Genesys Quality Management 8.1

Call Recording Administration Guide

About Genesys

Genesys is the world's leading provider of customer service and contact center software - with more than 4,000 customers in 80 countries. Drawing on its more than 20 years of customer service innovation and experience, Genesys is uniquely positioned to help companies bring their people, insights and customer channels together to effectively drive today's customer conversation. Genesys software directs more than 100 million interactions every day, maximizing the value of customer engagement and differentiating the experience by driving personalization and multi-channel customer service - and extending customer service across the enterprise to optimize processes and the performance of customer-facing employees. 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 and the Genesys logo are registered trademarks of Genesys Telecommunications Laboratories, Inc. All other company names and logos may be trademarks or registered trademarks of their respective holders. © 2012 Genesys Telecommunications Laboratories, Inc. All rights reserved.

The Crystal monospace font is used by permission of Software Renovation Corporation, www.SoftwareRenovation.com.

Technical Support from VARs

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

Technical Support from Genesys

If you have purchased support directly from Genesys, please contact Genesys Technical Support. Before contacting technical support, please refer to the ***Genesys Care Program Guide*** for complete contact information and procedures.

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_ad_cr_10-2012_v8.1.501.00

Table of Contents

Chapter

1 Introduction

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

This chapter contains the following sections:

Document Purpose

The purpose of this document is to describe the post-implementation administration and configuration of the Genesys Call Recording software and describe the most important maintenance tasks for Administrators. For information about preparing your system for recording and for preimplementation tasks including installing an operating system please see Pre-implementation Guide. To install and configure Call Recording please seeImplementation Guide.

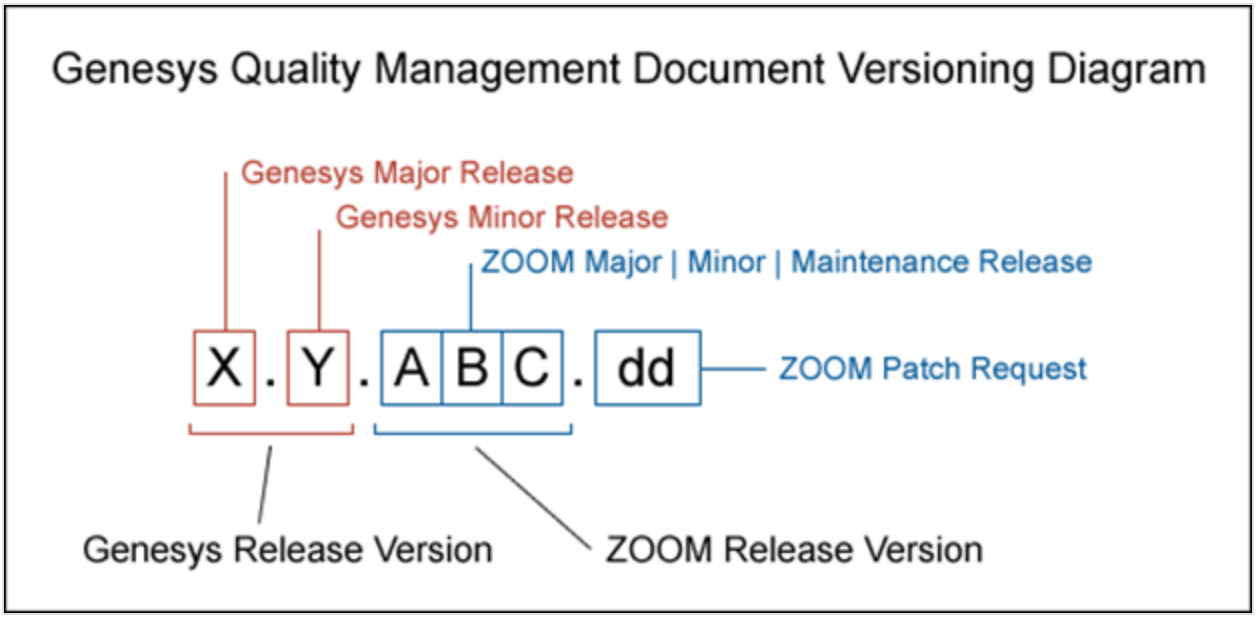
Audience

This document is intended for the technicians responsible for system administration and maintenance.

Document Version

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

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



Typographical Conventions

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

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

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

```
Code is placed on a gray background and bordered
```

Hyperlinks are shown in blue and underlined: http://genesyslab.com/support/contact.

Expected Knowledge

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

- Basic functionality of Genesys Call Recording system
- Knowledge of Red Hat Enterprise Linux or CentOS installation and configuration
- Unix-system 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.

Important:

Use Java 6 with *Internet Explorer* or use another Browser. There is a known issue with Java 7 which causes *Internet Explorer* to freeze.

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.You 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. You 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.

Important:

Use Safari or Firefox with Mac OS 10. There is a known issue with Chrome that causes problems with Universal player.

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 will affect the functionality, even if the server is in trusted sites (Internet Explorer only).

Technical Requirements for Playing Audio and Video Media

The following media players are recommended for successful video and audio playback. Please see the Screen Capture Administration Guide for more information about media player configuration.

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 Call Recording Licensing and Versions

This chapter covers product version information, licensing, and activation of GQM. Instructions on how to upload and activate a new license can also be found in the Implementation Guide.

This chapter contains the following sections:

Activating Call Recording

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

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

Important:

It is of utmost importance to activate your 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 will stop working.

To access your installation's licensing information once you have installed and started Call Recording

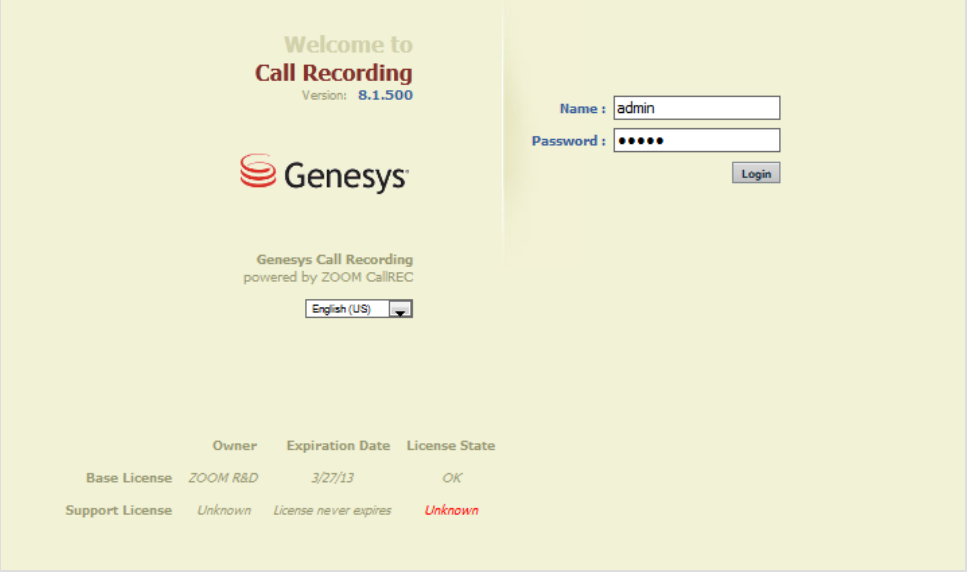


Figure 1: Log in for Activation

Open the Call Recording web interface. Log in as `admin` and enter the password. If this is the first login after installation, enter the default password: `admin`; you will be prompted to change your password.

