migration to an Oracle database for the given installed software versions. These scenarios use GQM 8.1.492 as the final target version; however the minimum target version is 8.0.48x, in order to leverage the Oracle database.

Call Recording Only (Existing version: 8.0.46x - 8.0.47x)

- Create a new 8.1.51 Installation with Oracle.
Upgrade the existing Call Recording PostgreSQL database to the latest minor version using the database scripts provided with the official Call Recording ISO in the `/opt/callrec/dbscripts/updates` directory.
- [Perform Call Recording database migration of calls](#) to 8.1.51 (using `/opt/callrec/bin/dbmigration` script included with the 8.1.5x installation, with a correctly configured `/opt/callrec/etc/migration.xml` file for PostgreSQL to Oracle migration).

Call Recording (8.0.46x – 8.1.5x) + Quality Manager

- Create new 8.1.51 Installation with Oracle
- Upgrade existing Call Recording PostgreSQL database to latest minor version (using database scripts provided with official Call Recording ISO in `/opt/callrec/dbscripts/updates` directory).
- [Perform Call Recording database migration of calls](#) to 8.1.51 (using `/opt/callrec/bin/dbmigration` script included with the 8.1.5x installation).
- Upgrade existing Quality Manager PostgreSQL database to version 8.1.51 (using `/opt/callrec/bin/scmigration2` script in the 8.1.5x installation, with a correctly configured `/opt/callrec/etc/migration.xml` file for PostgreSQL to PostgreSQL migration).
- [Perform Quality Manager database migration](#) from PostgreSQL to Oracle (using `/opt/callrec/bin/scmigration2` script in the 8.1.5x installation, with a correctly configured `/opt/callrec/etc/migration.xml` file for PostgreSQL to Oracle migration).

Migration Requirements

The following information specifies the product and database version requirements for Call Recording and Quality Manager database migration.

Important:

1. Quality Manager migration from PostgreSQL to Oracle requires a SOURCE installation of GQM 8.0.48x (or higher), due to schema incompatibilities with earlier database versions.
For Quality Manager 8.0.46x – 8.0.47x migration to Oracle, it is therefore necessary to FIRST upgrade the earlier GQM version to GQM 8.0.48x (or higher) before attempting data migration.
Refer to the supported upgrade procedure.
 2. Migrated Quality Manager evaluations do not play without separate (Call Recording) migration of the calls used in the evaluations.
-

Migration Overview

Before running the migration scripts, the target database must be empty; if any data does exist from an earlier migration, this is likely to be overwritten.

The following migration procedure is based on the migration of an existing GQM 8.1.5x installation with embedded PostgreSQL database to Oracle. A functional, empty Oracle database instance is assumed, with no pre-created Call Recording or Quality Manager schema.

The migration scripts create two separate Oracle schema for Call Recording and Quality Manager.

The entire migration process is performed at the command line, logged in as the root user with full permissions. A working knowledge of XML syntax is assumed.

Call Recording Database Migration from PostgreSQL to Oracle

Source database:

PostgreSQL database for an existing Call Recording 8.0.46x(or higher) installation (PostgreSQL 8.4 or higher is required for GQM (8.0.46x or higher) installations).

Target database:

Empty Oracle 11g (or higher) database.

Call Recording Database Migration from Oracle to PostgreSQL

Source database:

Oracle: 11g (or higher) database for an existing GQM 8.0.48x (or higher) installation.

Target database:

Empty PostgreSQL 8.4 (or higher) database.

Quality Manager Database Migration from PostgreSQL to Oracle

Source database:

PostgreSQL database for an existing GQM 8.0.48x (or higher) installation.

Target database:

Empty Oracle 11g (or higher) database.

Quality Manager Database Migration from Oracle to PostgreSQL

Source database:

Oracle: 11g (or higher) database for an existing GQM 8.0.48x (or higher) installation.

Target database:

Empty PostgreSQL 8.4 (or higher) database.

Call Recording Migration

Edit the migration configuration XML file at
`/opt/callrec/etc/migration.xml` as follows:

Source Database Pool

Within the `Database` node, create and insert a new database pool, representing the source ('from') database (in this case PostgreSQL), using the following code (with values for `host`, `port`, `dbName`, `username`, `password` updated appropriately):

```
<Pool name="callrec50xsource"
poolType="cz.zoom.util.db.pool.ibatis.IbatisPool">
  <Url host="localhost" port="5432" dbName="callrec"/>
  <Login userName="callrec" password="callrec"/>
  <Connections max="20" init="1" timeOut="5"/>
  <SpecificSetting>
    <Value name="sqlMapClass">
cz.zoom.callrec.tools.migration.db.version50.SqlMap</Value>
  </SpecificSetting>
</Pool>
```

Note that the `sqlMapClass` value must be correct, reflecting the correct version (version50 = Call Recording database version 8.1.51) and database driver (PostgreSQL).

The pool names used can differ, as long as they are unique and correctly referenced later.

Target Database Pool

Create and insert a second new database pool below the first, representing the target ('to') database (in this case Oracle), using the following code (with values for `host`, `port`, `dbName`, `username`, `password` updated appropriately):

```
<Pool name="callrec50xtarget"
poolType="cz.zoom.util.db.pool.ibatis.IbatisPool">
  <Url host="oracle.mycompany.com" port="1521" dbName="zoomdb"/>
  <Login userName="callrec" password="callrec"/>
  <Connections max="20" init="1" timeOut="5"/>
  <SpecificSetting>
    <Value name="sqlMapClass">
cz.zoom.callrec.tools.migration.db.version50.oracle.SqlMap</Value>
    </SpecificSetting>
  </Pool>
```

The `sqlMapClass` value must reflect the correct version and database driver. For Oracle, this value would be:

```
cz.zoom.callrec.tools.migration.db.version50.oracle.SqlMap
```

For PostgreSQL, this value would be the same as used for the earlier source pool, that is:

```
cz.zoom.callrec.tools.migration.db.version50.SqlMap
```

Source and Target Assignment

Finally, the new source and target database pools need to be correctly assigned for the migration operation. This is achieved by adding the following two nodes in the `SpecifiedConfiguration` section:

Export Node

Within the first `Group` node (with `name` value set as `export`) add the following `EqualGroup` node, ensuring the `dbPool` value reflects the source database pool name you defined earlier:

```
<EqualGroup name="export">
  <Value name="name">cr50xsource</Value>
  <Value name="dbPool">callrec50xsource</Value>
  <Value name="class">
cz.zoom.callrec.tools.migration.db.version50.ExportImpl</Value>
</EqualGroup>
```

The `class` value should again represent the correct version (8.1.492 here) and database driver (PostgreSQL here). The 8.1.492 Oracle class value would be:

```
cz.zoom.callrec.tools.migration.db.version50.oracle.ExportImpl
```

The `name` value used (`cr50xsource`) can be any permitted within XML syntax rules, and is the export reference name used later when running the migration scripts.

Import Node

Similarly, within the second `Group` node (with `name` value set as `imports`) add the following `EqualGroup` node, ensuring the `dbPool` value reflects the target database pool name you defined earlier:

```
<EqualGroup name="import">
  <Value name="name">cr50xtarget</Value>
  <Value name="dbPool">callrec50xtarget</Value>
  <Value name="class">
cz.zoom.callrec.tools.migration.db.version50.oracle.ImportImpl
</Value>
</EqualGroup>
```

Once again, ensure the correct `class` value is used (the class here representing database version 8.1.492 for the Oracle driver). The equivalent class value for the 8.1.492 PostgreSQL database driver would be:

```
cz.zoom.callrec.tools.migration.db.version50.ImportImpl
```

The name value used (`cr50xtarget`) can be any permitted within XML syntax rules, and is the import reference name used later when running the migration scripts.

Run the Migration Script

After saving the migration.xml file, the Call Recording migration script can be run. This takes the following form:

```
/opt/callrec/bin/dbmigration [-config <config> | -configfile <configfile>]
[-countCRC] [-dryrun] [-export <name>] [-import <name>] [-limit <limit>] [-
logger <logger>] [-migrate <options>] [-nobind]
```

The parameters and options are as follows:

Parameter	Option(s)
-config <config>	URL to running configuration manager, for example //localhost:30400/migration. Use this method OR -configfile.
-configfile <configfile>	Use a configuration file, for example /opt/callrec/etc/migration.xml. Use this method OR -config.
-countCRC	Check and count the CRC for each file. WARNING: this heavily impairs migration performance
-dryrun	Test mode, don't modify files or database. Displays all operations to be performed.
-export <export>	Specify the export database configuration group, for example cr50xsource.
-help	Display usage help.
-import <import>	Specify the import database configuration group, for example cr50xtarget.
-limit <limit>	Limit number of calls processed at one time. Default value: 1000.
-logger <logger>	log4j properties file to define the logging properties (doesn't exist by default) for example /opt/callrec/etc/migration.log4j.properties Similar to all Call Recording tool/script log4j parameters (see similar xxxx.log4j.properties files in the /opt/callrec/etc/ directory)
-migrate <migrate>	What to migrate – select from the following options: all – both OLD Quality Manager & Call Recording (note that this option removes OLD

Parameter	Option(s)
	Quality Manager if it exists in the target database) <code>callrec</code> – all Call Recording data <code>calls</code> – Call data <code>roles</code> – User roles
<code>-nobind</code>	Do not attempt to bind to the RMI registry. This option is only enabled in exceptional circumstances, normally it should be ignored. Default is to bind to RMI.

Table 23: Parameters and Options

Sample (minimal)

```
/opt/callrec/bin/dbmigration -migrate callrec -export cr50xsource -import cr50xtarget
```

It is recommended to try a test run of the script using the `-dryrun` option (see the parameters above), before attempting a 'real' data migration.

After running the 'real' migration, use an Oracle database administration tool, such as Oracle SQL Developer or TOAD, to verify that the migration has taken place.

Quality Manager Migration

Quality Manager migration configuration is very similar to the earlier Call Recording method. Quality Manager can either be migrated from or to the same Oracle database (but different schema) as Call Recording, or from/to a completely different Oracle database. In this case, the former default scenario is used, which migrates Quality Manager from an embedded PostgreSQL database to the same Oracle database as Call Recording (but different schema).

Once again, edit the migration configuration XML file at `/opt/callrec/etc/migration.xml` as follows.

Source Database Pool

Within the `Database` node, create and insert a new database pool, representing the source ('from') Quality Manager database (in this case PostgreSQL), using the following code (with values for `host`, `port`, `dbName`, `username`, `password` updated appropriately):

```
<Pool name="scorecard50xsource"
poolType="cz.zoom.util.db.pool.ibatis.IbatisPool">
  <Url host="localhost" port="5432" dbName="callrec"/>
  <Login userName="wbsc" password="wbsc"/>
  <Connections max="20" init="1" timeOut="5"/>
  <SpecificSetting>
    <Value name="sqlMapClass">
cz.zoom.scorecard.business.data.SqlMap</Value>
  </SpecificSetting>
</Pool>
```

Note that the `sqlMapClass` value must be correct (and is different to that for the Call Recording version).

For PostgreSQL, this value would be:

```
cz.zoom.scorecard.business.data.SqlMap
```

For Oracle, this value would be:

```
cz.zoom.scorecard.business.data.xmlOracle.SqlMap
```

The pool names used can differ, as long as they are unique and correctly referenced later.

Target Database Pool

Create and insert a second new database pool below the first, representing the target ('to') Quality Manager database (in this case Oracle), using the following code (again with values for `host`, `port`, `dbName`, `username`, `password` updated appropriately):

```
<Pool name="scorecard50xtarget"
poolType="cz.zoom.util.db.pool.ibatis.IbatisPool">
  <Url host="oracle.mycompany.com" port="1521" dbName="zoomdb"/>
  <Login userName="wbsc" password="wbsc"/>
  <Connections max="20" init="1" timeOut="5"/>
  <SpecificSetting>
    <Value name="sqlMapClass">
cz.zoom.scorecard.business.data.xmlOracle.SqlMap</Value>
  </SpecificSetting>
</Pool>
```

The `sqlMapClass` value must be correct as in the sample.

For Oracle, this value would be the same as used for the earlier source pool:

```
cz.zoom.scorecard.business.data.xmlOracle.SqlMap
```

For PostgreSQL, this value is:

```
cz.zoom.scorecard.business.data.SqlMap
```

Source and Target Assignment

The new Quality Manager source and target database pools need to be correctly assigned for the migration operation. However, unlike the earlier Call Recording method, a complete new `SpecifiedConfiguration` node must be created within the `Configuration` node, which then contains the export and import nodes.

For clarity, the whole new `SpecifiedConfiguration` node is shown below, which should be added after the first (Call Recording) `SpecifiedConfiguration` node (with name value migration), but still within the `Configuration` node.

```
<SpecifiedConfiguration name="scorecardMigration">
  <Group name="exports">
    <EqualGroup name="export" egName="sc50xsource">
      <Value name="dbPool">scorecard50xsource</Value>
      <Value name="class">cz.zoom.scorecard.migration.ExportImpl</Value>
    </EqualGroup>
  </Group>
  <Group name="imports">
    <EqualGroup name="import" egName="sc50xtarget">
      <Value name="dbPool">scorecard50xtarget</Value>
      <Value name="class">cz.zoom.scorecard.migration.ImportImpl</Value>
    </EqualGroup>
  </Group>
</SpecifiedConfiguration>
```

For the first `Group` node (with name value set as `exports`), ensure the `EqualGroup` node's `dbPool` value reflects the Quality Manager source database pool name defined earlier. Similarly, within the second `Group` node (with name value set as `imports`) ensure that the `EqualGroup` node's `dbPool` value reflects the Quality Manager target database pool name defined earlier.

Important:

The export and import Quality Manager `EqualGroup` configuration nodes are the same as for Call Recording, apart from two minor

differences:

- The name property for `EqualGroup` nodes is here renamed to `egName`
 - The class values do not change depending on database type and version
-

Run the Migration Script

After saving the changes made to the `migration.xml` file, the Quality Manager migration script can now be run. This takes the following form:

```
/opt/callrec/bin/scmigration2 [-config <config> | -configfile
<configfile>] [-export <name>] [-import <name>]
[-limit <limit>] [-logger <logger>] [-migrate <options>]
```

The parameters and options are as follows:

Parameter	Option(s)
-config <config>	URL to running configuration manager ,for example, //localhost:30400/migration. Use this method OR -configfile.
-configfile <configfile>	Use a configuration file, for example /opt/callrec/etc/migration.xml. Use this method OR -config.
-export <export>	Specify the export database configuration group, for example, sc50xsource.
-help	Display usage help.
-import <import>	Specify the import database configuration group, for example sc50xtarget.
-limit <limit>	Limit number of evaluations processed at one time. Default value: 1000.
-logger <logger>	log4j properties file to define the logging properties (doesn't exist by default) for example /opt/callrec/etc/scmigration2.log4j.properties Similar to all Call Recording tool/script log4j parameters (see similar xxxx.log4j.properties files in the /opt/callrec/etc/ directory)
-migrate <migrate>	What to migrate, select from the following options: all: all Quality Manager data (users, questionnaires, evaluation data) users: users only questforms: questionnaires only usersquestforms: users and questionnaires only Important: Playing Evaluations

Parameter	Option(s)
	Migrated Quality Manager evaluations do not play without separate (Call Recording) migration of the calls used in the evaluations.

Table 24: Migration Options

Sample (minimal)

```
/opt/callrec/bin/scmigration2 -configurl //localhost:30400/migration  
-export sc50xsource -import sc50xtarget -migrate all -limit 1000
```

After running the migration, use an Oracle database administration tool, such as Oracle SQL Developer or TOAD, to verify that the migration has taken place.

Chapter

34 Oracle Mapping and Maintenance

The majority of Oracle database maintenance tasks are beyond the scope of this document, and are the responsibility of the Oracle database administrator. However, the following procedures are specific to the GQM installation.

This chapter contains the following sections:

[Database Pool Mapping](#)

[Removing the Database Schema](#)

[Additional Reference](#)

Database Pool Mapping

Database pools, such as those for call data, Quality Manager data, etc, can be mapped to different database instances, if these are available to GQM. For example, several Oracle database instances, or both the embedded PostgreSQL database and an Oracle database instance, or other external PostgreSQL / Oracle databases, etc.

Re-mapping database pools can be accomplished in the Call Recording Web GUI and directly in the XML configuration files. In both cases, Call Recording needs to be restarted.

Important:

Switching databases can lead to configuration data loss!

If database pools such as the main `callrec` pool are re-mapped on a configured system, any existing configuration data, such as recording rules, users and passwords, need to be re-entered.

Call Recording Web GUI

After logging in as system administrator in the Call Recording Web GUI, navigate to the **Settings > Configuration > Call Recording Core > Database** tab.

The screenshot shows the 'Database' configuration page in the Call Recording Web GUI. On the left is a navigation menu with 'Database' selected. The main area is titled 'Database' and shows configuration for a pool named 'callrec'. The configuration fields are as follows:

Field	Value
Pool name (for CallREC set "callrec")	callrec
Pool type	lbatis pool
SQL map	Callstorage (PostgreSQL)
Host	192.168.110.78
Port	5432
Database	callrec
Login name	callrec
Password	callrec
Maximum connections	20
Connections on init	1
Timeout	5

At the bottom left, there are two buttons: 'Save configuration' and 'Reload configuration'. At the bottom right, there is a 'Remove' button.

Figure 244: Database Pool Mapping in the Web GUI

1. For each database pool (for example `callrec`), select the appropriate database mapping from the **SQL map** drop-down list.
2. Update the connection details as required.
3. Click **Save configuration**.

Restart Call Recording (see below for one method).

XML Configuration Files

Log on to the server running the configuration service as a root user. Edit the database pool configuration in the file `/opt/callrec/etc/core.xml`.

The following xml snippets show the main Call Recording call data pool xml for (default) Oracle and PostgreSQL mapping.

Oracle Mapping Sample:

```
<Pool name="callrec" poolType="cz.zoom.util.db.pool.ibatis.IbatisPool">
  <Url dbName="zoomdb" host="oracle.mycompany.com" port="1521"/>
  <Login password="callrec" userName="callrec"/>
  <Connections init="1" max="20" timeOut="5"/>
  <SpecificSetting>
    <Value name="sqlMapClass">
cz.zoom.callrec.core.callstorage.pojo.oracle.SqlMap</Value>
    </SpecificSetting>
  </Pool>
```

PostgreSQL Mapping Sample:

```
<Pool name="callrec" poolType="cz.zoom.util.db.pool.ibatis.IbatisPool">
  <Url dbName="callrec" host="192.168.110.78" port="5432"/>
  <Login password="callrec" userName="callrec"/>
  <Connections init="1" max="20" timeOut="5"/>
  <SpecificSetting>
    <Value name="sqlMapClass">
cz.zoom.callrec.core.callstorage.pojo.SqlMap</Value>
    </SpecificSetting>
  </Pool>
```

- Edit the database pool mapping, ensure the correct `sqlMapClass` is assigned, and save the file.
- Restart the Call Recording service by typing the command: `service callrec restart`.