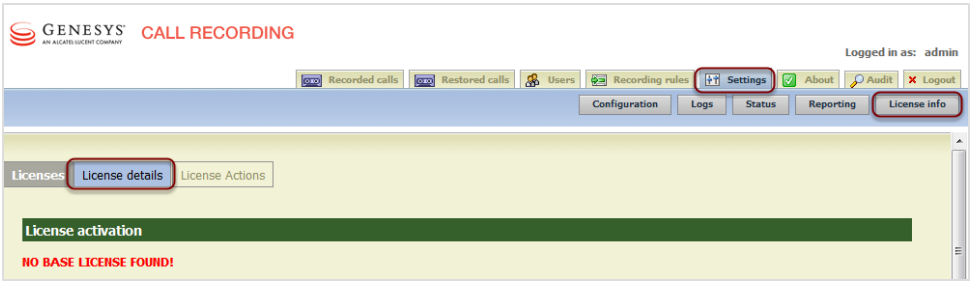


Figure 2: License Details

1. Open the **Settings** tab.
2. Click **License info**.
3. Click **License Detail**. The License activation form appears.

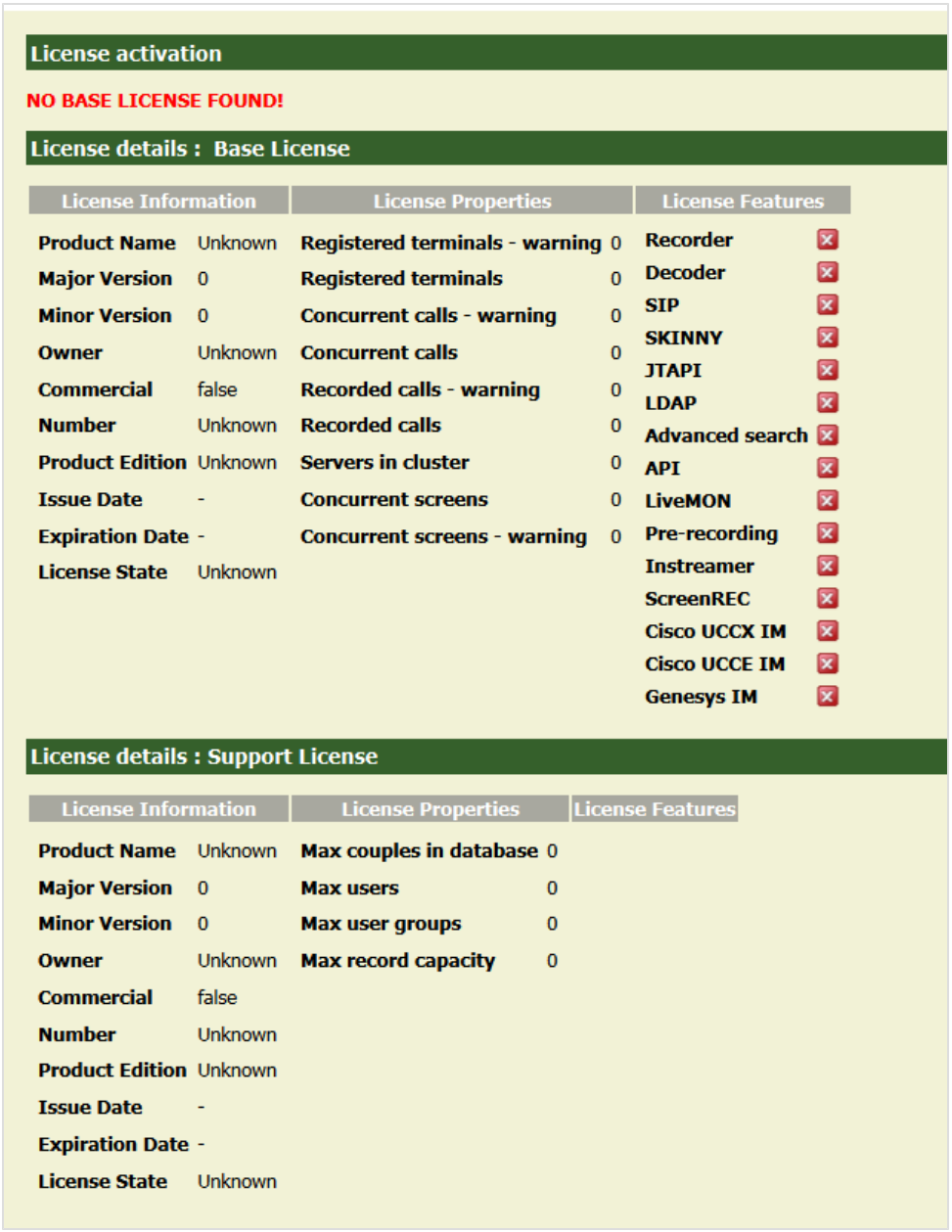


Figure 3: No Base License Found

Uploading the Un-Activated Call Recording License File

Genesys Support has sent you an email containing an un-activated license file named `callrec.license`. Save your un-activated license file on your local computer in a location that you will be able to find. Do not rename this file.

Important:
Call Recording will not record without a valid license file.

First you must upload your un-activated license file. This generates your unique license key, based on information including the MAC addresses of the NICs in the server. If you have to change these, then you will require a new license file. Please contact Support at the email address listed at http://genesyslab.com/support/contact.

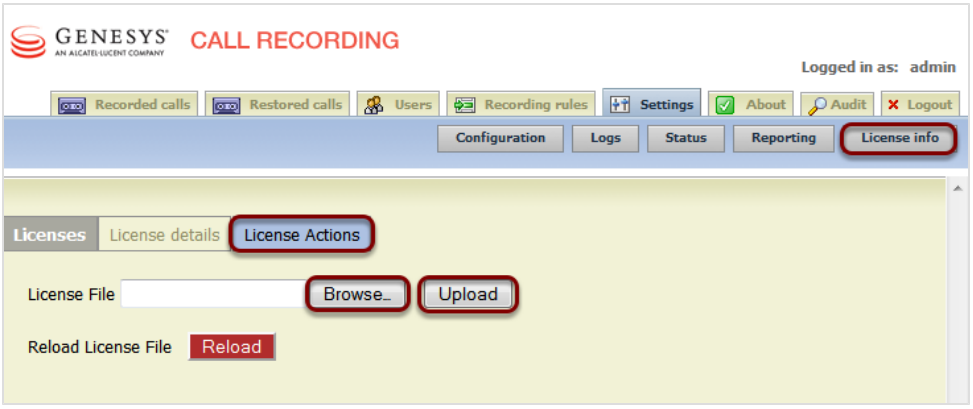


Figure 4: License actions dialog

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 un-activated license file on your local computer.
4. Click **Upload**.