Removing the Database Schema

If an attempt at installing the Call Recording and Quality Manager database schema was only partially successful, or they are no longer required in the Oracle database, remove the schema using the `drop_schemas` script (in the same scripts directory as the `create_schemas` script: `/opt/callrec/db_oracle_scripts/scripts`).

The removal script is available in two versions; the `drop_schemas.sh` script is a Linux shell script, and the `drop_schemas.bat` script is a Windows DOS script.

The script's usage and parameters are as follows (for the Linux version):

```
sh drop_schemas.sh [system_user] [system_password] [database_name]
[callrec_schema_name] [wbsc_schema_name] [options]
```

The DOS version is similar to the Linux version, but `drop_schemas.bat` is run without the `sh` command preceding it.

The following parameters are required:

- `system_user`: Username of database administrator account (see [Pre-install Tasks](#)).
- `system_password`: Password of database administrator account.
- `database_name`: Database name, in the form:
`//hostname.domain.com:port/servicename`
for example: `//oracle.mycompany.com:1521/zoomdb`.
- `callrec_schema_name`: Call Recording schema user; by default this is the **Oracle User** value on the Oracle parameters screen in GQM Setup.
- `wbsc_schema_name`: Quality Manager schema user; by default this is the **WBSC User** value on the Oracle parameters screen in GQM Setup.

Type: `sh create_schema.sh` [without parameters] to view this parameter list.

The following options can also be specified (not required in a standard installation):

`--drop_admin Y [or] N`: delete the user `callrec_wbsc_admin`. This user is created by the `create_schemas` script when the `create_admin Y` option is specified. The user has administrative rights for the Call Recording

and Quality Manager schema. See the topic [Install the Database Schema](#) for more information.

See the following Linux example:

```
cd /opt/callrec/db_oracle_scripts/scripts
sh drop_schemas.sh system sys //oracle.mycompany.com:1521/zoomdb
callrec wbsc --drop_admin Y
```

Additional Reference

For additional information about Oracle, refer to the official Oracle user documentation at:

<http://www.oracle.com/technetwork/database/enterprise-edition/documentation/index.html>

Using GQM Virtual Appliances

This chapter describes the use of the Genesys GQM Virtual Appliances.

This chapter contains the following sections:

[Virtual Appliance Overview](#)

[Installing VMWare Tools on a Virtual Server](#)

[Importing the Virtual Appliance](#)

[Reading and Accepting the EULA](#)

[Restarting CallREC](#)

[Restarting the Server](#)

[Configuring the Network](#)

[Configuring the Time Zone](#)

[Logging In](#)

[Mounting Storage for Calls for the VM Appliance](#)

[Converting a Virtual Appliance to VMware Workstation or VMware Server](#)

[Using More than One CPU in the VA](#)

Virtual Appliance Overview

The Genesys GQM Virtual Appliance includes the CentOS 6.2 operating system and a fully-featured version of ZOOM GQM 8.1.492 without a license file. To record calls, contact your local Genesys and request a trial license, a sales representative will contact you as soon as possible.

The Genesys GQM Virtual Appliance is packed in an uncompressed zip file, containing 2600MB. See below for prerequisites.

The Genesys GQM Virtual Appliance is built to run on the ESX 4 / ESXi 4/5 platform. It can be converted to the VMware Workstation and VMware Server format (see Appendix B for conversion instructions).

Genesys Labs, Inc. cannot guarantee any performance in the VMware environment.

Log in data required:

OS logins:

login1: root

pass1: zoomcallrec

login2: admin

pass2: zoomcallrec

Web GUI:

login: admin

pass: admin

Prerequisites

The following prerequisites are required for the Virtual Appliance:

- VMware ESX 4 / ESXi 4/5 (or VMware Workstation / VMware server after converting the Virtual Appliance to a compatible format - see Appendix B)
- A datastore with 25600+ MB of free space (Should you require more storage for calls, please refer to Appendix A)
- Two NICs (Network Interface Cards).
One virtual network for network management.
One virtual network for the SPAN port - (Select Promiscuous Accept mode in Virtual Appliance Port Group properties).
- At least 4 cores CPU (or 2 CPU with 2 Cores) with sufficient resources for the Virtual Appliance.

Default configuration

The Genesys GQM Virtual Appliance is configured for Skinny call recording by default.

To change this go to the command line log on as root and enter the command:
`/opt/callrec/bin/callrec-setup.`

To enter the Call Recording set up process.

The default IP address is: 192.168.1.100 (you can change the address in the Virtual Appliance menu, in console 1).

Installing VMWare Tools on a Virtual Server

The VMware tools package enhances the graphics and mouse performance of the virtual machine.

This chapter contains the following sections:

Starting the Installation Process

In the vSphere Client:

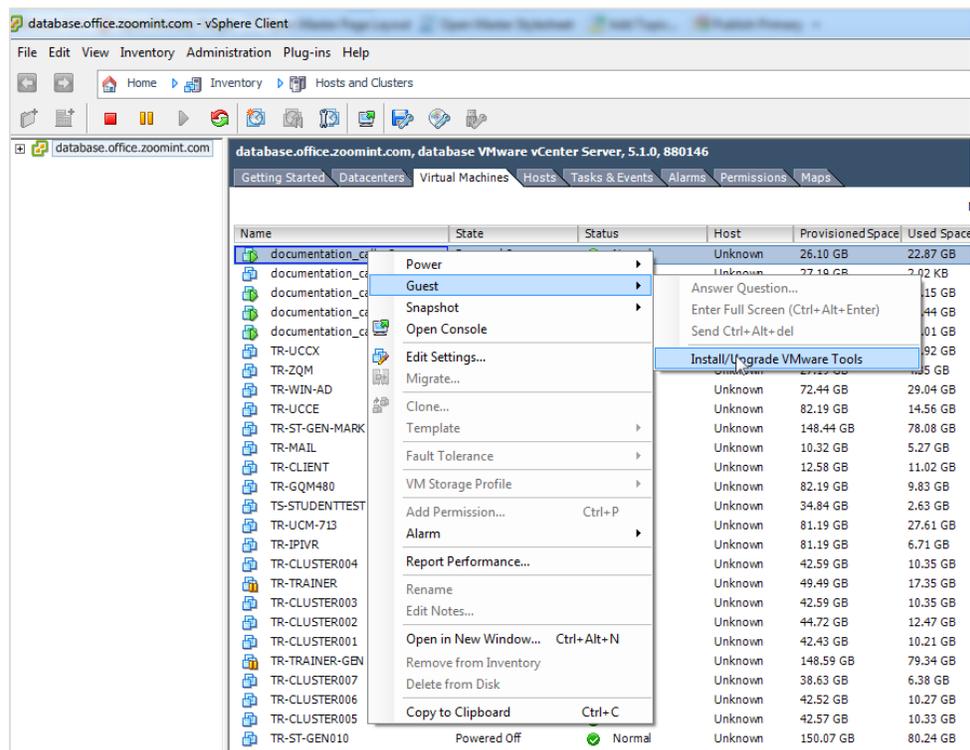


Figure 245: Selecting Install/Upgrade VMware Tools

1. Right click the virtual server from the list of servers.
2. Select **Guest** from the menu.
3. Select **Install/Upgrade VMWare Tools**.

The **Install VMware Tools** dialog displays.

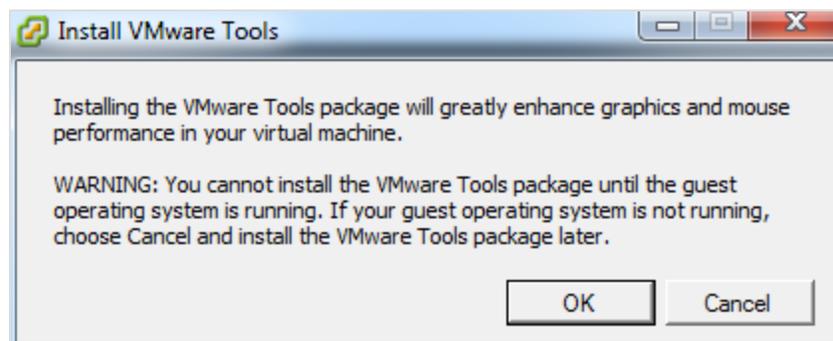


Figure 246: Install VMware Tools Warning

4. Click **OK**.

Checking that the CD/DVD is Connected:

1. Right click the virtual server from the list of servers.
2. Select **Edit Settings** from the menu .

The VMware Tools dialog displays.

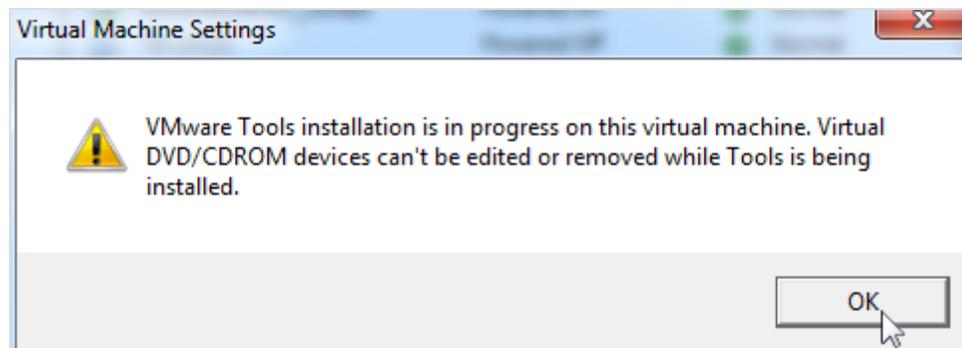


Figure 247: Virtual Machine Settings Warning

3. Click **OK** to remove the dialog.

The Virtual Machine Properties page appears.

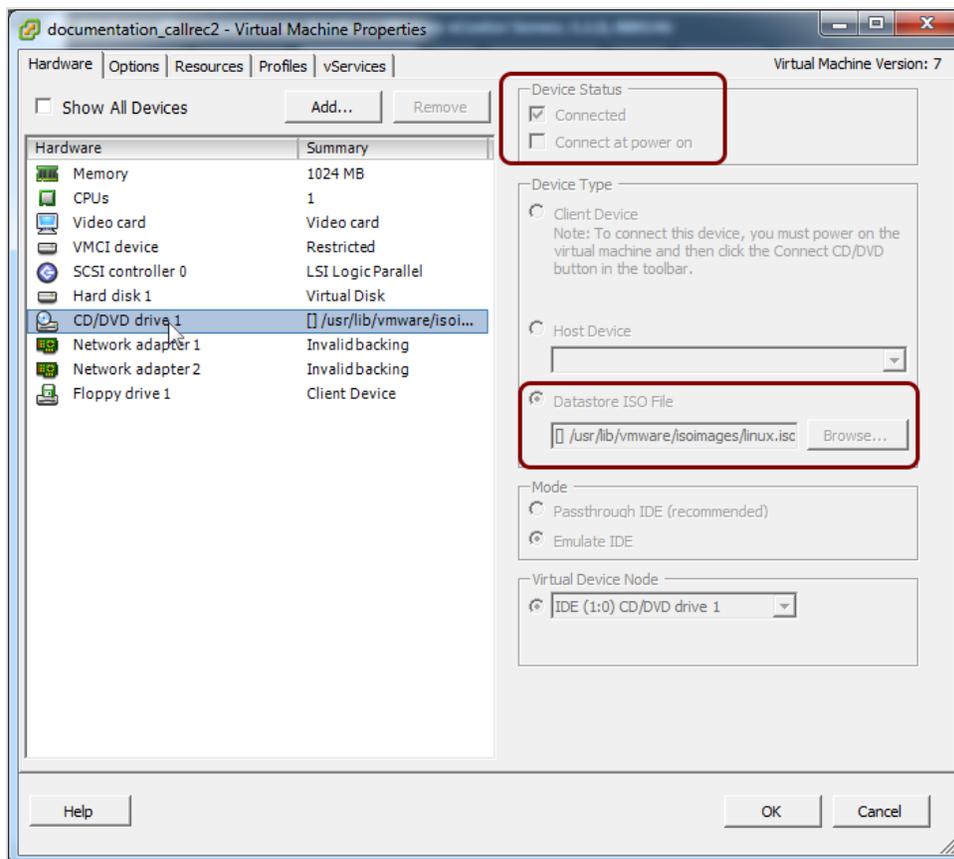


Figure 248: Virtual Machine Properties

4. Click **CD/DVD drive 1**.
5. Ensure that the **Connected** checkbox is selected, the **File Datastore ISO** radio button is selected, and that the path is shown as: []
/usr/lib/vmware/isoimages/linux.iso.
If the checkbox and radio button are not selected, then reset the machine, and start again.
6. If the checkbox and radio button are selected then click **OK**.

Installing the VMware tools.

Use any SSH client, for example, PuTTY.

1. Select the virtual server from the list of servers.
2. Login as root.
3. Enter the following commands:

```
mkdir /mnt/cdrom
mount -o loop /dev/cdrom /mnt/cdrom
cd /tmp
```

4. To get the correct version of `VMwareTools-X.X.X-XXXXX.tar.gz` in the next command line, type :
`tar xzpf /mnt/cdrom/VM` and press the **Tab** key to auto complete the filename:

```
tar xzpf /mnt/cdrom/VMwareTools-X.X.X-XXXXX.tar.gz
umount /dev/cdrom
cd vmware-tools-distrib/
./vmware-install.pl
```

5. Press **Enter** after the last command (`./vmware-install.pl`).
6. Press **Enter** for every prompt to install the tools in their default locations.
7. Follow the instructions at the end of the installation to update the drivers.
8. The SSH client displays the following message at the end.

```
Enjoy,
--the VMware team
```

9. Close the SSH client.

Important:

Always check what VNIC adapter type is configured on the VM before loading the VNIC driver! Note that E 1000 may not work properly under heavy load. Use of *Flexible* or *VMXNET VNIC* adapter types is recommended. There are reported bugs in the VMXNET adapter, check their ESXi version and apply any updates, if available.

Importing the Virtual Appliance

Unpack the .zip file downloaded from our web site. This file contains 2 files:

- ovf
- vmdk

Both must be unpacked to the same folder.

1. In the **vSphere Client**, select the appropriate resource pool (in Hosts and Clusters).

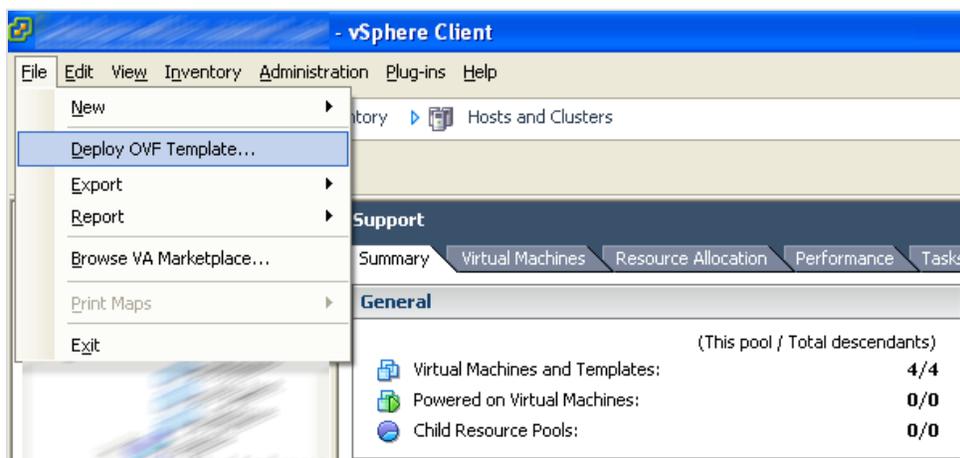


Figure 249: Deploy OVF Client

2. Select **File > Deploy OVF Template...** to open the Deploy OVF Template Wizard.

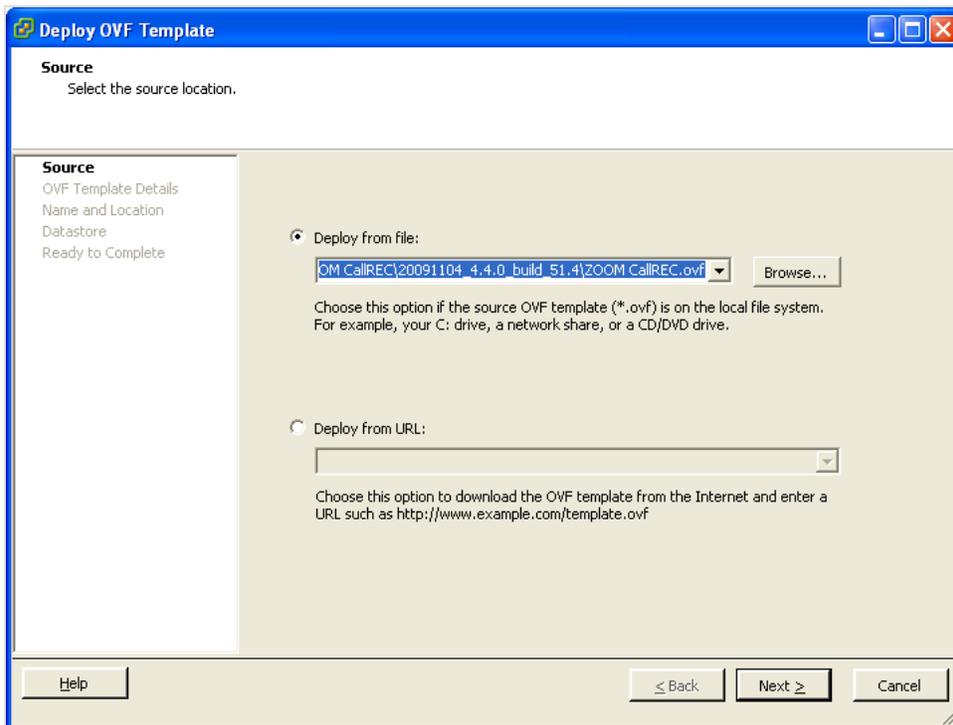


Figure 250: Deploy OVF Template

3. Select the unpacked ovf file and click **Next**.

The **OVF Template Details** screen information about the virtual appliance.