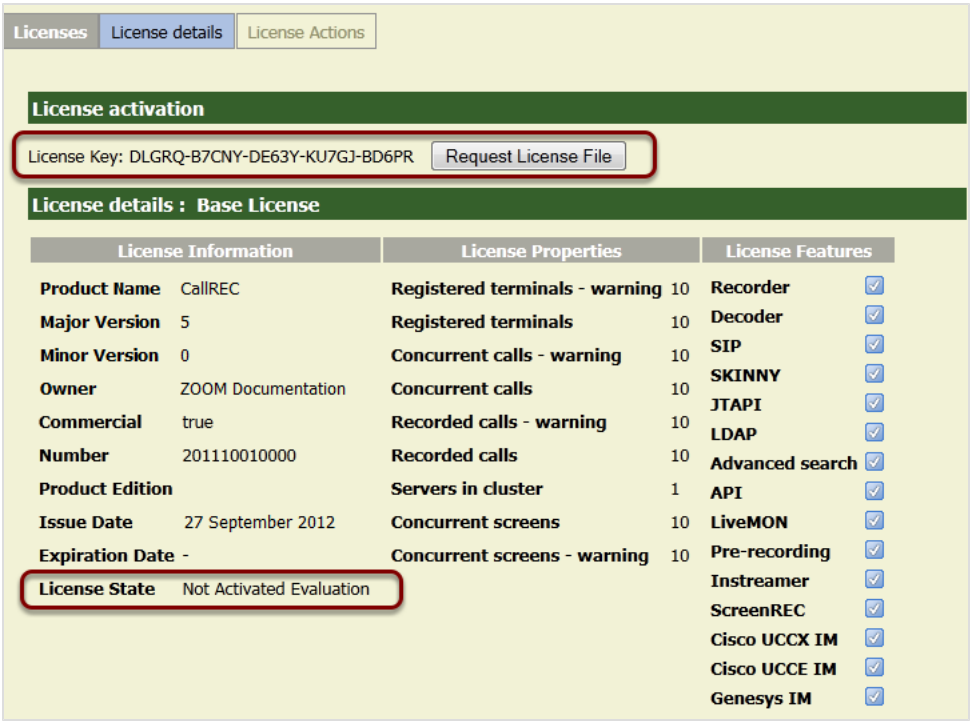


Figure 5: Un-Activated License

Once the license has been successfully uploaded:

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

Important:

If the system notifies you that you must reload your 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 you must upload a permanent activated license. You can get a permanent activated license file in two ways:

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 your 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 your complete license key. The key is required to generate your license file.

Genesys Support will send a permanent activated license file that corresponds to your system and purchase details. Save your activated license file on your local computer in a location that you will be able to find. Do not rename this file. The license file contains the parameters of your license, ensuring that all permitted features are properly activated.

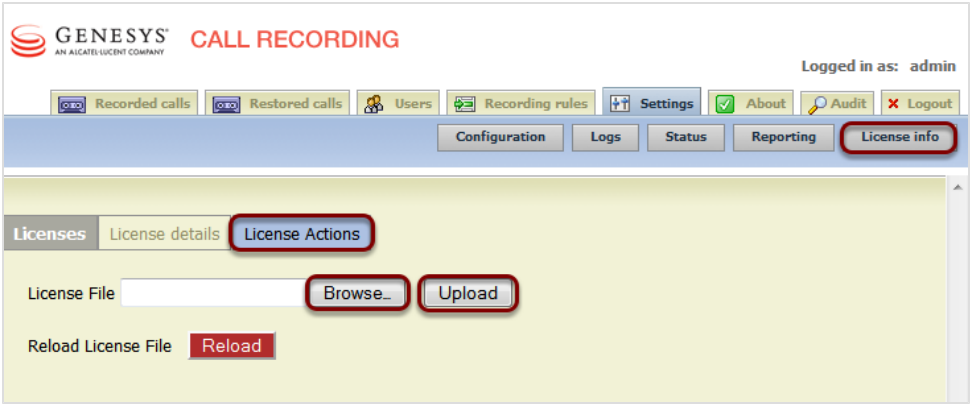


Figure 6: License Actions Dialog

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 on your local computer.
4. Click **Upload**.

Important:

If the system notifies you that you must reload your license file, follow the same procedure as above, and click **Reload.**

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

If you have a support License, repeat the process for the support license. The license file will be named `callrec-support.license`.

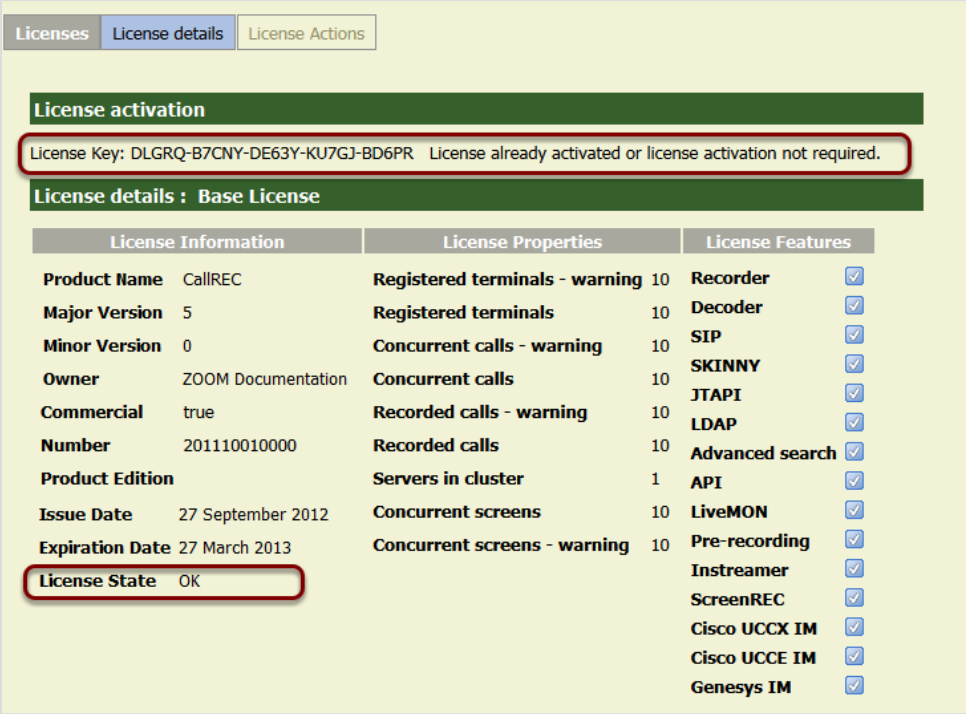


Figure 7: Activated Licence

Restarting Call Recording

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

Log in as `admin` and enter: `su -` to log in as the root user. Enter the password (default is: `zoomcallrec`).

Enter the following command:

```
service callrec restart
```

Call Recording will restart. This may take a few minutes.

Call Recording Version

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

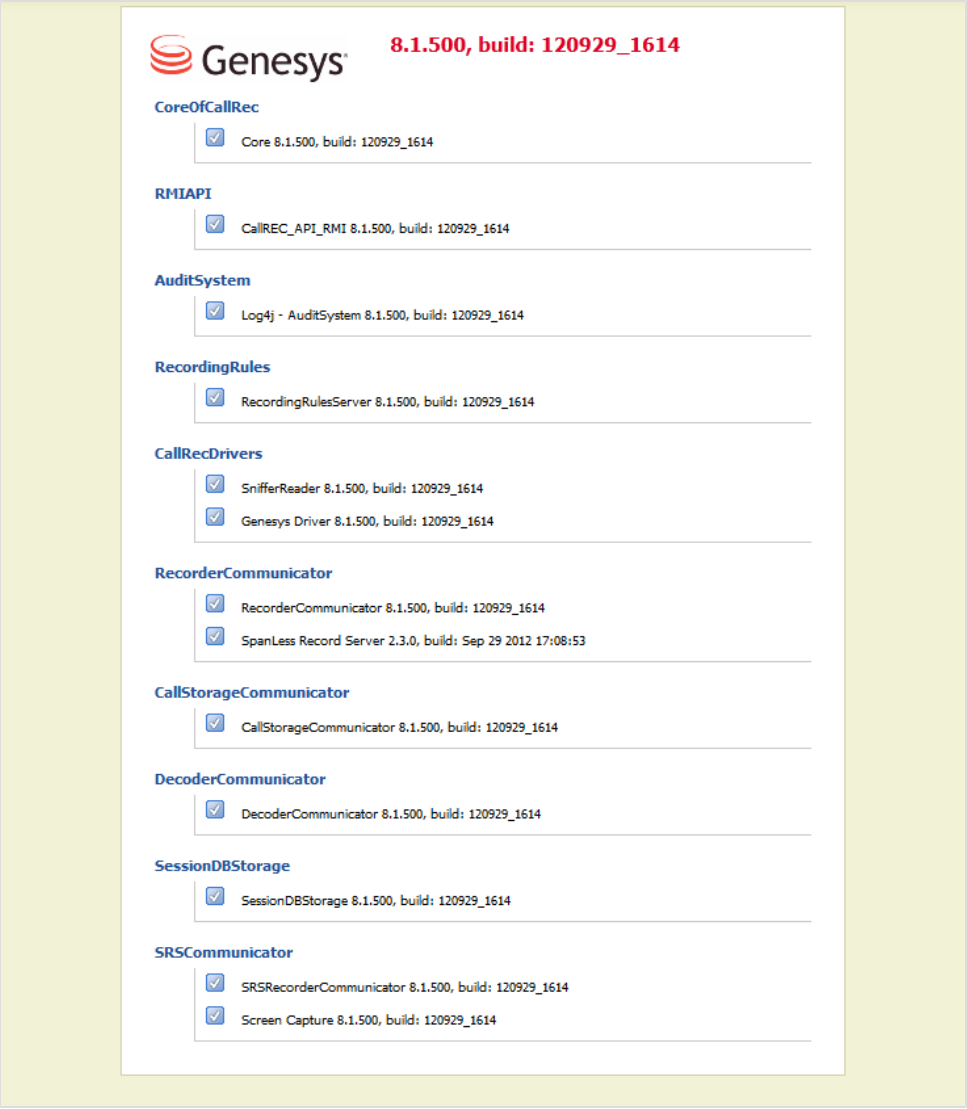


Figure 8: About Call Recording - Showing Current Call Recording Version and Version of Components

The information on the **About** tab can be especially helpful if you need to contact Genesys Support.

License Info

To access your installation's licensing information, open the **Settings** tab and click **License info**.

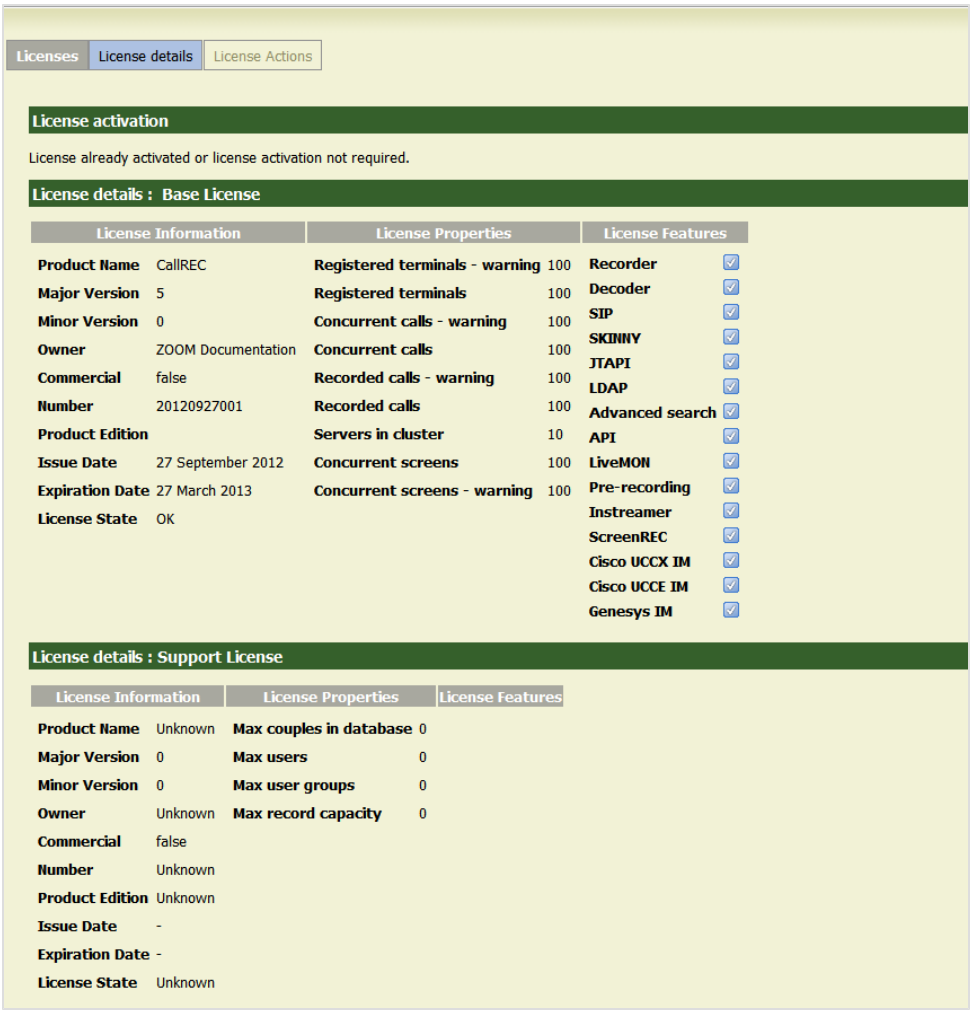


Figure 9: Example of License Info Screen from Fully Activated Call Recording 8.1.50x

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

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.