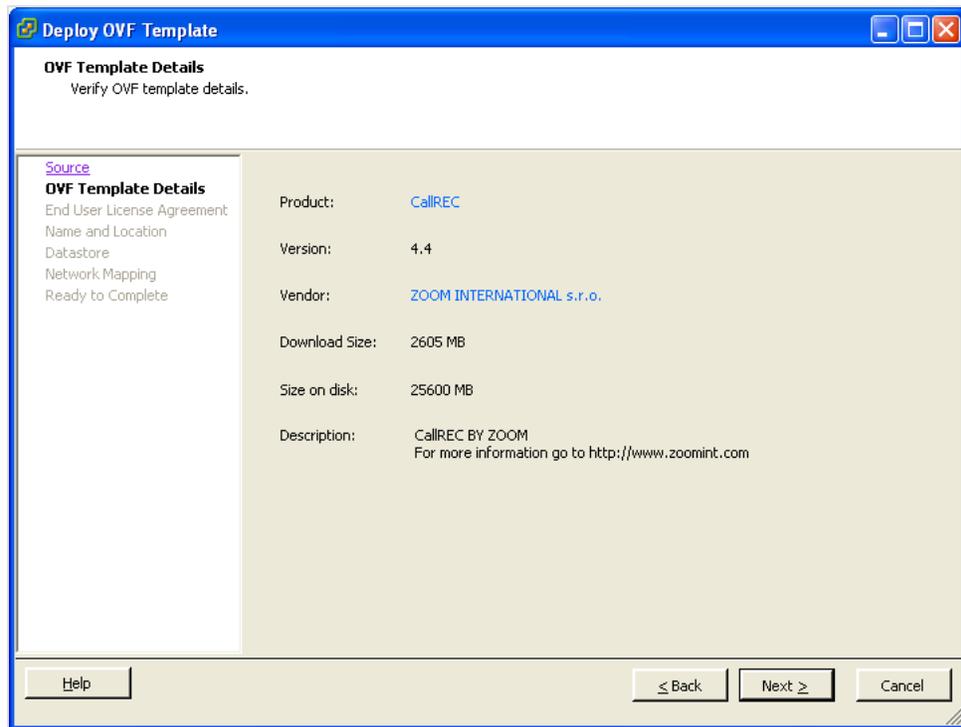


Figure 251: View Information About the Virtual Appliance

4. Select **Next** to continue.

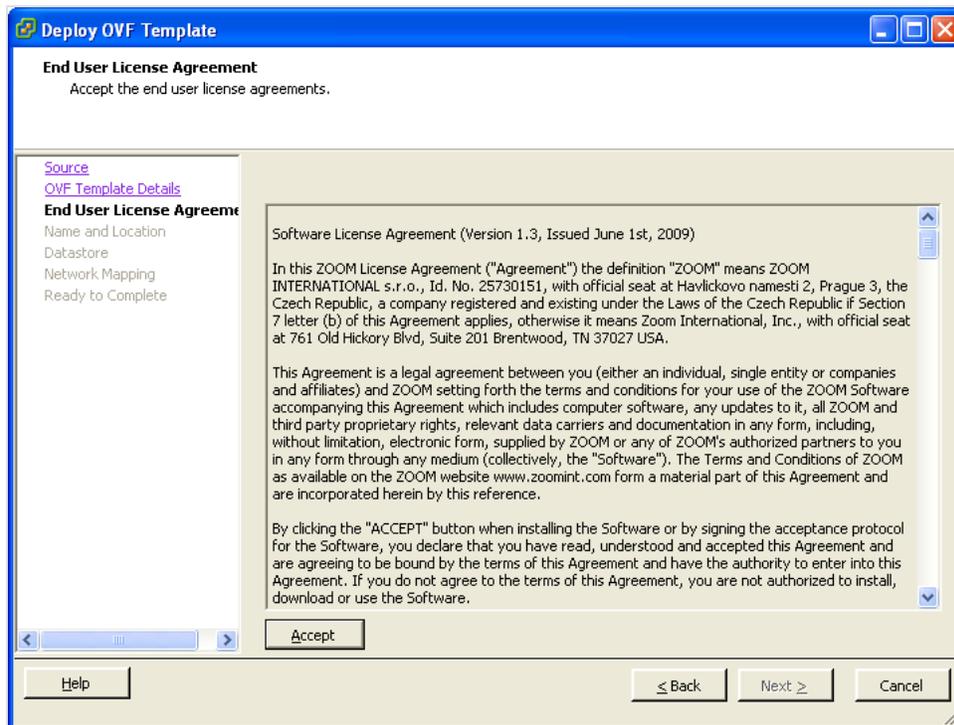


Figure 252: Deploy OVF Template

5. Read and Accept the End User License Agreement (EULA). Select **Next** to continue.

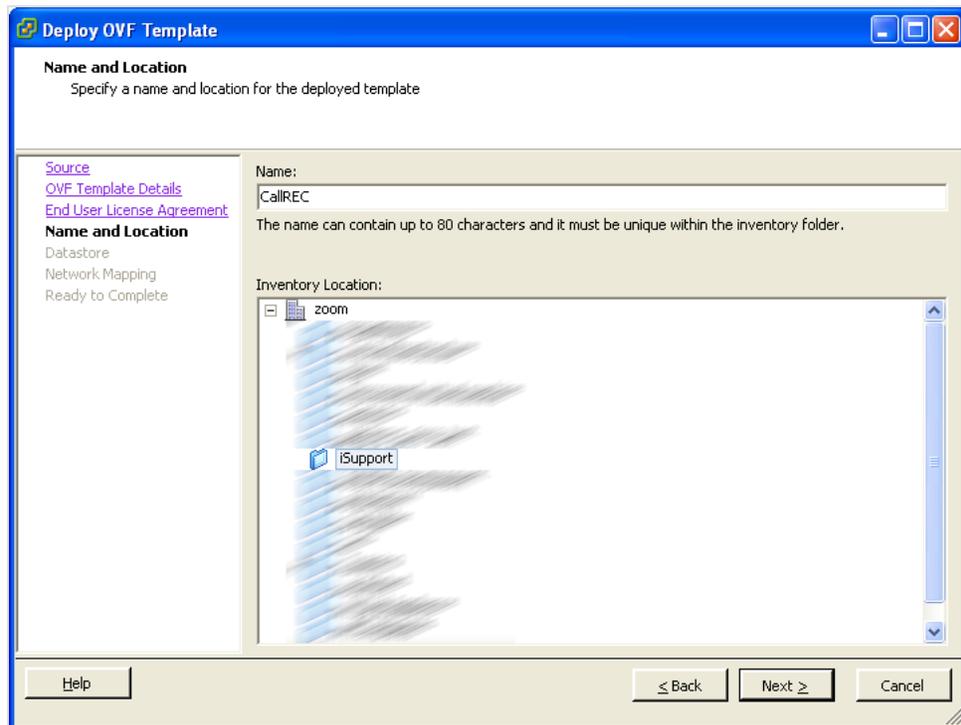


Figure 253: Select an Appropriate Folder

6. Select the inventory **Name and Location** folder and enter a name for the new virtual machine. Click **Next**.

If the resource pool in step 1 was not selected, define it here.

7. Select the appropriate folder for the new virtual machine.

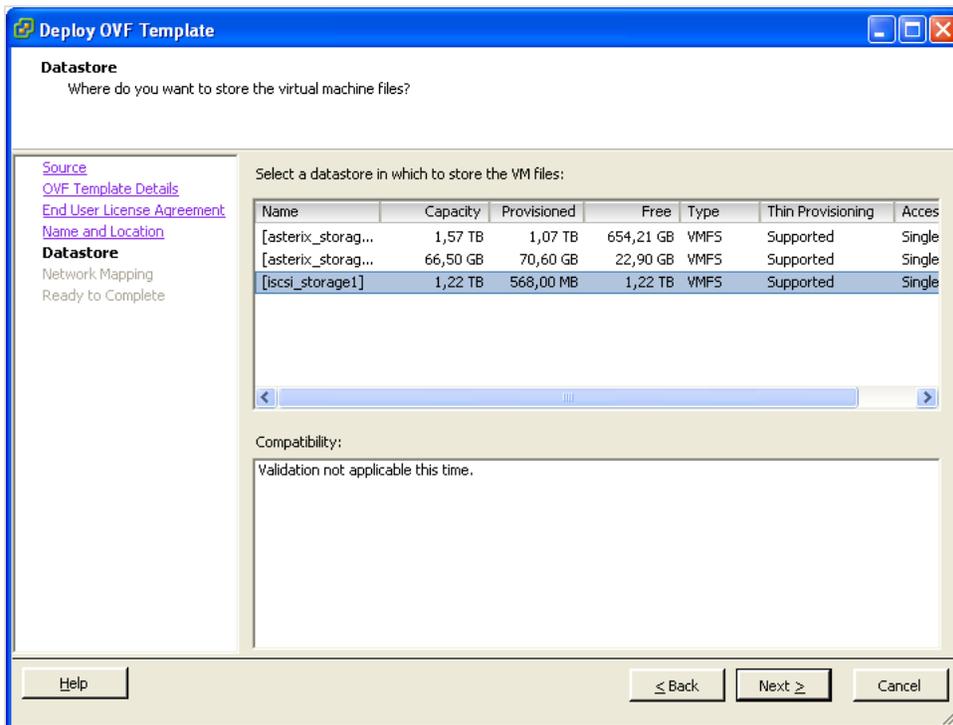


Figure 254: Select an Appropriate Datastore

8. Select the appropriate **Datastore**.

Use local SAS 15k rpm hard drives or iSCSI / Fibre Channel remote storage with 15k rpm hard drives.

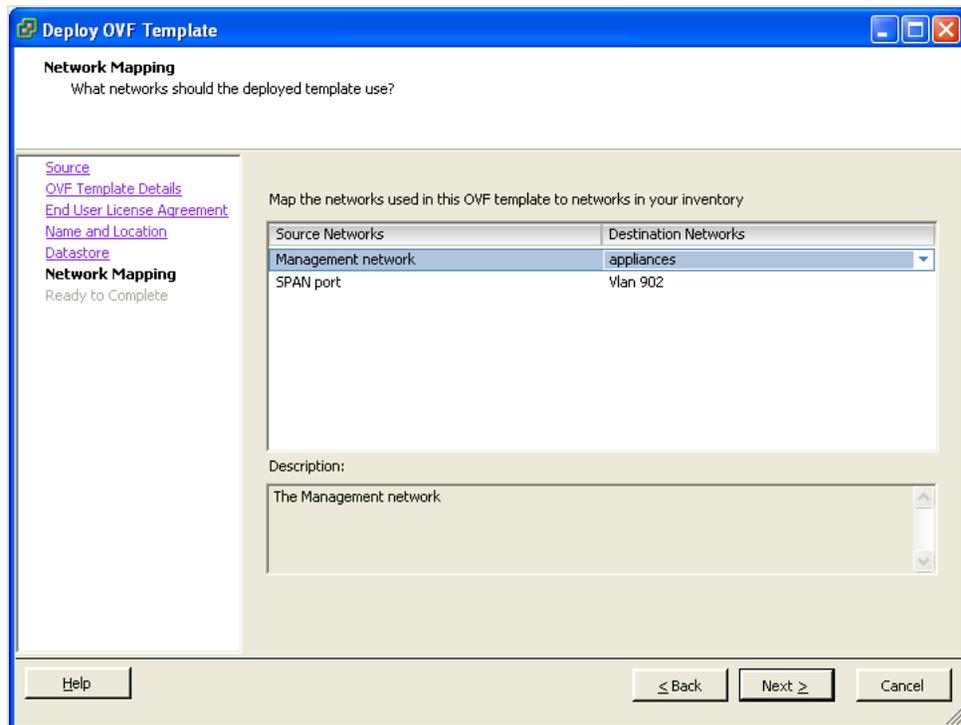


Figure 255: Network Mapping

9. Select the appropriate network for Management and the SPAN port. (Refer to the prerequisites in section 1.1).

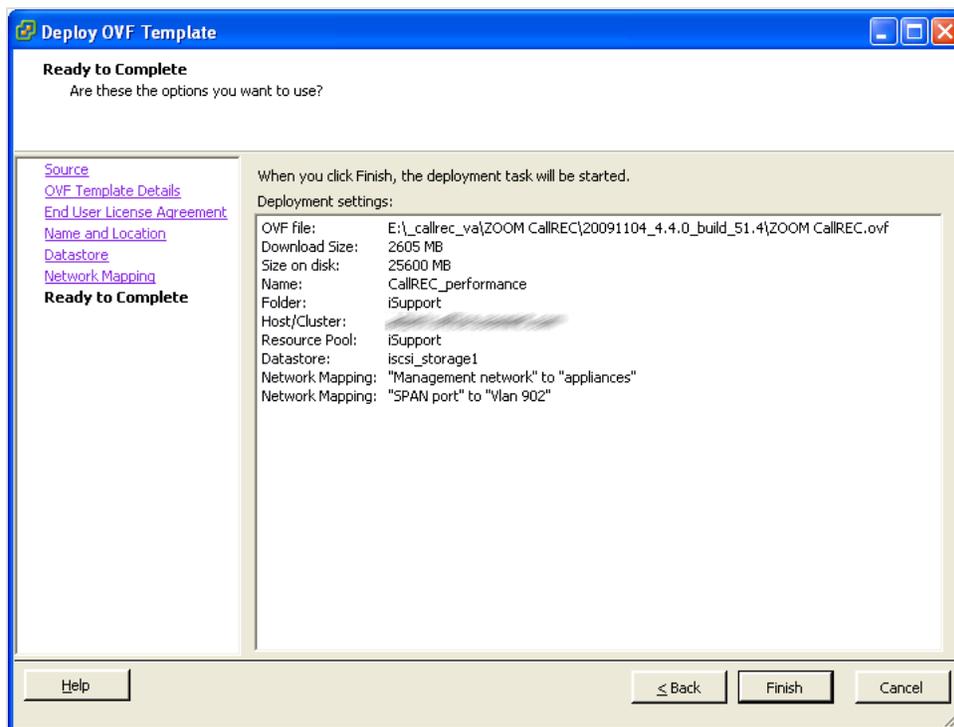


Figure 256: Ready to Complete

10. Review the configured settings and select **Finish** to start the deployment process.

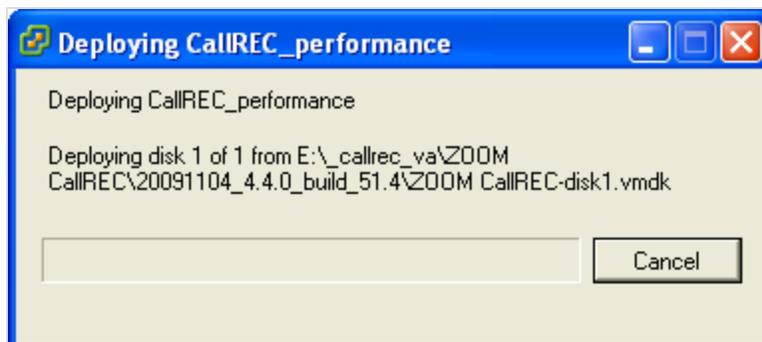


Figure 257: Deploying Call Recording Performance

View the progress of the deployment.

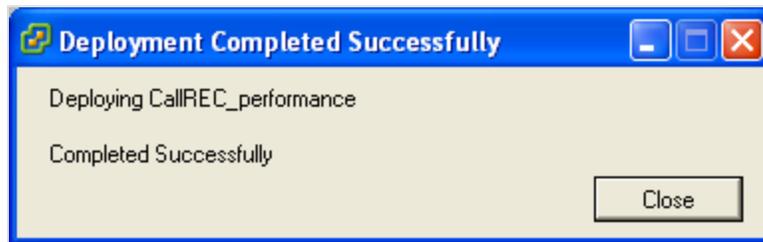


Figure 258: Deploying Completed Successfully

11. Select **Close** to complete the deployment process.

Reading and Accepting the EULA

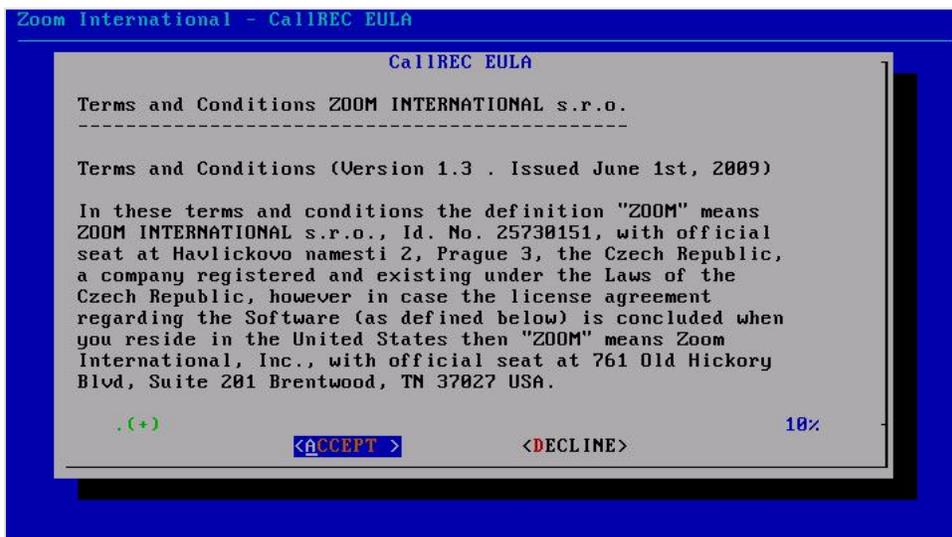


Figure 259: Call Recording EULA

1. Read and Accept the QM Suite EULA.

Use the arrow keys or Page Up or Page Down keys to view the agreement.

If **DECLINE** is selected the virtual machine stops.