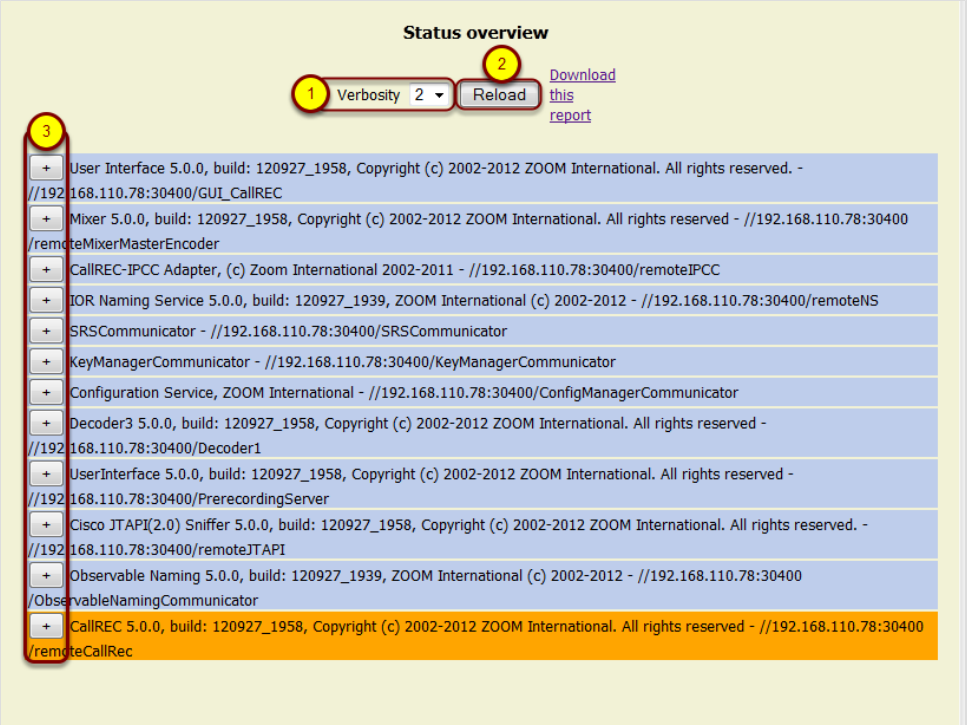


Figure 10: Example of Status Report

1. Select the required **Verbosity** (level of detail) from the dropdown list. Selecting a verbosity of 1 gives the least detail and selecting 5 gives 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 you about potential problems.

- A blue row indicates that the particular module is functioning 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 your 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. You must correct this parameter, and adjust it or fix it as needed.

3. Click **+** on that row to expand the view for that module and display the details. When you have finished viewing detailed information click **-** to collapse the list.

Chapter

3 Genesys Call Recording Administration GUI

When you log in as an administrator, you can perform administrative and maintenance on the Call Recording system.The configuration described in this manual is based on default settings.

This chapter contains the following sections:

Configuration

You can change Call Recording configuration settings using the Admin GUI.

Navigate to **Settings > Configuration**.

The **Servers** screen appears by default.

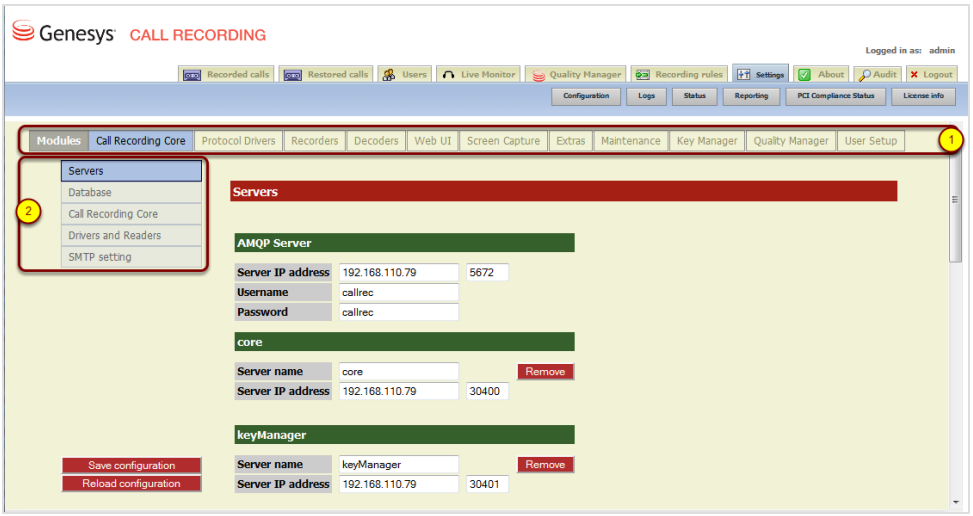


Figure 11: Call Recording Core Configuration Screen

1. Click on the navigation buttons at the top of the screen to reach a module to configure.
2. Click on an item in the list at the left to navigate to a particular setting screen.

Configuring Call Recording Core

Important:

Do NOT change the configuration of Call Recording Core unless you are a skilled administrator. In many cases, you will not need to modify these parameters if you are using a single server installation.

The main configuration of Call Recording core is set during the installation process and is essential for Call Recording functionality. Under the **Call Recording Core** tab you can change any of these parameters and also add a new server. Changing any of these settings may dramatically change your system performance.

Adding New Servers

Navigate to **Settings > Configuration >Call RecordingCore > Servers** and scroll down.

The **Servers** screen displays all installed servers and ports, including the Core and Key Manager servers. At the bottom of the list you can define aliases here that will be used in other configuration dialogs.

Figure 12: Servers Tab

To add a new server:

1. Type the **Server name**, **Server IP address** and **Port**.
2. Click **New**.
3. Click **Save configuration**

Important:
Each server name must be unique.

Displaying Database Pools

Navigate to **Settings > Configuration > Call RecordingCore > Database**.

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

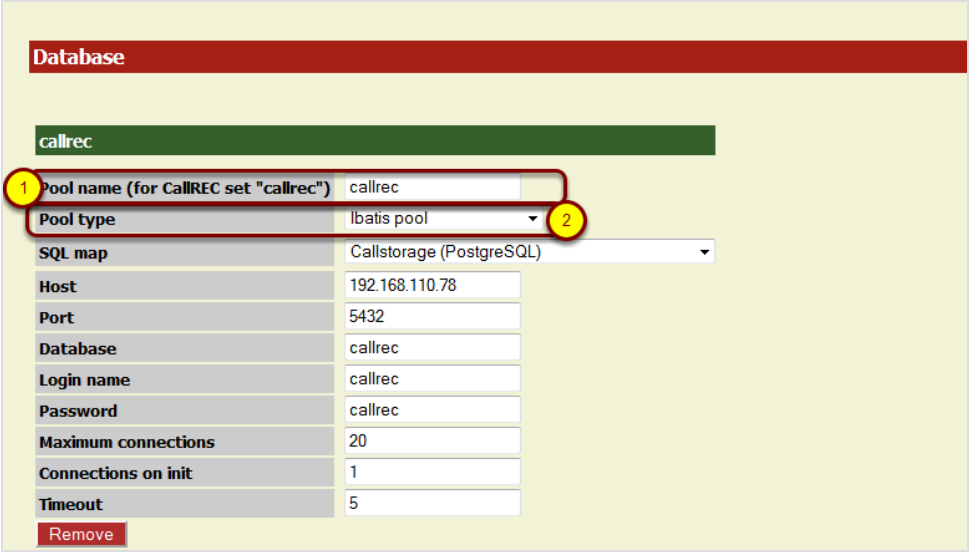


Figure 13: Database Tab

There can be multiple pools, according to your Call Recording settings, and 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 your Call Recording settings, in most cases this is set as **lbatis** pool.

Tip:

The Genesys Connection pool type is used only for special purposes. If selected, the Database driver selection appears instead of Sql map.

- **Sql map**: Allows you to select an XML description of the database structure. This setting is determined by the type of database you select – 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.

Tip:

If the User define option is selected in Sql map, then the option SQL map path appears and you can 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 RecordingCore > Database** scroll to the bottom.

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

Figure 14: Database Add New Pool

To add a new pool:

1. Type the **Pool name**.
2. Click **New**. The new pool is added.
3. Define all fields.
4. Click **Save configuration**.

Call Recording Core

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

The **Call Recording Core** screen allows you to set the registry address for the Application Communicator. You can also set the main core server in multi-site installations. In most cases you will select the same server alias from both dropdown menus.

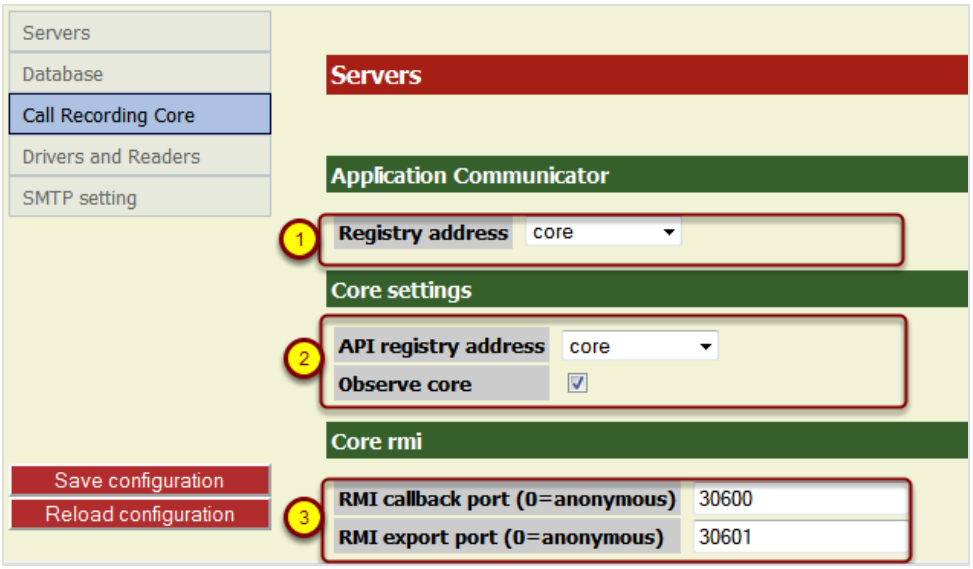


Figure 15: Call Recording CORE Settings

1. **Registry address**: Points to the server where your application communicator service is running (RMI service).
2. **API registry address**: Points to the Call Recording API (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.

Changing the SMTP Settings

Navigate to **Settings > Configuration > Call RecordingCore > SMTP Setting**.

The **SMTP setting** allows you to send Call Recording emails to users and administrators.

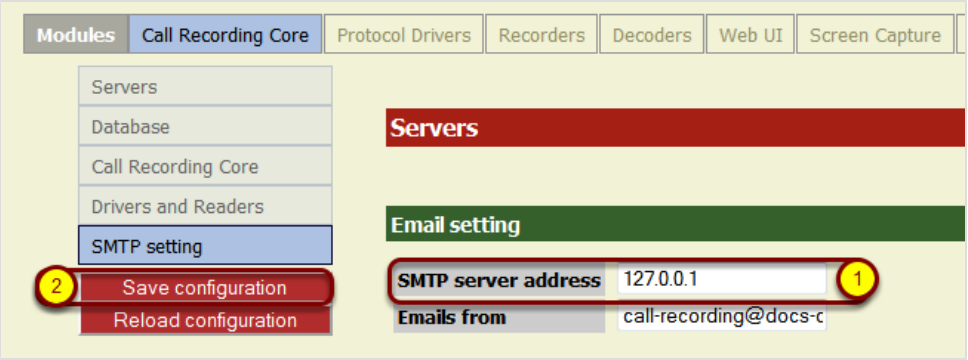


Figure 16: SMTP Settings

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 (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. Then you must restart the WebGUI with the following command.

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

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 an 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 Core.

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

JTAPI adapter

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

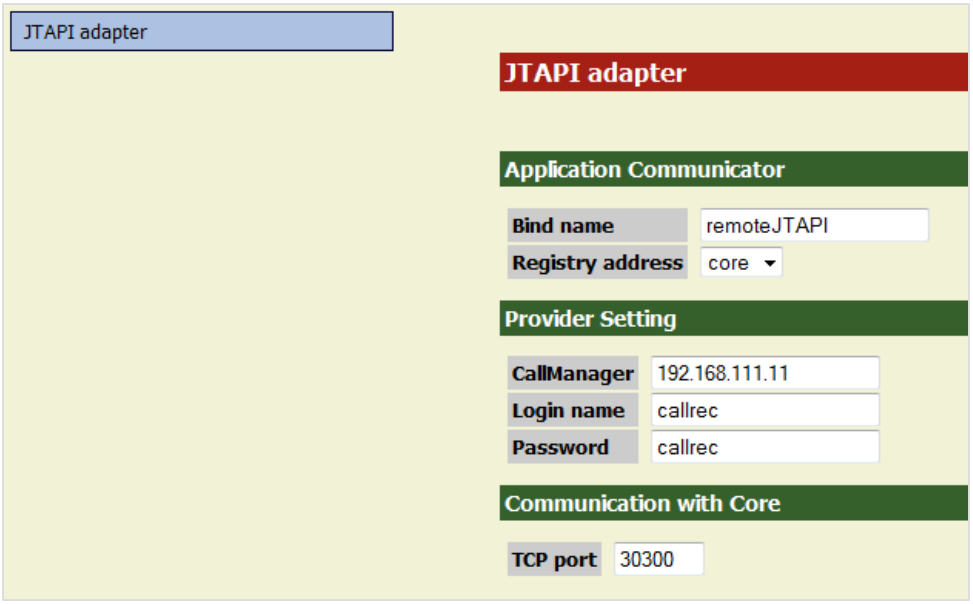


Figure 17: JTAPI Adapter Configuration

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 of your 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

Drivers and Readers for JTAPI Adapters

Navigate to **Settings > Configuration > Call RecordingCore > Drivers and Readers**

Drivers and readers are configured during installation. In most cases 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 you use more protocol adapters, for example, if you need to listen on more network interfaces then you must create more readers.