Restarting CallREC

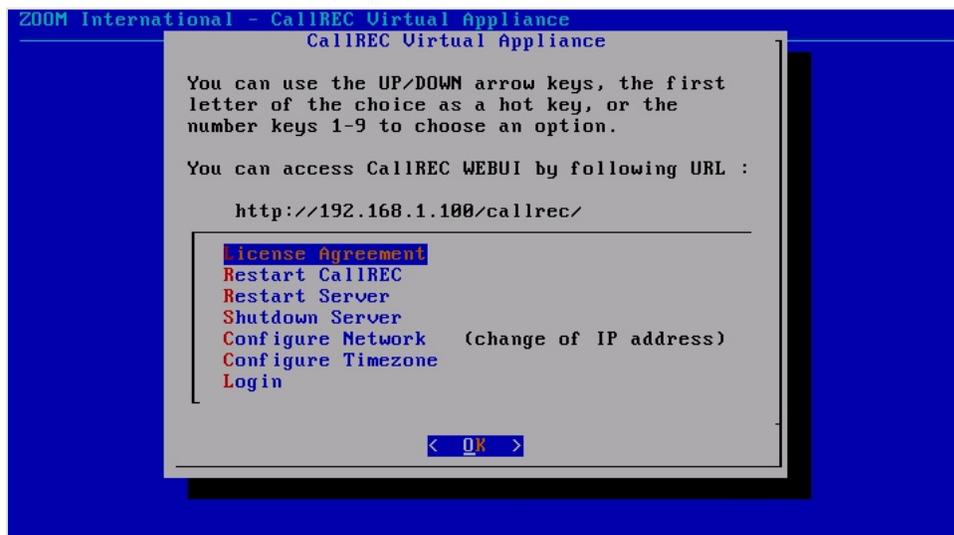


Figure 260: Call Recording Virtual Appliance Menu

1. To restart Call Recording services use the second item in the menu.

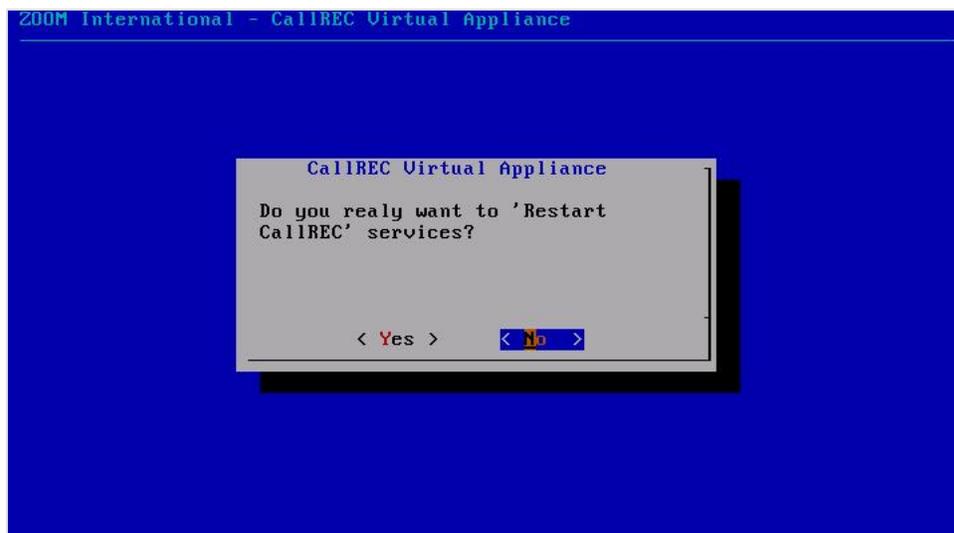


Figure 261: Call Recording Virtual Appliance Menu

2. Select **Yes** to confirm the restarting of Call Recording services.

```
Restarting CallREC services ...
-----
Stopping CallREC WEB: .... [ OK ]
Stopping CallREC Tools: [ OK ]
Stopping CallREC CORE: ... [ OK ]
Stopping CallREC SLR: . [ OK ]
Stopping CallREC RS eth1: . [ OK ]
Stopping CallREC DECODER - DecoderMasterCommunicator: .. [ OK ]
Stopping CallREC JTAPI: ... [ OK ]
Stopping CallREC CONFIGMANAGER: .. [ OK ]
Stopping CallREC NAMING: . [ OK ]
Stopping CallREC RMI: ..... [ OK ]

Starting CallREC RMI: . [ OK ]
Starting CallREC NAMING: . [ OK ]
Starting CallREC CONFIGMANAGER: _
```

Figure 262: Example of Services Restarting

The Services Restart and display **OK** if successful.

Restarting the Server

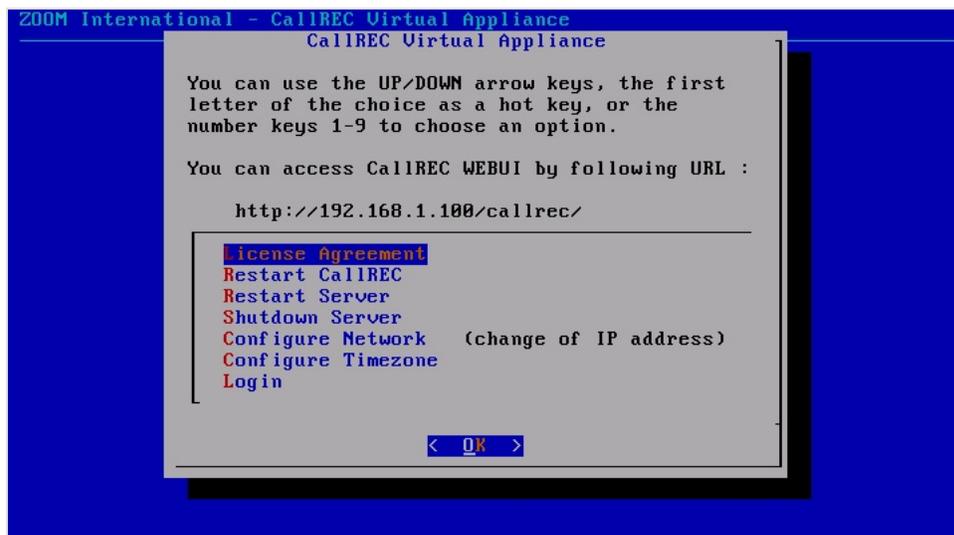


Figure 263: Call Recording Virtual Appliance Menu

1. To restart the GQM server use the third item in the menu.
2. Select **Yes** to confirm the services restart.

Shutting down the Server



Figure 264: Configuring the Network

1. To shutdown the QM Suite server use the fourth item in the menu. After this selection a confirmation window displays.
2. Select **Yes** to confirm the shutdown of the QM Suite server.

Configuring the Network

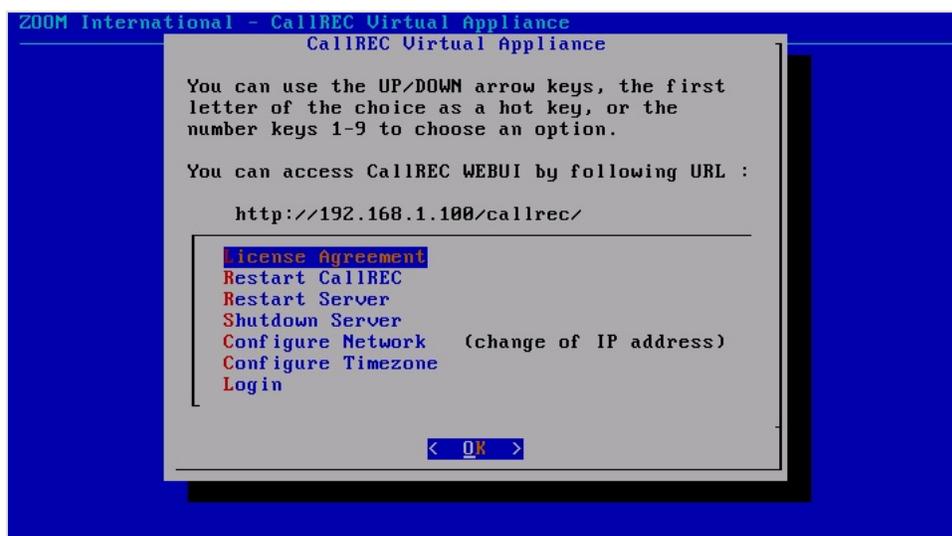


Figure 265: Configuring the Network

1. Select **Configure Network** from the menu.
2. Enter the configuration details.

These details automatically update the QM Suite settings.

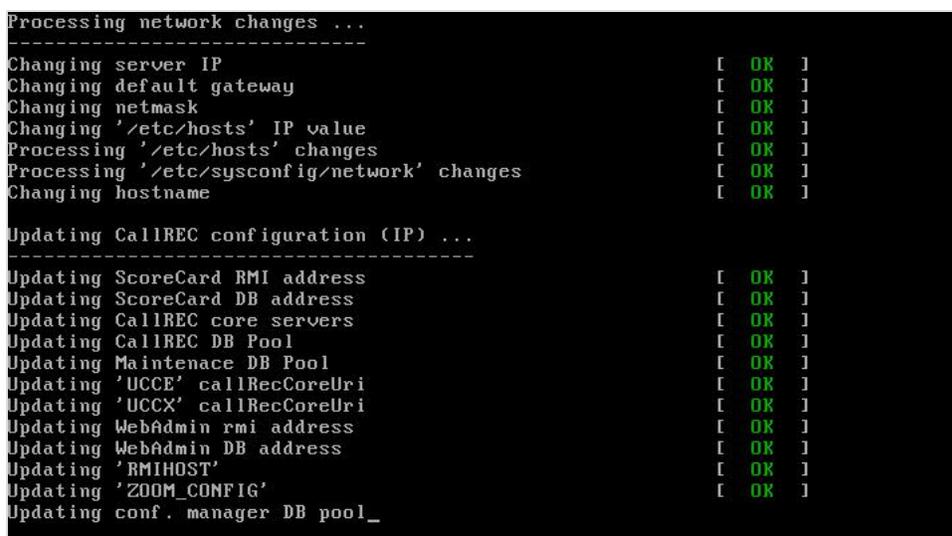


Figure 266: Processing and Updating

The network changes process and displays **OK** if successful.

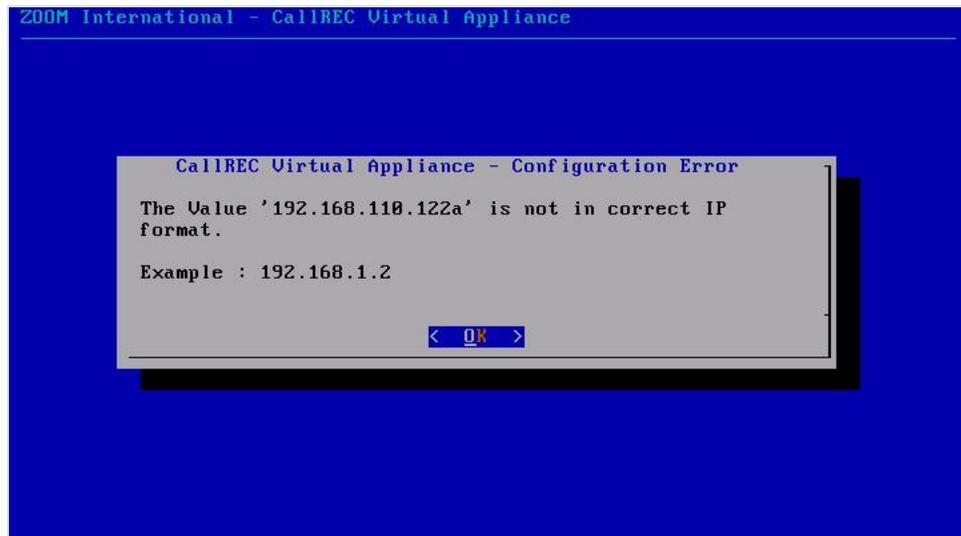


Figure 267: Configuration Error

Entering incorrect information results in an error message. Where incorrect values for IP addresses or hostname are inserted, the form reloads with the original data.

Configuring the Time Zone

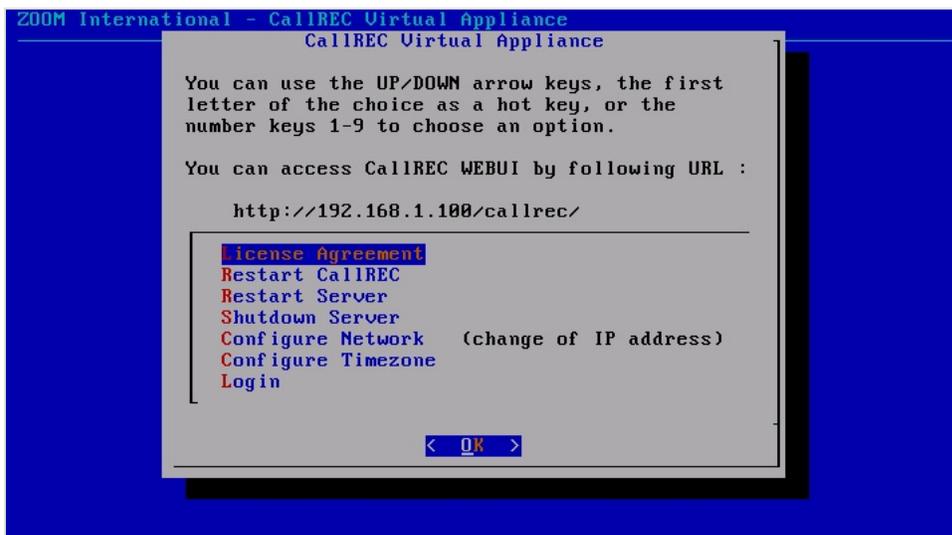


Figure 268: Configuring the Network

Select **Configure Timezone** to select a preferred Time Zone.

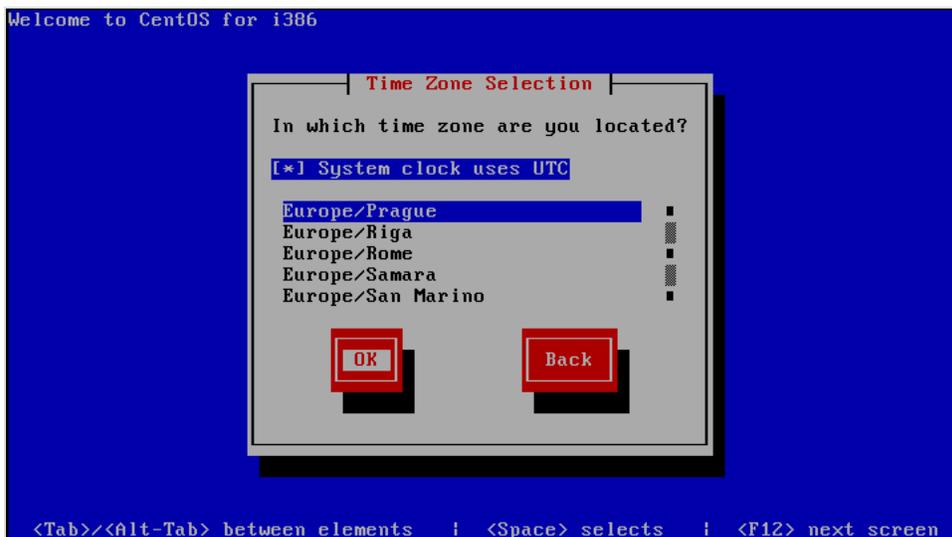


Figure 269: Configuring the Time Zone

Select the Time Zone from the list.

Mounting Storage for Calls for the VM Appliance

This part of the document describes the configuration of new storage for QM Suite Virtual Appliance.

Mounting and formatting a partition in QM Suite Virtual Appliance

To use a partition greater than 2TB, follow the article:

<http://www.cyberciti.biz/tips/fdisk-unable-to-create-partition-greater-2tb.html>

The following provides a brief overview of mounting and formatting a new disk to QM Suite Virtual Appliance.

1. Login to QM Suite as root (default password is zoomcallrec)

```
[root@callrec ~]# fdisk -l
Disk /dev/sda: 26.8 GB, 26843545600 bytes
255 heads, 63 sectors/track, 3263 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1  *           1           13     104391   83  Linux
/dev/sda2                14         3263     26105625   8e  Linux LVM

Disk /dev/sdb: 107.3 GB, 107374182400 bytes
255 heads, 63 sectors/track, 13054 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

Disk /dev/sdb doesn't contain a valid partition table
```

Figure 271: Attaching the fdisk

2. Enter the following command:

```
fdisk -l
```

Note that /dev/sdb disk is attached and no partition is created.

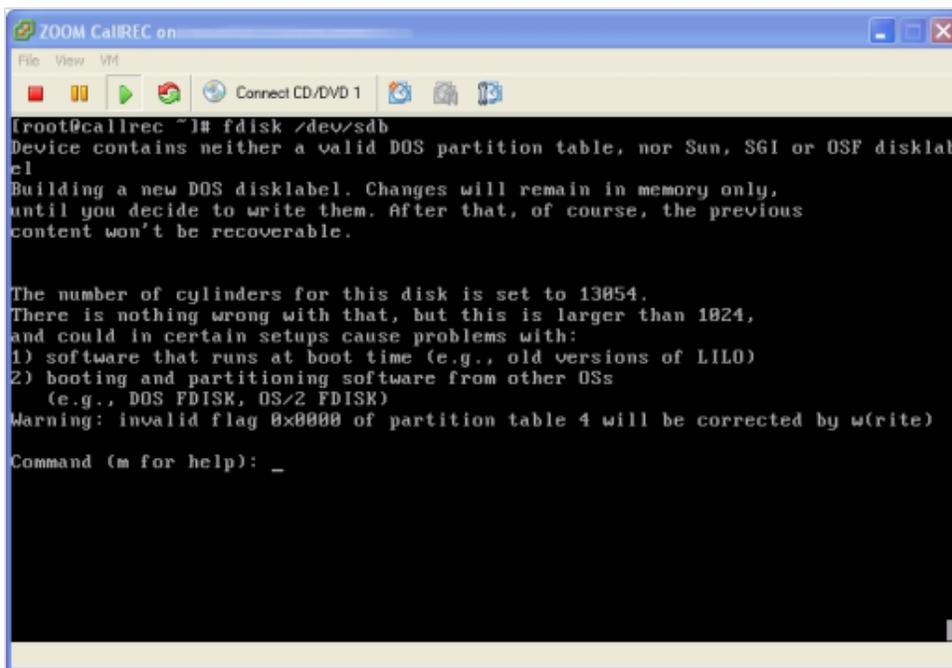
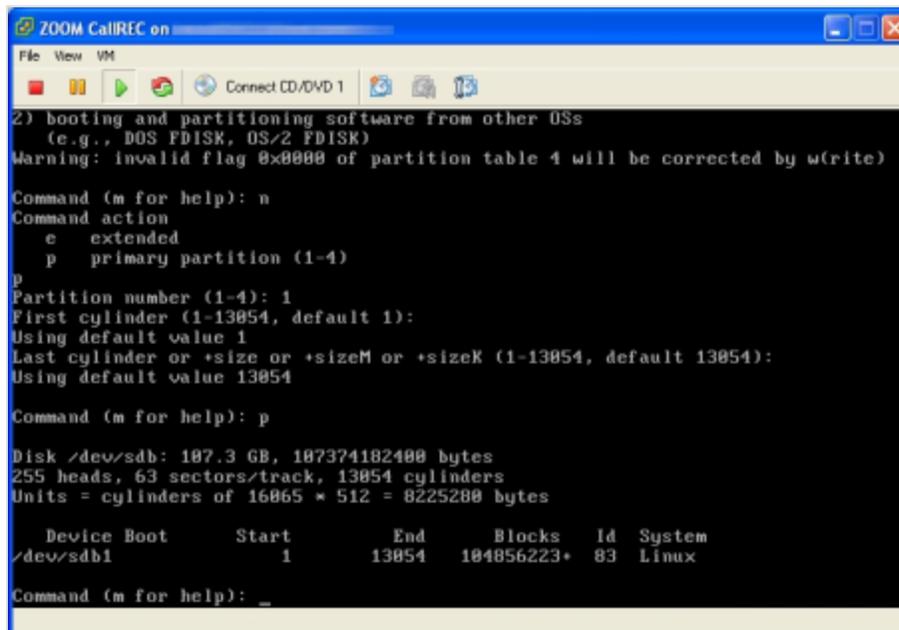