Ensure that all readers are configured properly:

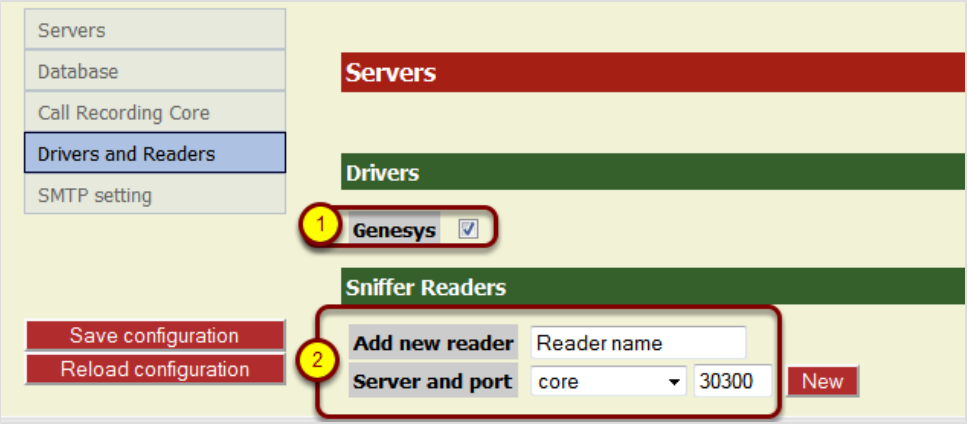


Figure 18: Drivers and Readers

1. Select the appropriate checkbox to enable the appropriate Driver for the Protocol Adapter. If a driver is disabled the particular signaling protocol will not be processed, regardless of the Protocol Adapter settings.
2. Type unique name for the reader, select the correct server from the dropdown 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.

Genesys Driver

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

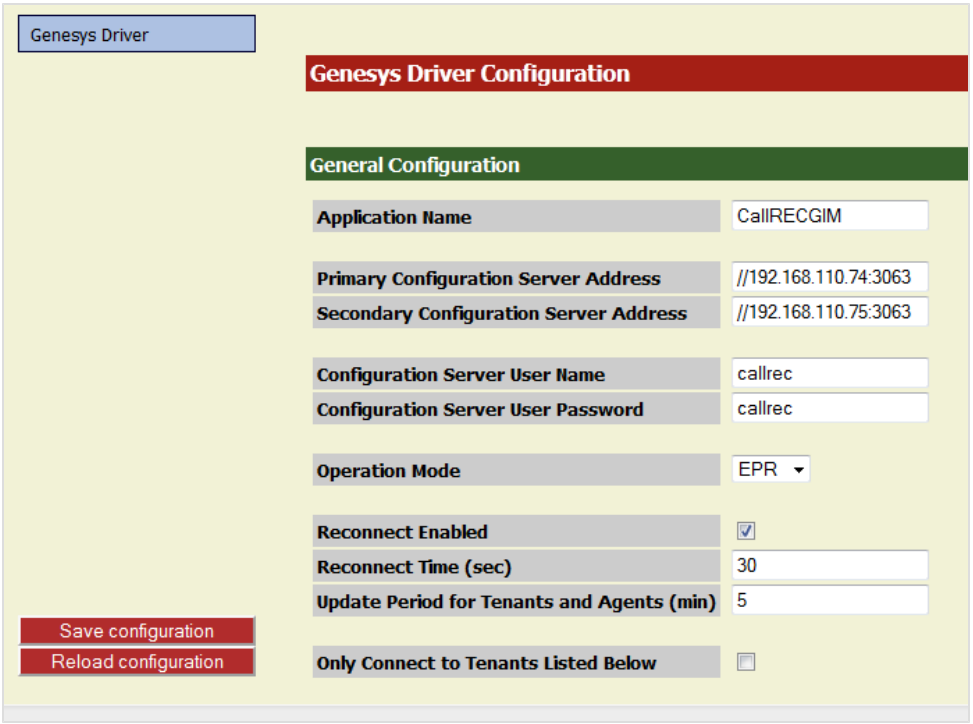


Figure 19: EPR Configuration in Call Recording Web GUI

Select the Operational Mode **EPR** or **MSR**.

Select the Checkbox **Reconnect Enabled**.

Type the **Reconnect Time** in seconds.

Set the **Update Period for Tenants and Agents (min)**.

For full details of how to configure Genesys Driver refer to the Configuring EPR and MSR for Recording section in the Implementation Guide and Genesys Active Recording Ecosystem documents.

Avaya Driver

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

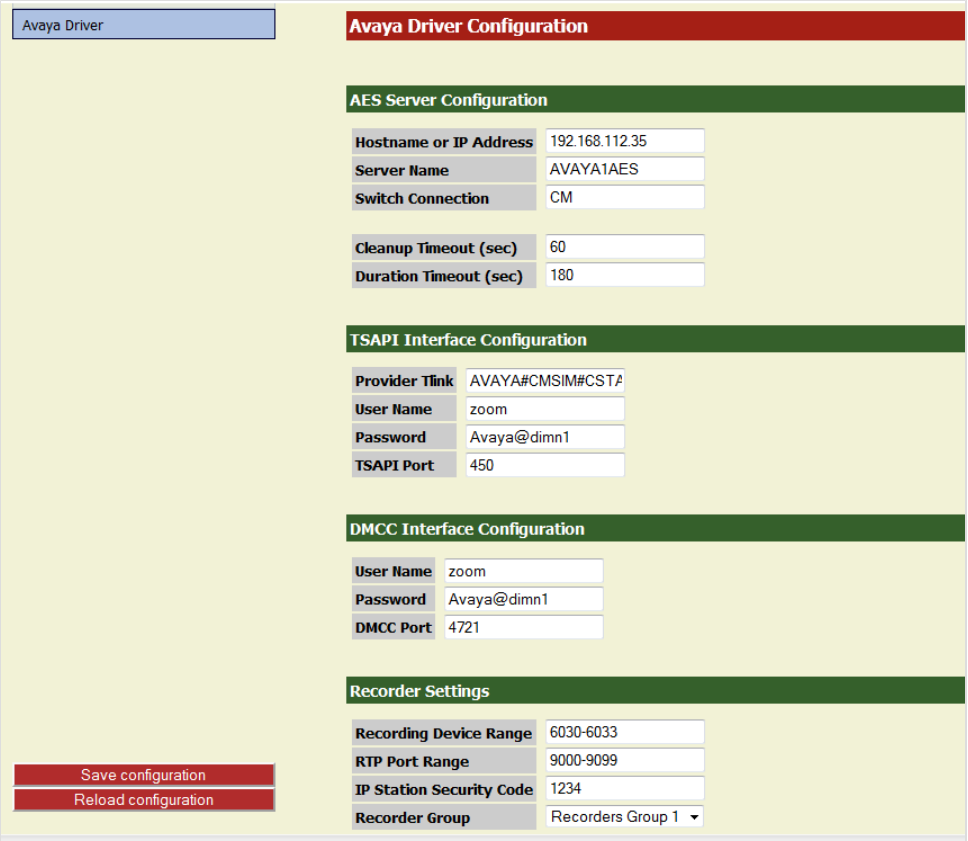


Figure 20: Avaya Configuration

For full details please refer to the Configuring Avaya section in the Implementation Guide and Avaya Whitepaper documents.

Recorders

The **Recorders** tab contains connection settings for all recorder servers used by your Call Recording system.

Record Server Communicator

Navigate to **Settings > Configuration > Recorders**

You can add or remove Recording servers here. For every recorder you need to choose a unique Recorder name.