Figure 272: Creating Partitions

1. Enter the following command:

```
fdisk /dev/sdb
```

The fdisk software is executed to create new disk partitions:



```
ZOOM CallREC on
File View VM
Connect CD/DVD 1
2) booting and partitioning software from other USs
(e.g., DOS FDISK, OS/2 FDISK)
Warning: invalid flag 0x0000 of partition table 1 will be corrected by w(rite)

Command (m for help): n
Command action
  e   extended
  p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-13854, default 1):
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-13854, default 13854):
Using default value 13854

Command (m for help): p

Disk /dev/sdb: 107.3 GB, 107374182400 bytes
255 heads, 63 sectors/track, 13854 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

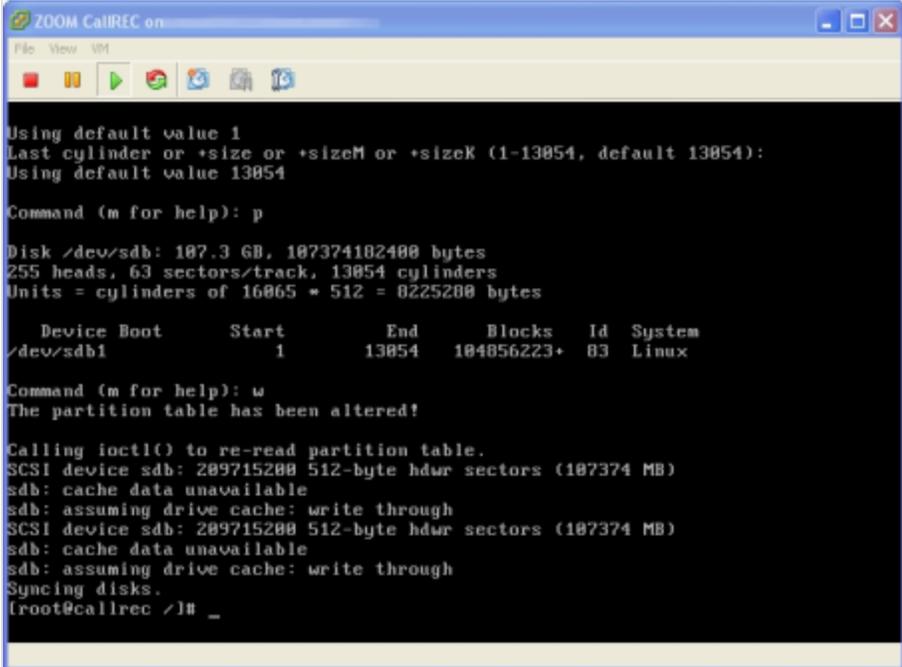
   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1            1        13854    104856223+  83  Linux

Command (m for help): _
```

Figure 273: Creating a New Partition

Create a new partition:

1. Type **n** and then **Enter** to start the new partition wizard.
2. Type **p** and then **Enter** to create a primary partition.
3. Select **Enter** to accept the default value and start the partition from the beginning of the disk.
4. Select **Enter** to accept the default and end the partition at the end of the disk.
5. Type **p** to check that the partition has been created.



```
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-13854, default 13854):
Using default value 13854

Command (m for help): p

Disk /dev/sdb: 187.3 GB, 187374182400 bytes
255 heads, 63 sectors/track, 13854 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
 /dev/sdb1            1        13854    104856223+  83  Linux

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
SCSI device sdb: 289715200 512-byte hdwr sectors (187374 MB)
sdb: cache data unavailable
sdb: assuming drive cache: write through
SCSI device sdb: 289715200 512-byte hdwr sectors (187374 MB)
sdb: cache data unavailable
sdb: assuming drive cache: write through
Syncing disks.
[root@callrec /]# _
```

Figure 274: Write the Changes to the Disk

Type **w** and **Enter** to write the changes to the disk.

```

ZOOM CallREC on
File View VM
Syncing disks.
[root@callrec /]# mkfs.ext3 /dev/sdb1
mke2fs 1.35 (28-Feb-2004)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
13187200 inodes, 26214055 blocks
1318702 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=29360120
000 block groups
32768 blocks per group, 32768 fragments per group
16384 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000, 7962624, 11239424, 20480000, 23887872

Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 39 mounts or
100 days, whichever comes first. Use tune2fs -c or -i to override.
[root@callrec /]# _

```

Figure 275: Format the New Partition

1. Enter the following command:

```
mkfs.ext3 /dev/sdb1
```

```

# This file is edited by fstab-sync - see 'man fstab-sync' for details
/dev/volgrp01/rootlv / ext3 defaults 1 1
LABEL=/boot /boot ext3 defaults 1 2
none /dev/pts devpts gid=5,mode=620 0 0
none /dev/shm tmpfs defaults 0 0
/dev/volgrp01/home1v /home ext3 defaults 1 2
/dev/volgrp01/opt1v /opt ext3 defaults 1 2
none /proc proc defaults 0 0
none /sys sysfs defaults 0 0
/dev/volgrp01/tmplv /tmp ext3 defaults 1 2
/dev/volgrp01/swaplv swap swap defaults 0 0
/dev/fd0 /media/floppy auto pamconsole,exec,noauto,m
anged 0 0

/dev/sdb1 /opt/callrec/data/calls ext3 defaults 1 2

```

Figure 276: Edited by fstab

Mount the partition to the file system:

1. Edit the file `/etc/fstab`
2. Enter the following at the end of the file. Press enter to create a new line ending

```
/dev/sdb1 /opt/callrec/data/calls ext3 defaults 1 2
```

Converting a Virtual Appliance to VMware Workstation or VMware Server

To use this virtual appliance in a VMware Workstation or VMware Server, convert the virtual hard drive file to a format compatible with these products.

For this purpose VMware creates the application: OVF Tool (<http://www.vmware.com/resources/techresources/1013>).

Converting the virtual appliance to VMware Workstation / Server format:

1. Download the OVF Tool from VMware (need to be registered).
2. Unpack ZOOM CallREC Virtual Appliance to X:\Callrec (where X means drive in the computer with appropriate space, at least 10GB).
3. Using Windows Explorer, navigate to X:\Callrec and create a sub folder for example X:\Callrec\converted.
4. Select Start > Run...

In Windows Vista / Windows 7 select the search field, type `_cmd_`, right click and select 'Run as administrator')

5. Navigate to X:\Callrec ('cd X:\Callrec').
6. Run the command (' ' ' is part of the command and must be entered):
 - For a 32-bit system: `"c:\Program Files\VMware\VMware OVF Tool\ovftool.exe" -tt=vmx "ZOOM CallREC.ovf" .\converted\`

OR:

- For a 64-bit system: `"c:\Program Files (x86)\VMware\VMware OVF Tool\ovftool.exe" -tt=vmx "ZOOM CallREC.ovf" .\converted\`

7. Use any key move through the EULA, answer yes and press Enter

Now import the converted virtual appliance to VMware workstation / server.

Using More than One CPU in the VA

For more than 1 CPU in the Virtual Appliance please follow these steps:

1. Stop Call Recording in the command line:

```
service callrec stop
```

2. Shutdown the virtual machine:

```
shutdown -h now
```

3. Select the virtual machine in vSphere Client, right click to Edit Settings.

4. Select **CPUs** and change the number of CPUs to 2 or more.

5. Select **OK** and start the virtual machine.

6. After the virtual machine has started log in to console and run these commands:

```
chkconfig irqbalance on  
/etc/init.d/irqbalance start
```


Command Line Scripts

Many basic maintenance tasks in Call Recording can be executed directly from the command line. For each of the following tasks, log in as an Administrator with Root privileges.

This chapter contains the following sections:

[Starting and stopping Call Recording](#)

[Starting Call Recording](#)

[Stopping Call Recording](#)

[Restarting Call Recording](#)

[Automatic running](#)

[Reloading the Configuration manager](#)

[Checking the Status of Call Recording](#)

[Restarting and Shutting Down the Server](#)

[Restarting the Decoder](#)

[Restarting Call Recording Core](#)

[Restarting the Call Recording System](#)

[Restarting other Call Recording Components](#)

[Restarting Clustered Servers](#)

[Restarting Redundant Servers](#)

[Restoring the Default Configuration](#)

[Using Symlinks to the Call Recording PCAP Storage Directory](#)

[Important Note on Synchronization](#)

[Mounting Windows File Shares](#)

[Advanced Configuration Parameters](#)

[Limit on the Maximum Number of Threads](#)

Starting and stopping Call Recording

Use the service commands for starting, stopping and restarting Call Recording services when logged on as root. The service command functions as a shortcut to the `/etc/init.d` directory.

```
[root@callrec ~]# service callrec
```

Use the absolute path for these commands as this does not require a change of directory and avoids issues with directory permissions. Usage:
`/etc/init.d/callrec {start|stop|restart|status}`

Starting Call Recording

Use the following command to start the Call Recording application:

```
/etc/init.d/callrec start
```

Or:

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

```
service callrec start
```

The system displays confirmation of all services that start.

```
Starting CallREC RMI: . [ OK ]
Starting CallREC NAMING: . [ OK ]
Starting CallREC CONFIGMANAGER: .. [ OK ]
Starting CallREC JTAPI: . [ OK ]
Starting CallREC RS eth1: [ OK ]
Starting CallREC DECODER - DecoderMasterCommunicator: . [ OK ]
Starting CallREC ScreenREC: . [ OK ]
Starting CallREC CORE: .... [ OK ]
Starting CallREC IPCC: .. [ OK ]
Loading CallREC Tools configuration views: [ OK ]
Starting CallREC WEB: ..... [ OK ]
```

Stopping Call Recording

Use the following command to stop the Call Recording application:

```
/etc/init.d/callrec stop
```

Or:

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

```
service callrec stop
```

The system displays confirmation of all services that stop.

```
Stopping CallREC WEB: ..... [ OK ]
Stopping CallREC IPCC: .. [ OK ]
Stopping CallREC CORE: .... [ OK ]
Stopping CallREC ScreenREC: ..... [ OK ]
Stopping CallREC RS eth1: ... [ OK ]
Stopping CallREC DECODER - DecoderMasterCommunicator: .. [ OK ]
Stopping CallREC JTAPI: .. [ OK ]
Stopping CallREC CONFIGMANAGER: .. [ OK ]
Stopping CallREC NAMING: .. [ OK ]
Stopping CallREC RMI: ..... [ OK ]
```

Restarting Call Recording

Use the following command to restart the Call Recording application:

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

Or:

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

```
service callrec restart
```

The system displays confirmation of all services that restart.

```
Stopping CallREC WEB: ..... [ OK ]
Stopping CallREC IPCC: .. [ OK ]
Stopping CallREC CORE: .... [ OK ]
Stopping CallREC ScreenREC: ..... [ OK ]
Stopping CallREC RS eth1: ... [ OK ]
Stopping CallREC DECODER - DecoderMasterCommunicator: .. [ OK ]
Stopping CallREC JTAPI: .. [ OK ]
Stopping CallREC CONFIGMANAGER: .. [ OK ]
Stopping CallREC NAMING: .. [ OK ]
Stopping CallREC RMI: ..... [ OK ]
Starting CallREC RMI: . [ OK ]
Starting CallREC NAMING: . [ OK ]
Starting CallREC CONFIGMANAGER: .. [ OK ]
Starting CallREC JTAPI: . [ OK ]
Starting CallREC RS eth1: [ OK ]
Starting CallREC DECODER - DecoderMasterCommunicator: . [ OK ]
Starting CallREC ScreenREC: . [ OK ]
Starting CallREC CORE: .... [ OK ]
Starting CallREC IPCC: .. [ OK ]
Loading CallREC Tools configuration views: [ OK ]
Starting CallREC WEB: ..... [ OK ]
```

Important:

During restarting or stopping Call Recording may list processes or modules which have stopped responding. These processes are then terminated, and this does not influence restarting the system.

Automatic running

To automatically run Call Recording on startup, add Call Recording to server run levels during setup. This is the default during installation.

To add Call Recording to the startup sequence of the server, run the command in root:

```
/sbin/chkconfig --add callrec
```

Enable automatic startup of Call Recording with the following command:

```
/sbin/chkconfig callrec on
```

Disable automatic startup of Call Recording with the following command:

```
/sbin/chkconfig callrec off
```

Reloading the Configuration manager

If Call Recording is restarted while recording calls, the recordings of the calls being recorded at the time are lost. However Call Recording uses an independent configuration server to store configuration information for all the components of the system. This means the entire Call Recording system does not need to be restarted to change the configuration of individual components that do not affect the recording of calls, such as the Tools service and Synchro service.

By reloading these configuration parameters, configuration can be reset in these components without restarting the system.

Reload the configuration with the following command:

```
/opt/callrec/bin/rc.callrec_configmanager reload
```

Reloading the Configuration manager causes the following:

- All configuration files are reloaded as changed
- Pending configuration operations are consolidated
- Registered observers remain active (other services do not need to reconnect)

Reloading the configuration manager is ineffective if the main system configuration changes, specifically decoder or encoder settings. This means that changing the sniffing method or encoding type needs a complete restart of the Call Recording system.

Checking the Status of Call Recording

Use the Application Communicator to check the status of Call Recording. The Application Communicator reports all processes and modules running and their current state.

The Application Communicator is invoked from command line. It has the following parameters:

- **port [port]** - rmi port (default: 30400)
- **host [host]** - rmi host (default: localhost)
- **names** - returns all names supported Application Communicator interface
- **name [name]** - rmi bind name (default: remoteCallRec)
- **bindName [bindName]** - rmi bind name - all path (default: //localhost:30400/remoteCallRec)
- **help** – shows help for all parameters
- **stateNames** - returns module names to provide state information
- **state [{name}]all** - state information about a module or all modules
- **verbosity [1|2|3|4|5]** - set state verbosity (all information: 5, default: 2)
- **stateOption [status|failed]** - set state option
status - only status row (OK or FAILED)
failed - only FAILED row
- **versionNames** - return module names provide version information
- **version [{name}]all** - version info about application (one module, all modules)
- **modifyNames** - return module names you can modify properties
- **modifyHelp [{name}]all** - return help about modifiable properties (one module, all modules)
- **modifyInt [module,property,value]** - modify int value (property of module)
- **modifyString [module,property,value]** - modify String value (property of module)

To check the status of the entire Call Recording system while Call Recording is running, use the shortcut command:

```
/etc/init.d/callrec status
```

Below is a typical extract from the command output:

```
[root@callrec ~]# service callrec status
Application communicator trunk-SNAPSHOT, build: 100523_0107 (c) ZOOM
```

```
International 2003 - 2007
Application state information: (//192.168.110.78:30400/remoteCallRec)
Verbosity: 5
~~~~~
CallREC 4.6.0, build: 100525_2234, Copyright (c) 2002-2009 ZOOM
International. All rights reserved
```

```
-- CoreOfCallRec --
1001010 [Calls]          [***...] - Count of active calls ...
0
1001015 [Calls]          [****.] - Last call id ... 0
1002010 [Couples]       [***...] - Count of active couples
... 0
1002015 [Couples]       [****.] - Last couple id ... 0
1003010 [Streams]        [***...] - Count of active streams
... 0
1003015 [Streams]        [****.] - Last stream id ... 0
1004010 [ThreadManager]  [***...] - Thread manager status ...
Used - 2, unused - 2
1004011 [ThreadManager]  [***..] - Min unused threads ... 20
```

```
-- DecoderCommunicator --
7000020 [decoderServerCommunicator] [****.] - Prefer archives for files
... mp3, zip, wave
7000030 [decoderServerCommunicator] [****.] - Prefer archives for emails
... mp3, zip, wave
7001001 [decoderManager]    [*....] - Info ... Decoder3
(Decoder3 4.6.0, build: 100525_2232)
..... [ OK ]
7000039 [decoderManager]    [***...] - Email Template ... email
7000040 [decoderManager]    [***...] - Email Error Template ...
emailerror
```

Restarting and Shutting Down the Server

To restart the server from the local console, press **CTRL+ALT+DEL** combination. The system safely terminates all services and restarts.

To restart the server remotely, log in as `admin` then type `su -` and the password into the console and enter the command `reboot`.

To shut down the server, log in as `admin` then type `su -` and the password into the console and then enter the command `halt`.

Restarting the Decoder

If new calls are not visible in the GUI, then restart the Decoder:

1. Log in as `admin` then type `su -`
2. Type the command

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

Restarting Call Recording Core

To restart only Call Recording Core, while the rest of components stay running:

1. Log in as `admin` then type `su -`
2. Type the command

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

Restarting the Call Recording System

To restart the entire Call Recording system without rebooting:

1. Log in as 'admin' then type `su - root`
2. Type the command

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

Restarting other Call Recording Components

To restart individual Call Recording components:

1. Log in as `admin` then type `su -`
2. Type the command

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

Where `COMPONENT_NAME` is:

COMPONENT_NAME	Component to be Restarted
<code>callrec</code>	All Call Recording components
<code>callrec_archive</code>	Archive Tool
<code>callrec_callmonitor</code>	Call Monitor
<code>callrec_configmanager</code>	Configuration Manager
<code>callrec_core</code>	Call Recording Core
<code>callrec_delete</code>	Delete Tool
<code>callrec_ds</code>	Decoder Server
<code>callrec_genesys</code>	Genesys Integration Module
<code>callrec_instreamer</code>	Audio Stream Recording
<code>callrec_ipcc</code>	UCCE Integration Module
<code>callrec_ipccex</code>	UCCX Integration Module
<code>callrec_mixer</code>	Audio and Video Mixer
<code>callrec_naming</code>	Naming Tool
<code>callrec_relocation</code>	Relocation Tool
<code>callrec_restore</code>	Restoring Tool
<code>callrec_rmi</code>	RMI Service
<code>callrec_rs</code>	Recorder Server

COMPONENT_NAME	Component to be Restarted
callrec_rts_jtapi	JTAPI Adapter
callrec_rts_sip	SIP Adapter
callrec_rts_skinny	Skinny Adapter
callrec_slr	Active Recorder
callrec_synchro	Synchronization Tool
callrec_screenrec	Screen Capture
callrec_tools	All Tool Components
callrec_web	Web Server (Tomcat5)

Table 25: Restarting Individual Call Recording Components

Restarting Clustered Servers

Go to `/etc/callrec/callrec.conf` on each server of the cluster to see which services are enabled.

The components must be restarted in a specific order.

First stop Call Recording services on all clusters:

```
/etc/init.d/callrec stop
```

Then start the cluster that has the core service enabled:

```
/etc/init.d/callrec start
```

Start the rest of the cluster and check the status of all components.

If a component is located on more than one server and these servers are configured as a cluster, then you must name each component and restart them individually:

1. For each server, log in as `admin` then type `su -`
2. Type the command

```
/opt/callrec/bin/rc.COMPONENT_NAME restart (see table above)
```

3. Repeat steps 1 and 2 for each server
4. After restarting all servers in the cluster, log in to the server with the Call Recording Core module and type the command:

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

5. Restart the configuration manager with the command

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

Restarting Redundant Servers

Redundant servers allow you to ensure there is no loss of data when you restart services. To restart redundant servers, restart the primary server (or cluster) and then the Call Recording Core and Configuration Manager. After Call Recording Core has restarted, restart the secondary server (or cluster). Finish the process by restarting Call Recording Core and Configuration Manager again.

Restoring the Default Configuration

Important:

Do not change your configuration settings without consulting the system administrator. Write down all custom settings so that they can be restored.

To revert all the Call Recording configuration settings to the original defaults, follow this process:

1. Stop the Call Recording service:

```
service callrec stop
```

2. Backup current configuration files, for example using tar:

```
tar -cf backup-cfg.tar /opt/callrec/etc/*
```

3. Replace current configuration files with the defaults:

```
/bin/cp /opt/callrec/etc/default/* /opt/callrec/etc
```

4. Execute the main Call Recording configuration script (see the Implementation Guide):

```
/opt/callrec/bin/callrec-setup
```

5. Start Call Recording:

```
service callrec start
```

6. Log in to Call Recording and use the web configuration interface to confirm your default settings.

Using Symlinks to the Call Recording PCAP Storage Directory

It has been reported that there are occasional problems during Call Recording migration or upgrading if Linux symbolic links ('symlinks') have been used for key Call Recording folders. Specifically, an issue has been reported when the 'pcap' storage folder has been linked to a different physical location, using the Linux 'ln -s' command. In some cases, the symlink(s) are no longer found, causing failure of the associated Call Recording components.

It is therefore recommended that symbolic links are not used for the `/opt/callrec/data/pcap` PCAP storage directory.

Instead, specify the physical pcap folder location in the `/opt/callrec/etc/callrec.conf` configuration file, in the following section:

```
#  
# Path to store pcaps  
#  
PCAP="/opt/callrec/data/pcap"
```

Important Note on Synchronization

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

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

Check the NTP daemon configuration file which is located in `/etc/ntp.conf` if it contains correct addresses of NTP servers. Look for "server" records and change the addresses of the servers to the ones you use in your network.

For example `server 3.cz.pool.ntp.org`

Stop the NTP daemon using the following command:

```
/etc/init.d/ntpd stop
```

Stop Call Recording and the Database using the following command:

```
/etc/init.d/callrec stop  
/etc/init.d/postgresql stop
```

Synchronize time manually using the following command:

```
ntpdate <timeserver IP address>
```

Write the current time to the system BIOS using the following command:

```
hwclock --systohc
```

Start the NTP daemon using the following command:

```
/etc/init.d/ntpd start
```

Check if the time/date is correct now using the following command:

```
date
```

Start the database and Call Recording again using the following command:

```
/etc/init.d/postgresql start  
/etc/init.d/callrec start
```

The system takes a while before it is synchronized (usually around 15 minutes from when the NTP daemon was started):

Check the synchronization state using the following command:

```
ntpstat
```

Mounting Windows File Shares

Connecting a Windows-based remote file storage facility to a Linux operating system can be tricky. To configure a connection to (or 'mount') a Windows file share for archive or backup media storage, for example, use the following procedure:

1. Ensure the following information is available:
 - Windows share username and password
 - Windows server IP address or share address (of the form `//winserver/path/to/folder` - note the use of forward slashes / instead of backslashes \)
 - Root (administrator) access to the Call Recording Linux server

Important:

When a Windows file share is used for Call Recording data storage, ensure that the password change policy is disabled for the Call Recording user account. Failure to disable enforced password changes can lead to Windows shares being made inadvertently inaccessible to Call Recording.

2. Log in to the Call Recording server and switch to the root account if necessary (using the `su` command):

```
su -
```

3. Create the required mount point (the directory to later access the Windows share). This can be any directory path, for example `/mnt/winserver`:

```
mkdir -p /mnt/winserver
```

4. Use the `mount` command as follows (where `user` and `pass` are replaced by your Windows share username and password, and the share address & mount point are modified appropriately). This command should all be on one line:

```
mount -t cifs //winserver/path/to/folder -o username=user,password=pass /mnt/winserver
```

Tip:

To remove a mounted file share, use the `umount` command:

```
umount -t cifs /mnt/winserver
```

5. Once mounted, the Windows file share can now be accessed from the Linux system using standard directory commands:

```
cd /mnt/winserver
ls -l
```

6. In Call Recording Web GUI settings, enter the mount point directory path to reference the Windows file share (for example `/mnt/winserver/path/to/folder`).
7. Step 4 needs to be repeated each time the Linux system is restarted. To auto-mount this file share when the system starts, add the following single line to the `/etc/fstab` file (updating the share address, mount point, `user` and `pass` parameters as required):

```
//winserver/path/to/folder /mnt/winserver cifs username=user,
password=pass 0 0
```

Troubleshooting Tips

The following information may help to troubleshoot errors that result from trying to mount a Windows file share:

- Authentication issues may be fixed by providing more information. If the Windows server uses domain authentication, add the domain either in the options (`username=user, domain=domain, password=pass`), or as part of the username (`username=domain/username`).
- Password issues may be fixed by adding quotes around the password (`username=user, password="pass"`)
- Connection issues may be due to a firewall. SMB connections from Linux require TCP ports 137, 138, 139, 445 to be open in the Windows server.
- If a `cifs_mount` error (value `-22`) is received, you may need to install the Samba client first: `yum install samba-client`.
- On older Linux releases (RHEL ≤ 4 and similar), the `smbfs` type needs to be used in the mount command, for example:

```
mount -t smbfs //winserver/path/to/folder -o username=user,password=pass  
/mnt/winserver
```

For more information on accessing an SMB file share from Linux, see the following how-to page: <http://tldp.org/HOWTO/SMB-HOWTO-8.html>.

Advanced Configuration Parameters

Some Call Recording components have advanced configuration parameters that are not included in the Call Recording Web GUI Settings section. These parameters can be specified in Call Recording configuration files, therefore root administrator access to the Call Recording servers is required.

After modifications have been made to configuration files, restart the Configuration Service and related components. For example, this can be achieved for the Active Recorder (SLR) as follows:

```
/opt/callrec/bin/rc.callrec_configmanager restart
Stopping CallREC CONFIGMANAGER: .           [ OK ]
Starting CallREC CONFIGMANAGER: .           [ OK ]
/opt/callrec/bin/rc.callrec_slr restart
Stopping CallREC SLR 1: .                   [ OK ]
Starting CallREC SLR 1:                      [ OK ]
```

Active Recorder (SLR) Configuration Parameters

The Active Recorder (SLR) is configured in the `callrec.derived` configuration file, located by default at `/opt/callrec/etc/callrec.derived` on the Call Recording server. This file contains an SLR section, similar to the following:

```
#
# SpanLess Recorder server
#
# SLR_IORFILE is prefix of files to save oir file for slr instance.
# SLR_COUNT defines required count of SLRs instances to run.
# SLR_PARAM[x] defines params for specific instance of SLR.
#
#         Every instance must differ from others at least in address(-
a)
#
#         or port(-P) to listen on. Also RPT port range must be
exclusive
#
#         for all instances (-R and -S).
#
SLR_IORFILE="$TMP/slr"
SLR_COUNT=1
SLR_PARAMS[1]="-t 120 -m 40 -A 0 -A 8 -A 9 -A 18 -A 13 -A 19 -l
/etc/callrec/slr.log4cxx.properties"
```

The `SLR_PARAMS[1]` property contains the parameters for the first Active Recorder instance. The main parameters and their values are shown in the following table. A complete list of parameters can be obtained by querying the `slr` module directly:

```
/opt/callrec/bin/slr --help
```

Parameter	Description
<code>-A --accept <num></code>	Accept payload num. can be specified as several options (0, 8, 9, 18, 13, 19)
<code>-m --minpackets <num></code>	Minimum packets representing not empty stream (default: 0)
<code>-l --logger <name></code>	File with log4cxx configuration (default: <code>slr.log4cxx.properties</code>)
<code>-e --sessionexpires <num></code>	Timeout of SIP session expiration in seconds (default: 1800). Valid range: 90 - 86400
<code>-s --rejectedsessions <num></code>	Max. rejected SIP sessions between 2 states (default: none)

Parameter	Description
-a --sipaddress <ip>	Listening SIP address (default: 0.0.0.0)
-P --sipport <port>	Listening SIP port (default: 5060)
-R --rtpport <port>	Starting RTP port (default: 16384)
-c --rtpportscout <num>	Count of allocated RTP ports in pool (default: SIP sessions * 2)
-n --notcp	Do not use TCP protocol
-S --maxsessions <max>	Max. concurrent SIP sessions (default: 400)
-M --requiremark	Starting mark for SIP session is required

Table 26: Active Recorder Configuration Parameters

Notes on Parameters

-e (--sessionexpires):

The Active Recorder supports the SIP Timer extension ([RFC-4028](#)). During SIP session negotiation, the Recorder initially assumes that the remote party handles session renewal via the Timer extension mechanism. However, if the remote party does not support the timer extension or its processing, the Active Recorder performs this 'session audit' functionality itself. It starts a timer (configured with this parameter's value) after a re-INVITE request issued to the remote party has timed out, and issues a BYE request to terminate the session if that timer also times out.

Limit on the Maximum Number of Threads

Note for system administrators:

Since RHEL 6.2 the number of created threads for an application has a soft limit applied. This can cause erratic behavior and random failures of the application. The installation scripts remove this configured limit but if the installation has been done without the installation then the limit still applies.

https://bugzilla.redhat.com/show_bug.cgi?id=432903

Edit the `/etc/security/limits.d/90-nproc.conf` file to remove the limitation:

```
/etc/security/limits.d/90-nproc.conf
```

```
* soft nproc unlimited
```

Additional Call Recording Scripts

Routine tasks like backup are performed with Call Recording tools, located on the Maintenance tab in Settings.

Specialized and occasional tasks in Call Recording are performed with Call Recording scripts, executed directly from the command line.

All Call Recording scripts are located in:

```
/opt/callrec/bin
```

Call Recording scripts are executed like any other shell script. Most scripts also require additional parameters.

This chapter contains the following sections:

[bugreport](#)

[call2mp3](#)

[callrec_status](#)

[repaircalls](#)

[selectivebackup](#)

[status.pl](#)

[tools](#)

[gen_cfgtest](#)

[Additional Scripts](#)

bugreport

Use the `bugreport` script to report bugs or request assistance from Genesys Labs, Inc..

The `bugreport` script collects all relevant system information, including logs, configuration, error messages, and server status. The report is stored in the root folder by default, and the file size varies between 1-10MB.

Important:

To automatically send the results of the `bugreport` script to Genesys, Enable SMTP within Call Recording so it can send email outside the local network.

The `bugreport` script has the following additional parameters (none of them are required):

```
usage: /opt/callrec/bin/bugreport + params
-a | --about - about the tool
-b | --db_dump - dump information about calls from the db for the entered
  time steps using a combination of -t and -e switches; turned off by default
  this option does not work with -s
-c | --cfiles - check for cfile integrity in the filesystem
  turned off by default; slow on a large db; not working with -s
-d | --directory <directory> - place report into specific directory
  default directory is /opt/callrec/data
-e | --end <YYYY-MM-DD> - end date for db_dump; format YYYY-MM-DD
  default: 2030-12-31; only to be used in combination with -b
-h | --help - print this help
-m | --mail - send file by email after finishing report to Genesys Support
-l | --list - information about calls in the filesystem
  turned off by default; not working with -s
-r | --callrec - only Call Recording statistics
-s | --system - only system statistics
-t | --start <YYYY-MM-DD> - start date for db_dump; format YYYY-MM-DD
  default 1970-01-01; only to be used in combination with -b
-g | --log_date - also collect logs from specific date; format YYYY-MM-DD
  default: none
```

The `bugreport` script requires administrator (`root`) privileges to run. Run it using one of the following methods:

1. Log in to the server console or start an SSH session as the `root` user OR log in using a non-administrator user account (for example `admin`) and switch to an account with higher privileges using the `su` utility: `su - root`
2. Run the following command, including any appropriate parameters as required:

```
/opt/callrec/bin/bugreport
```

Tip: RedHat Linux also includes the `sudo` command, enabling a normal user to run a command with administrative permissions, if the user is included in the `/etc/sudoers` file:

```
sudo -i /opt/callrec/bin/bugreport
```

Typical output from the command is as follows:

```
[root@tstcr003 bin]# /opt/callrec/bin/bugreport
Retrieving information from this machine: ..... [ OK ]
Zipping into archive: . [ OK ]
Copying results to "./CallREC_report_1235398690.zip" : [ OK ]
```

call2mp3

The `call2mp3` script enables “raw” streamed data to be converted into audio files.

Use this script in the event an error occurs during encoding. Some streams may have remained un-encoded. The `call2mp3` script enables these un-encoded streams to be selected and encoded as MP3 or WAV files.

Important:

The `call2mp3` script does **NOT** add files to the database.

```
/opt/callrec/bin/call2mp3 FILE1 [FILE2] [OPTIONS]
```

You can identify multiple file for encoding; FILE1 is the source file or directory, and additional files are identified within square brackets [FILE2] and so on. If you identify an entire directory, all the files within that directory will be processed.

If no additional parameters are set, the default values are used.

Parameters:

- `-e`: Allows you to select the encoding used for output – MP3 or WAV (the default setting is MP3)
- `-d`: Specifies a destination file or directory for the encoded files. This allows you to rename the output file if only one call is encoded.
- `-p`: Plays the encoded file immediately after encoding
- `-b`: Allows you to define the output file’s bitrate (for MP3 only -- see chapter See Audio Quality settings in Decoders for more information)
- `-logger`: Enables logging of encoding, this option must specify the path to the `log4j` properties file.
- `-help`: Displays help text.

callrec_status

The `callrec_status` script displays information about a Call Recording component's status, configuration, and availability. If you identify a Call Recording service with a single parameter, only that parameter's status displays.

Use `callrec_status` to change some service parameters.

The `callrec_status` script uses the Application Communicator component.

```
/opt/callrec/bin/callrec_status -PARAMETER(S)
```

Parameters:

- `-bindName [bindName]` – allows you to specify the RMI bind name of the selected Application Communicator –use the complete path (the default value is `//localhost:30400/remoteCallRec`)
- `-help`: Displays help.
- `-host [host]`: Allows you to specify the RMI host of the selected Application Communicator (the default value is `localhost`).
- `-modifyHelp [{name}|all]`: Displays available help information about modifiable properties (for specific module or `all` modules).
- `-modifyInt [module,property,value]`: Allows you to modify a property of the selected module if the property type is an `Integer`. Use the format `ModuleName,PropertyName,NewValue` (possible values and names can be seen with `modifyHelp`).
- `-modifyNames`: Returns names of modules allowing modification of properties.
- `-modifyString [module,property,value]` : Allows you to modify properties of a selected module if the property type is `String` Use the format `ModuleName,PropertyName,NewValue` (possible values and names can be seen with `modifyHelp`).
- `-name [name]`: Allows you to specify the RMI bind name for the selected Application Communicator (the default value is `remoteCallRec`).
- `-names`: Returns all available names for the Application Communicator interface.
- `-port [port]`: Allows you to specify the RMI bind port for the specified Application Communicator (the default value is `30400`).
- `-restart` : Remotely restarts the Application Communicator.
- `-state [{name}|all]`: Returns state information about selected module or all modules (the `-state all` output is identical to service `callrec status`)

- `-stateNames`: Displays the names of all modules providing state information.
- `-stateOption [status|failed]`: Allows you to limit displayed information to status (OK and FAILED) lines (`status`) or to limit display to only the lines where the status is FAILED (`failed`).
- `-states`: Displays status of all modules providing state information (this is an extended version of `-state all`).
- `-stop`: Remotely stops the Application Communicator .
- `-verbosity [1|2|3|4|5]`: Sets the verbosity of state displays (all information: 5, default: 2, only state: 1)
- `-version [{name}|all]`: Displays version information for a named module, or all modules.
- `-versionNames`: Returns names of modules providing version information.

Sample usage:

```
/opt/callrec/bin/callrec_status -state all -name <module name> -verbosity 5
```

You can obtain the list of modules by running:

```
/opt/callrec/bin/callrec_status -states
```

Please note that module names are case sensitive.

repaircalls

The `repaircalls` script is designed to help you recover from a decoder server dropout or other malfunction in the encoding process.

During normal operations, if there is an error preventing encoding of call data (for example, an unknown codec is used), the recorded streams are packed as zip files, and then stored for future recovery. In the event of decoder server failure during encoding, the raw data stays uncompressed in raw form.

The `repaircalls` script tries to recover all available un-encoded calls by moving them back into the decoding queue for processing by the decoder server. In other words, this tool repairs calls and makes them available for Call Recording users.

The `repaircalls` script searches all calls that can be recovered and encodes them into MP3 (or another selected format). You can specify a call's couple ID for processing one call, or a time interval and maximum number of calls for automatic recovery of all calls within the specified interval.

Important:

Connection strings for core RMI and decoder are compulsory parameters.

Example: Repairing calls from a specified period

```
/opt/callrec/bin/repaircalls -config_core [path and port] -config_decoder [path and port] -hour [interval] -limit[max files] -PARAMETERS
```

Example: Repairing a specific call

```
/opt/callrec/bin/repaircalls -config_core [path and port] -config_decoder [path and port] -coupleid [ID] -PARAMETERS
```

- **Parameters:**
 - config_core [configuration service] – compulsory option, has to point to Core – as: //address:port/core
 - -config_decoder [configuration service] - compulsory option, has to point to decoder - //address:port/decoders

- `-type [result type]` – used for defining output format - MP3, WAV, ZIP (the default value is mp3)
- `-hour [interval]` – defines how many hours to look backwards for data, 0 means all data.
- `-coupleid [db call id]` - ID of call couples that will be decoded
- `-limit [max. files]` – sets how many calls to repair when more calls are found within the selected interval (default value is 100, 0 means all files). This option is compulsory – it takes a lot of server resources to repair calls and this option prevents overloading the server.
- `-zipfiles` – Allows you to include ZIP files containing raw data for repair. If you do not include ZIP files, they are ignored by the `repaircalls` script.
- `-nouupdatedb` – when this option is used, no updates will be made to the database and source files will stay on the server – use this, if you want to test “repairability” of selected couples.
- `-logger [logger properties]` –defines the path to properties for Log4J, when you want to create a log file.
- `-help` – displays help

Sample usage:

```
/opt/callrec/bin/repaircalls -hour 2000 -limit 2000
```

Where the Hour states the delay how many hours ago the queue is checked until.

Limit stands for maximum number of fixed calls If you want to fix all calls until now, use 0 as a value for both parameters. Note it takes significant time to fix all files if the queue is long and it can also affect performance of the system. It is recommended to use this command during off-peak hours.

selectivebackup

Normal backup is controlled through the Call Recording interface. The `selectivebackup` script enables the specification of additional backup parameters, such as UCCE or external data, by directly editing the `tools.xml` configuration file values.

```
/etc/callrec/tools.xml
```

There are no command line parameters. The `selectivebackup` function outputs files to a ZIP archive.

Open the `tools.xml` configuration file and locate Specified Configuration for `selectivebackup`.

```
<SpecifiedConfiguration name="selectivebackup">  
  <Value name="enabled">>false</Value>
```

- `enabled` can be set to `true` (enabled) or `false` (disabled).

```
<Value name="exportFilename">calls.xml</Value>  
<Value name="basename">export</Value>  
<Value name="maxSize">30</Value>  
<Value name="crc">>true</Value>
```

- `exportFilename` specifies the name of the XML file exported by `selectivebackup`.

Important:

No changes are required in this value. The exported xml file is stored in a different directory than that used by the standard backup tool.

`basename` is the filename of the backup zip archive and can be freely changed. The output filename will be `basename+timestamp+.zip`.

the `maxSize` value sets the maximum file size of the archive in MB. If the archive is bigger than this value, `selectivebackup` splits it into multiple files.

`crc` Create a checksum control. Set this to `true` or `false`.

```
<Value name="xslFilename">calls.xsl</Value>
<Value name="exportIndex">calls.html</Value>
```

`xslFilename` must end with the `.xsl` extension.

`exportIndex` must end with the `.htm` or `.html` extension

```
<Value name="resourceDir">res</Value>
```

`resourceDir` specifies the subdirectory with resources related to the description files, such as pictures used by `exportIndex`. Do not change this value.

```
<Value name="database">callrec</Value>
```

The `database` value identifies the source of call information to be backed up. This database is also used in any filtering. This must be the database used by Call Recording – typically this is the `callrec` pool. Use the Call Recording GUI to verify the name of this value.

```
<Value name="time">start=1.1.1800 end=1.1.1900</Value>
```

`time` specifies times to start and end date the backup. All calls within this interval will be processed. The format of date and time values is the same as for all other tools.

```
<Value name="filesOnly">>true</Value>
<Value name="deleteFiles">>false</Value>
```

- `filesOnly` can be set to true or false. When the value is true, only files with calls or video are stored. When the value is false, then the related database records are also stored.
- `deleteFiles` allows you to enable (true) or disable (false) the deletion of database files once they have been backed up.

```
<Value name="cfgDir">/opt/callrec/tools</Value>
<Value name="tmpDir">/tmp/export/tmp</Value>
<Value name="sourceDir">/home</Value>
<Value name="targetDir">/tmp/export</Value>
<Value name="intervalPeriod"/>
<Value name="backupDir">{$USER}/</Value>
```

`cfgDir`: Identifies the directory where main tools files (java executables) are stored. Usually `/opt/callrec/tools`.

`tmpDir`: Identifies the temporary directory for backup.

`sourceDir`: Identifies the source directory where calls are stored.

`targetDir` : Identifies the target directory where the backup will be created.

`intervalPeriod`: Allows you to define the time period to run `selectivebackup`. You can define wake up and suspend times to prevent running regular backup simultaneously with `selectivebackup`.

`backupDir` : Identifies the directory to be created within the target directory where backups are stored. The variable `{$USER}` is set as the default – the directory has the name of the user who executes `selectivebackup`.

Important:

The values of directories used by `selectivebackup` should NOT ordinarily be changed.

```
<Value name="wakeupTime">00:10</Value>
<Value name="suspendTime">23:30</Value>
```

`wakeupTime` and `suspendTime` allows you to prevent running regular backup simultaneously with `selectivebackup`.

```
<Value name="limitQuery">description = &apos;XYZ&apos;</Value>
</SpecifiedConfiguration>
```

`limitQuery` – allows you to specify a search string that filters the backup. Identify any string within the call description, or standard Call Recording database entity.

Important:

You must use the format `'string'`

Example: To limit the backup to only the calls that contain the word “training” in the call description field:

```
<Value name="limitQuery">description = &apos;training&apos;</Value>
```

Important:

Do not use wildcards or multiple values. The `limitQuery` script finds only exact matches.

When the `r selectivebackup` values are defined, save the changes to the xml file.

To execute the `selectivebackup` script, use the command line. All parameters are defined in the configuration file.

```
selectivebackup
```

status.pl

The status.pl script is run every five minutes by cron. It checks the status of system components. If an error is found, it sends a report by default to the Genesys Support team.

When all components are running properly, no message is generated.

tools

The tools script initializes maintenance tools and executes them. The tools script is executed periodically by cron. The default period is every day at 0:00. To check the status of this script, check the crontab.

gen_cfgtest

The `gen_cfgtest` script updates system configuration when the Genesys integration module is used. This script interconnects Call Recording and Genesys Configuration server.

Additional Scripts

There are two additional scripts used during installation:

- `chkcalls` changes attributes of storage directories to grant read/write permission to Call Recording
- `mkcalls` is used for creating the directory structure

There is no need to execute these two scripts manually.

38 AMQP Implementation

This chapter describes how Call Recording uses the AMQP protocol for message interchange between Core and Decoder. Call Recording uses persistent queues stored on the hard drives making all unprocessed messages available after recovery if the decoder fails. The AMQP broker is RabbitMQ.

This chapter contains the following sections:

[Resources Required for RabbitMQ](#)

[AMQP Queues in Call Recording](#)

[Listing All Available Queues](#)

[The Decoding Process](#)

[Repair Call Process](#)

[Media Removal Process](#)

[RabbitMQ configuration](#)

[Changing Where RabbitMQ Stores the Content of the Queues Clean installation](#)

[Changing Where RabbitMQ Stores the Content of the Queues Running installation](#)

[Troubleshooting AMQP](#)

[Typical Issues with Decoding performance](#)

[Typical Issues with Available Disk Space](#)

Resources Required for RabbitMQ

The minimum resources required for RabbitMQ in Call Recording are:

- 2 GB RAM
- 2 GB HDD space
- A Dual Core CPU based on Intel Core 2 architecture or better (Xeon 3000 series or later)

The exact requirement for RAM and disc space depend heavily on the speed and availability of the Decoder server. This is determined by the amount of concurrent calls and requirements for call records availability in web UI after call is finished.

AMQP Queues in Call Recording

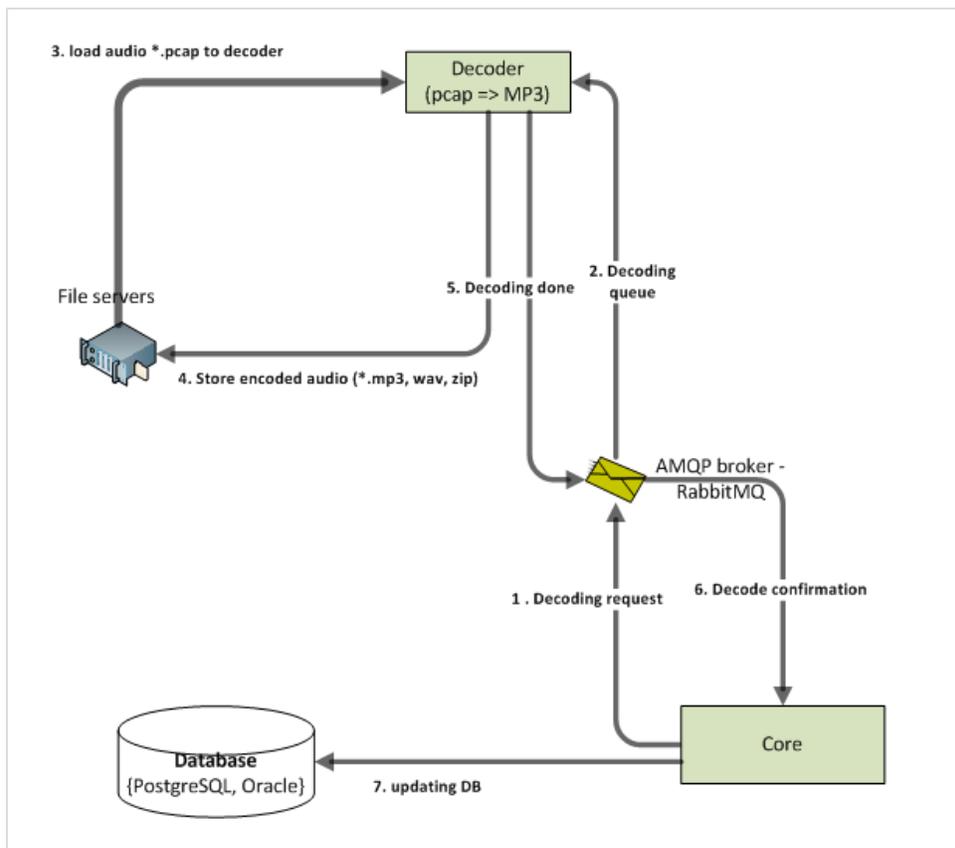


Figure 277: Data flow between Core and Decoder

The figure shows communication between Core and Decoder from high level point of view. AMQP communicates asynchronously and uses less resources to exchange messages between the Core and Decoders, compared to previous synchronous RMI communication.

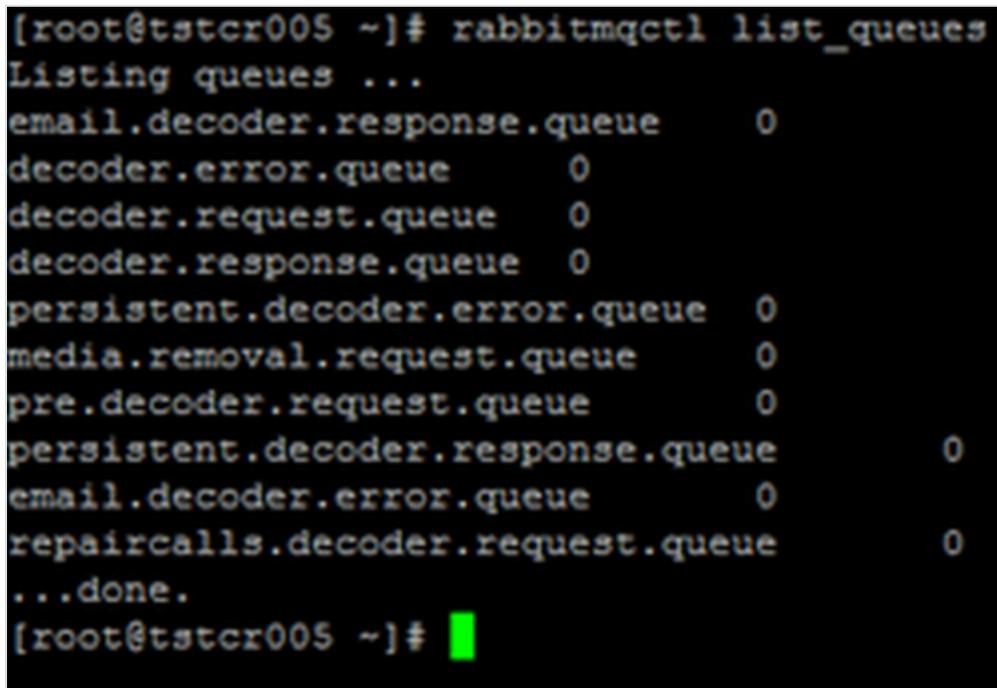
Listing All Available Queues

To list all available queues:

On the server running the AMQP broker: Log in as `admin`. Enter `su -` to log in as the root user. Enter the password, the default is `zoomcallrec`.

Enter the command:

```
rabbitmqctl list_queues
```



```
[root@tstcr005 ~]# rabbitmqctl list_queues
Listing queues ...
email.decoder.response.queue      0
decoder.error.queue               0
decoder.request.queue             0
decoder.response.queue            0
persistent.decoder.error.queue    0
media.removal.request.queue        0
pre.decoder.request.queue          0
persistent.decoder.response.queue  0
email.decoder.error.queue          0
repaircalls.decoder.request.queue  0
...done.
[root@tstcr005 ~]#
```

Figure 278: Rabbit Queue List

The Decoding Process

All communication between core and the decoder is handled by the decoder communicator.

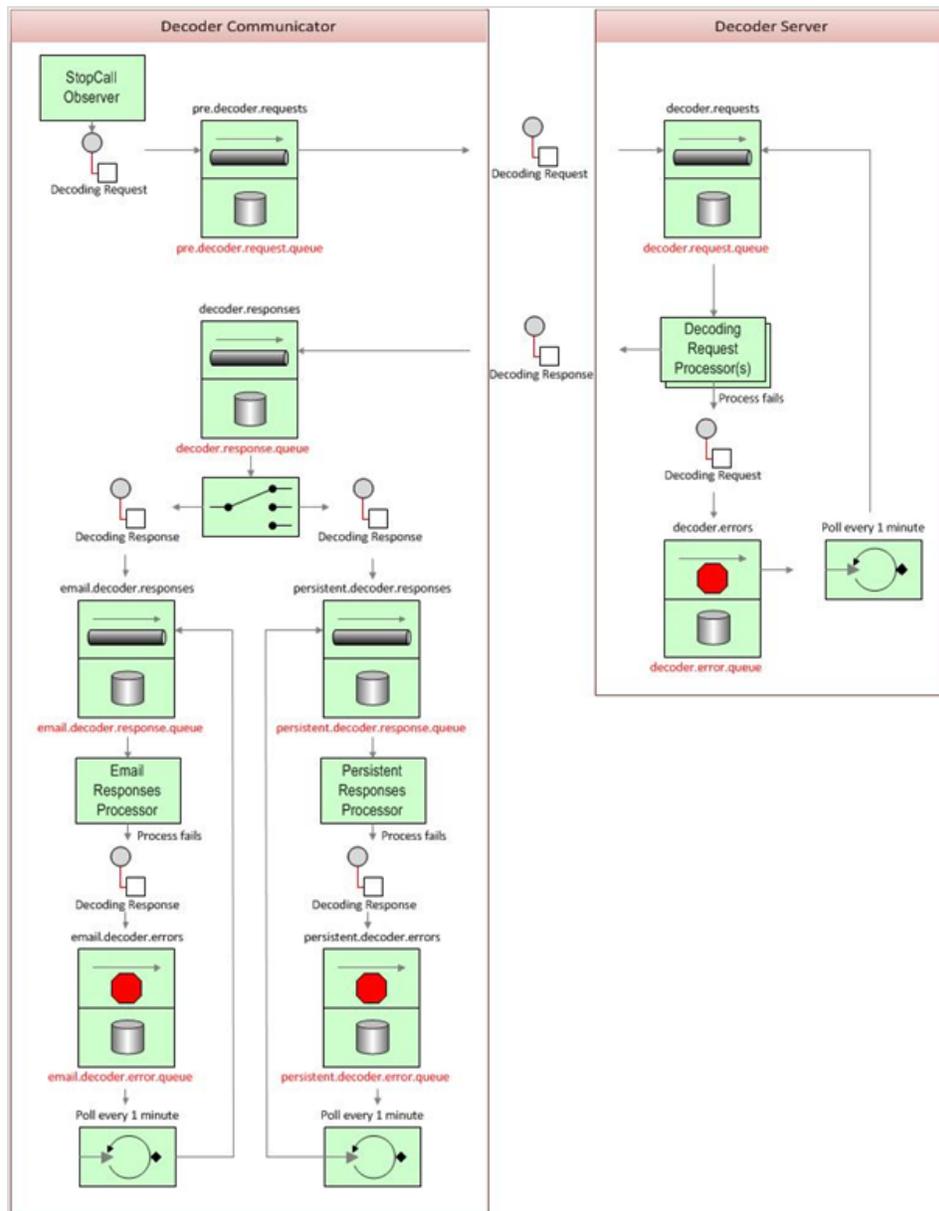


Figure 279: Decoder Communicator

The figure shows detailed messages workflow related to decoding process.

The decoding process is as follows:

1. When the call finishes `StopCallObserver` creates the decoding request and sends it to `pre.decoder.requests`.
2. The message is filtered for duplicate requests and the couple is marked as sent for decoding and forwarded to `decoder.requests`.
3. The decoding requests processor takes this decoding request and tries to process it.
4. If the decoding fails to return a response with either a successful result or information about a decoding error, the decoding request is moved to the `decoder.errors` queue. This channel is pooled once a minute and up to 500 messages in it are moved again back to `decoder.requests` in one cycle.
5. If the decoding request process can create an error or success response, it creates a decoding response and sends it to the `decoder.responses` channel.
6. The `decoder.responses` channel has a registered router, that copies the response to either `email.decoder.responses` or `persistent.decoder.responses`. The routing is performed based on payload content. A message containing an email to send the result is copied to `email.decoder.responses`. A message set to be persistent is copied to the `persistent.decoder.responses` queue. If the message contains both, it is copied to both channels.
7. These specific queues are processed separately by their own processors. If a process fails the decoding response message is moved to the `email.decoder.errors` resp. `persistent.decoder.errors` channel as shown in the figure. These error channels are polled once a minute for existing messages and up to 500 of them are moved back for another process attempt. If the database is unavailable and the persistent process is not able to store the decoding result in the database, then the re-triggering process ensures that the response is stored once the database is available again.
8. If the response is successfully processed its couple is unmarked as sent for decoding.
9. At the end the process checks whether the system is configured to remove the PCAP source files and if so it creates the media removal request for each of them and send it to the corresponding channel as is described

Repair Call Process

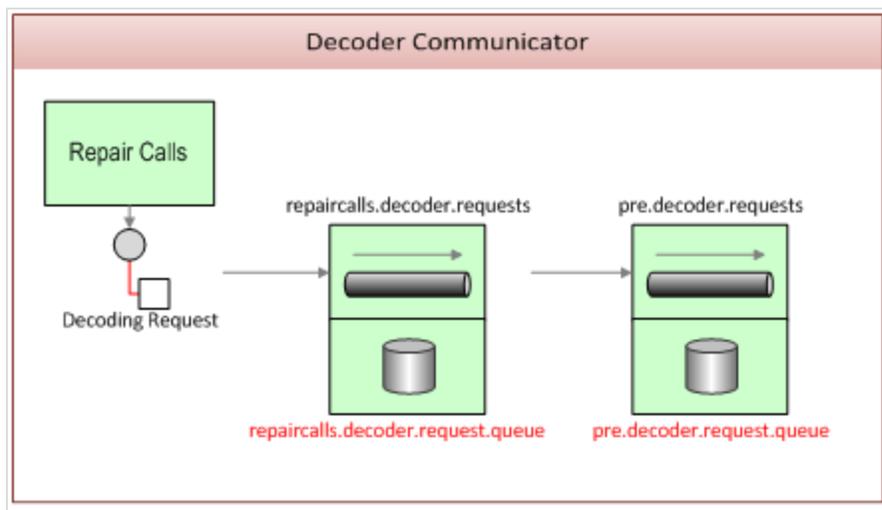


Figure 280: Decoder Communicator

The repair calls process requests decoding for failed decoding requests. Failed decoding requests are requests that were not inserted to main decoding process at all or their result was not sufficient for some reason, for example, a zip with unprocessed PCAPs. Repair calls removes the "sent for decoding" mark so that the couple can be resent for decoding.

The repair calls process creates a decoding request for repaired couple and passes it to the `repaircalls.decoder.request` channel. Requests passed to this channel are immediately moved to `pre.decoder.requests` channel, processed as normal by the decoding process.

Media Removal Process

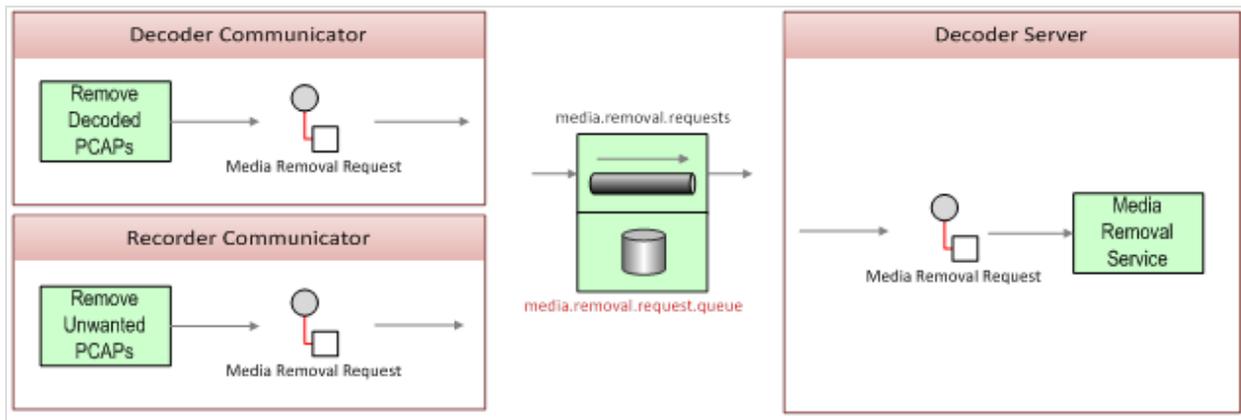


Figure 281: Media Removal Process

When more than one recorder records a call, then only one set of PCAPs is required. The other set of PCAPs can be deleted. Once the source files are successfully processed they can be deleted if the system is not configured to store them. The decoder communicator and recorder communicator modules can decide that a media file is no longer needed and should be deleted and so they create a media removal request and send it to the `media.removal.requests` channel.

RabbitMQ configuration

The default configuration created by the callrec-setup script installs RabbitMQ together with Core on the same machine.

RabbitMQ As a Dedicated AMQP Server

If needed for performance reasons or if the customer already has Rabbit MQ installation, the AMQP broker can be installed on dedicated server and Call Recording configuration can be changed accordingly via the web interface (or by editing core.xml config file.

Changing the AMQP Server via the Call Recording UI

To change the AMQP Server settings via the Call Recording UI:

Navigate to **Settings > Configuration > CallREC Core > Servers > AMQP Server**, on the server running the configuration service.

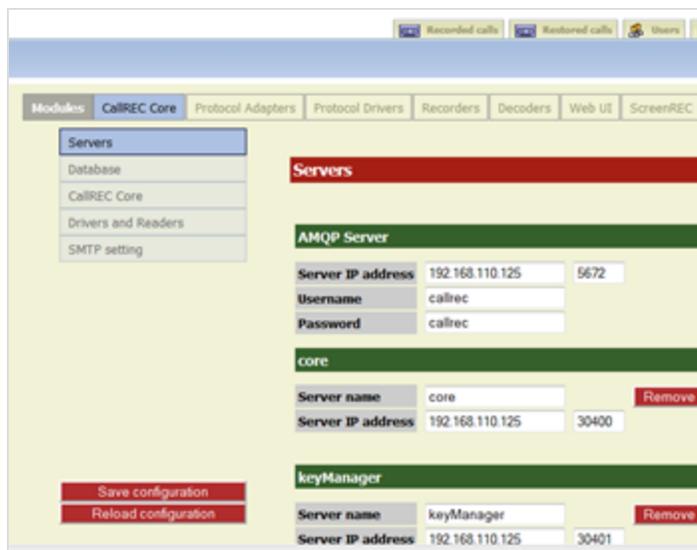


Figure 282: AMQP Server Settings via Web Interface

Type the Server IP address and port number.

Restart Call Recording to activate the changes.

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

On the server running the configuration service.

```
service callrec restart
```

Changing Where RabbitMQ Stores the Content of the Queues Clean installation

1. Install Call Recording, do not configure Call Recording or run the default_callrec_installation script yet.
2. Log in to server as root
3. Create rabbitmq directory in /opt/callrec/ (

```
mkdir /opt/callrec/rabbitmq
```

```
mkdir /opt/callrec/rabbitmq/mnesia
```

4. Edit the file /usr/lib/rabbitmq/bin/rabbitmq-defaults
5. Change MNESIA_BASE from

```
/var/lib/rabbitmq/mnesia
```

to

```
/opt/callrec/rabbitmq/mnesia
```

6. Change owner and group of newly created folders to

```
rabbitmq (chown -R rabbitmq:rabbitmq /opt/callrec/rabbitmq)
```

7. Run the default_callrec_installation
8. Open Call Recording and log in as admin
9. Go to **Settings > Configuration > Protocol Adapters** and set up the CallManager
10. Go to **Recording rules** and insert new rule: Record, mask *
11. Restart Call Recording

```
service callrec restart
```

12. Start making calls

Changing Where RabbitMQ Stores the Content of the Queues Running installation

Running installation (CallREC installed, recording set and working)

1. Log in to server as root
2. Edit the file `/usr/lib/rabbitmq/bin/rabbitmq-defaults`
3. Change `MNESIA_BASE` from

```
/var/lib/rabbitmq/mnesia
```

to

```
/opt/callrec/rabbitmq/mnesia
```

4. Copy `Rabbitmqm` folder from `/var/lib` to `/opt/callrec`

```
cp -r /var/lib/rabbitmq /opt/callrec/
```

5. Change owner and group of copied folders to `rabbitmq` (`chown -R rabbitmq:rabbitmq /opt/callrec/rabbitmq`)

6. Restart Rabbitmq

```
/etc/init.d/rabbitmq-server restart
```

7. Restart Call Recording

```
service callrec restart
```

8. Start making calls

Changing the AMQP Server Settings via the configuration file

To change the AMQP Server settings via the configuration file.

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

On the server running the configuration service.

```
File: core.xml      Line 112 Col 0      5186 bytes
<Group name="amqpServer">
  <Value name="ipaddress">192.168.110.129</Value>
  <Value name="port">5672</Value>
  <Value name="username">callrec</Value>
  <Value name="password">callrec</Value>
</Group>
<EqualGroup name="server">
  <Value name="name">core</Value>
  <Value name="port">30400</Value>
  <Value name="ipaddress">192.168.110.129</Value>
</EqualGroup>
<EqualGroup name="server">
  <Value name="name">keyManager</Value>
  <Value name="port">30401</Value>
  <Value name="ipaddress">192.168.110.129</Value>
</EqualGroup>
</SpecifiedConfiguration>
<SpecifiedConfiguration name="smtp">
  <Value name="smtpAddress">127.0.0.1</Value>
  <Value name="emailFrom">callrec@tstcr009.office.zoomint.com</Value>
</SpecifiedConfiguration>
</Configuration>
```

Figure 283: Editing the AMQP Settings via the Configuration File

Edit the IP address and port values.

Restart Call Recording to activate the changes.

```
service callrec restart
```

Troubleshooting AMQP

There are two tools included in Call Recording installation to see the current state of AMQP broker:

1. A web management plugin available by default on port 55672
2. Command line tool `rabbitmqctl`

Both tools provide information about the status of the AMQP broker, the connections, the RAM / HDD occupation, and the number of processed messages. Both tools can perform configuration tasks.

Taking into consideration the message flow schema and meaning of each queue, the status information about the AMQP broker, indicates potential problems between Core and Decoder and connected subsystems such as the file system and the database.

- An increasing number of messages in the `persistent.decoder.error.queue`, indicates that the database is unavailable.
- An increasing number of messages in the `decoder.request.queue` is indicates that the Decoder server cannot keep up with the number of incoming decoding requests or is completely down.

The command line tool `rabbitmqctl` a functional equivalent of the web interface for shell and provides all the information web interface does.

If the web management plugin is disabled, use `rabbitmq-plugins` the `enable rabbitmq_management` command to enable web interface. Keep in mind that access from remote machines might be blocked by a firewall.

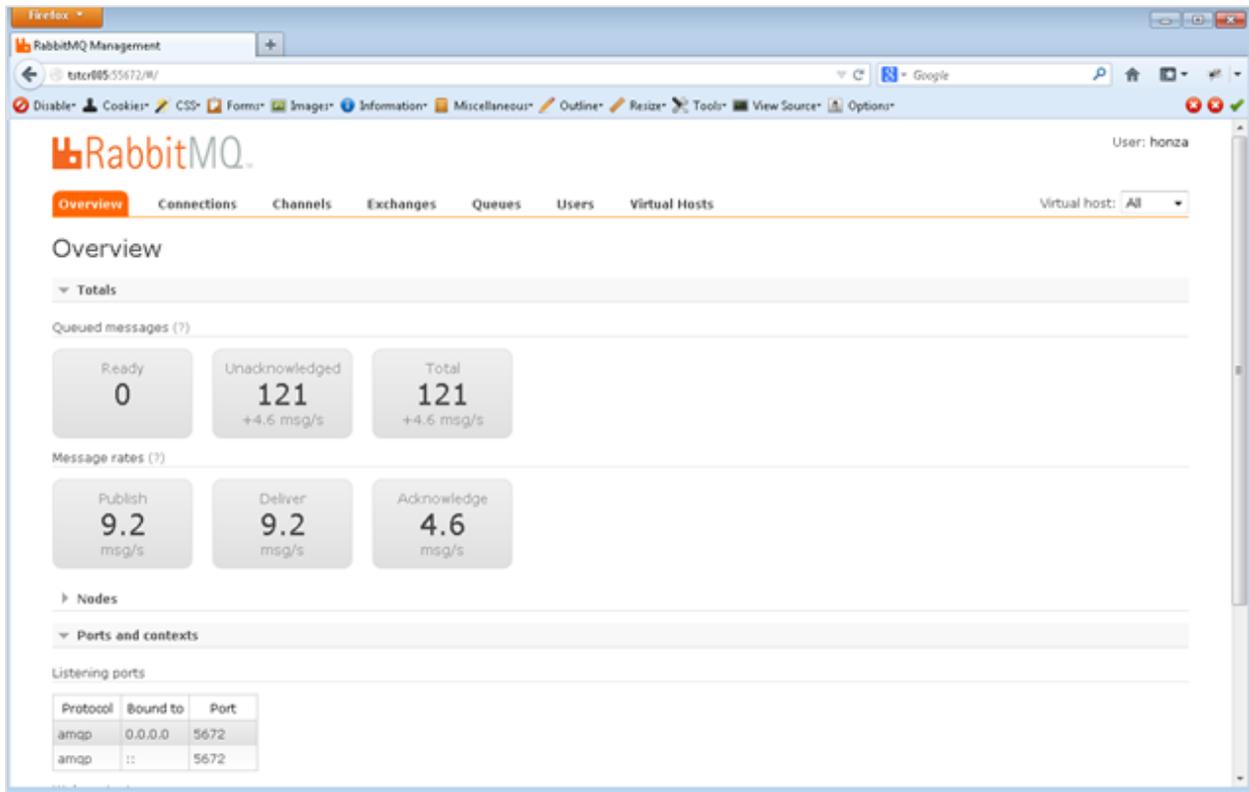


Figure 284: Web interface overview screen

An overview screen shows a basic overview about current situation for all queues together.

Overview				Messages			Message rates		
Name	Exclusive	Parameters	Status	Ready	Unacked	Total	Incoming	deliver / get	ack
decoder.error.queue		D	Idle	0	0	0			
decoder.request.queue		D	Idle	0	0	0			
decoder.response.queue		D	Idle	0	0	0			
email.decoder.error.queue		D	Idle	0	0	0			
email.decoder.response.queue		D	Idle	0	0	0			
media.removal.request.queue		D	Idle	0	0	0			
persistent.decoder.error.queue		D	Idle	0	0	0			
persistent.decoder.response.queue		D	Idle	0	0	0			
pre.decoder.request.queue		D	Idle	0	0	0			
repaircalls.decoder.request.queue		D	Idle	0	0	0			

Figure 285: Web interface queues screen

Queues screen shows state and amount of messages in each queue. From amount of messages in each queue and its trend can be seen Call Recording status. More information about web management interface can be found here:

<http://www.rabbitmq.com/management.html>

Typical Issues with Decoding performance

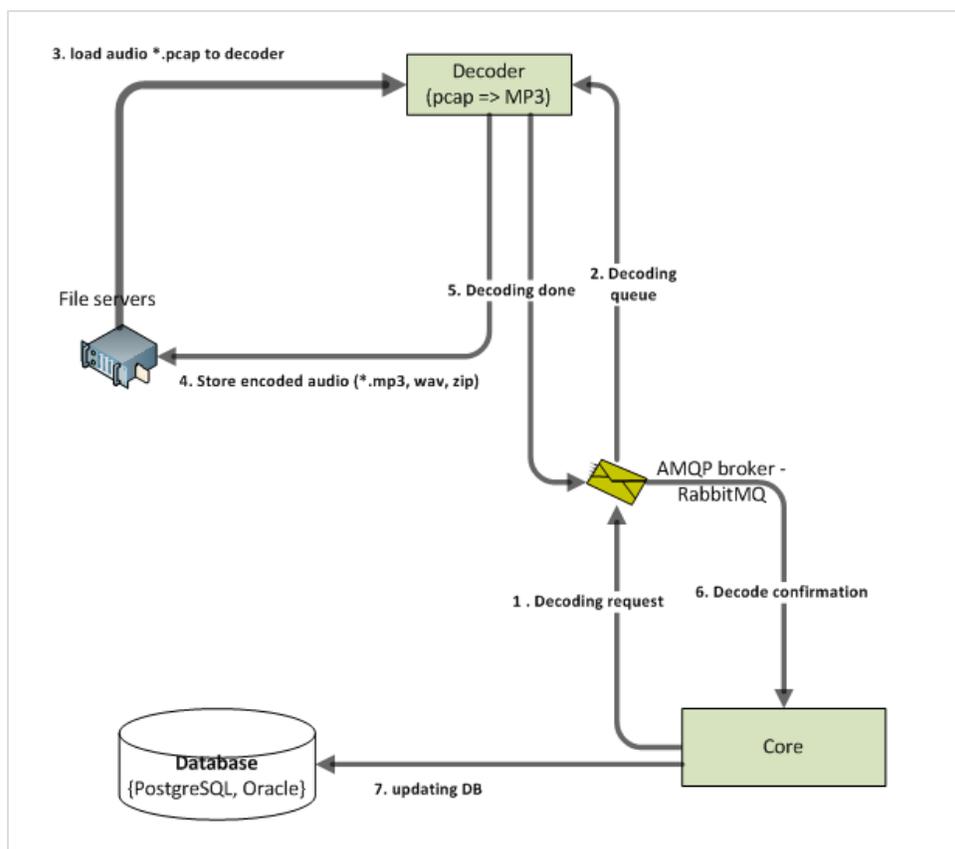


Figure 286: Data flow between Core and Decoder

In peak hours the Decoder may not be able to decode all the audio files in within acceptable delays. This can occur because of:

- Network bottlenecks (step 3 – loading PCAP files and step 4 – storing encoded audio files in),
- Decoder outage etc. Whatever the reason is, the consequence is disc space occupied by RabbitMQ queues grows (Call Recording uses persistent queues for Core – Decoder communication).

In environments that do not record twenty four hours a day the Decoder can decode all remaining files in the queue during off-peak hours. This can be

acceptable if the calls are not required in the web UI or Quality Manager immediately .

In environments that do record twenty four hours a day or if the Decoder server is too slow then decoding queue grow If decoding queue always grows and decoder server is fully loaded, upgrade the decoder server(s) to be able to process more audio files.

If decoding queue grows when the Decoders are not fully loaded, look at the network connection between decoders and file servers. PCAP files loaded to the Decoder are relatively large and the network bandwidth often appears to be a bottleneck.

Putting the Recorder and Decoder in one properly dimensioned server eliminates network bandwidth issues, because the Recorder mainly stresses the hard disks with write operations whereas the Decoder mainly stresses the CPU with read operations that are served from the cache. One server for the Recorder and Decoder containing RAID with battery backup caching significantly improves the number of available IOPS.

Typical Issues with Available Disk Space

If the `MNESIA_BASE` value points to the root file system (or on MS Windows environment to the C: drive), there is for typical configurations a risk (low disc space allocated for OS) all available space on this partition is consumed by AMQP persistent queues.



Chapter

39 **Known Issues**

This chapter details the known issues.

This chapter contains the following sections:

[Incorrect Handling of Hunt Lists in CUCM versions older than 8.0](#)

Incorrect Handling of Hunt Lists in CUCM versions older than 8.0

Hunt List recording in CUCM was (until recently) affected by an issue . The internal event model of the Hunt List caused incorrect processing of related calls if a particular call was processed by a Hunt List or if the target extension was a member of a Hunt List.

This issue was fixed in CUCM version 8.0. A new method for handling Hunt Lists has been introduced to ensure applications can correctly process related calls and retrieve detailed call information. Call Recording automatically enables this new functionality when Cisco UCM 8.0 or newer is detected. No manual changes in configuration are needed.

A call that has been targeted to a Hunt List is recorded as any other call. The calling extension (for instance, the customer) is saved as the calling number, while the Hunt List Pilot Number is saved as the called number. The extension number of the final Hunt List member who picked up the call (for instance the agent) is saved in External Data as the key: JTAPI_CALLED_TERMINAL_ADDRESS.

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.