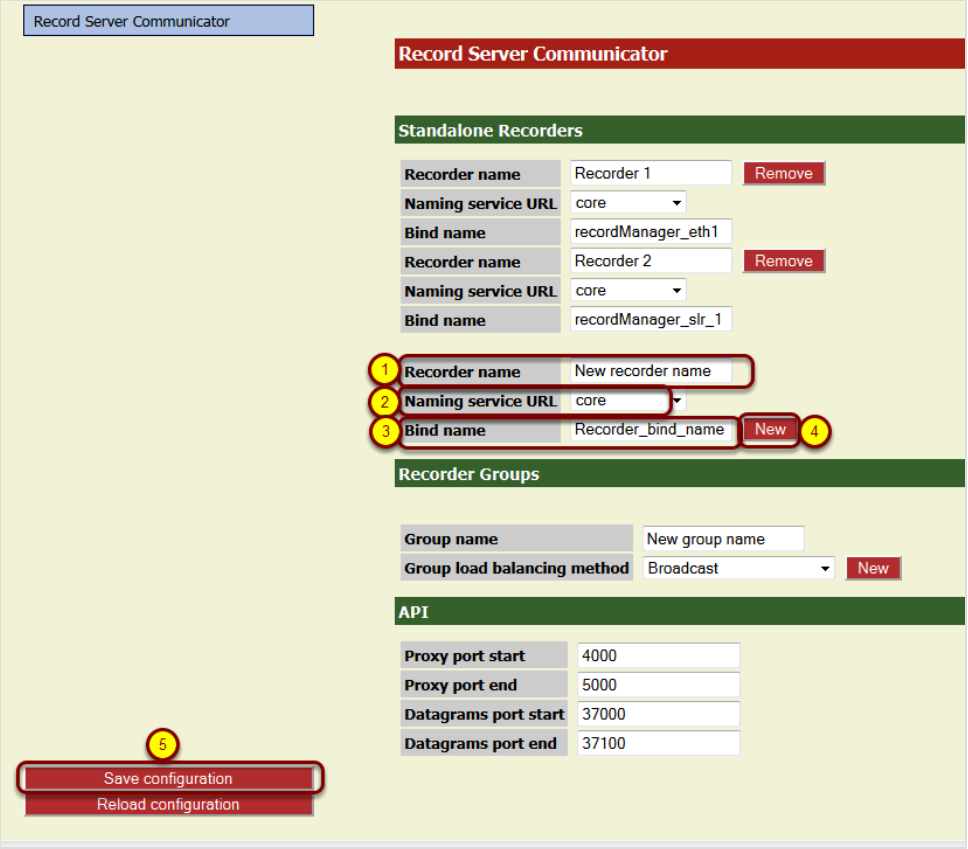


Figure 21: Recorder Server Communicator

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**.

Important:

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

Decoders

The **Decoders** tab allows you to identify the decoder servers and configure decoding parameters.

Configuring Decoders

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.

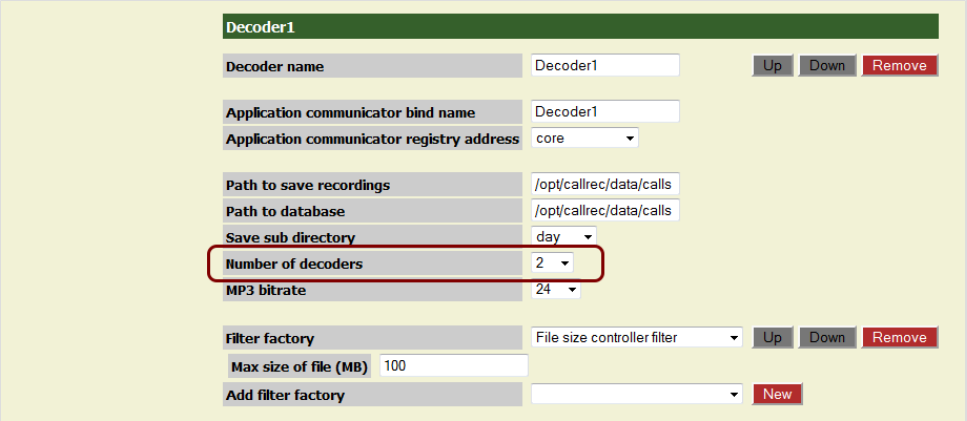


Figure 22: Decoder 1

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:

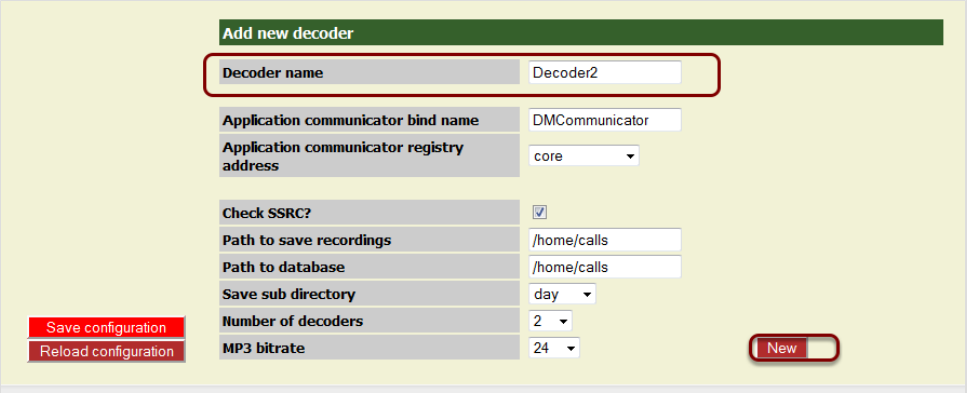


Figure 23: Adding a Decoder

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.

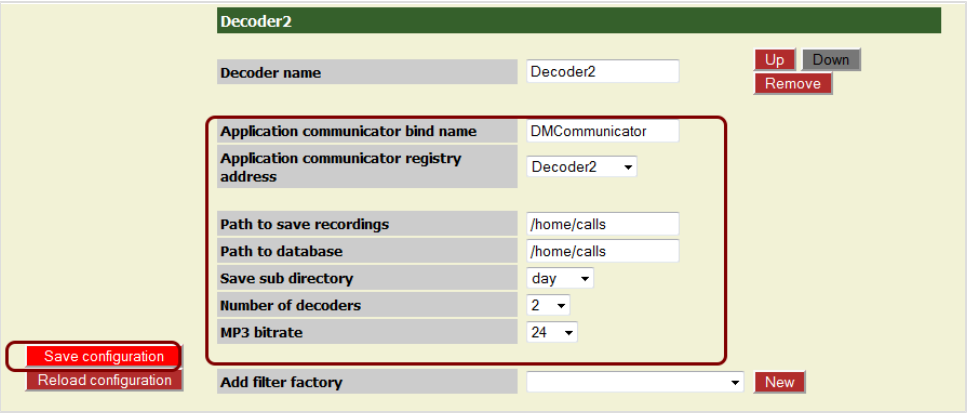


Figure 24: Decoder2

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 dropdown menu. 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 thePath for storing database entries – 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. You can change the quality settings to minimize storage space, or maximize audio quality.

Audio Gain Settings for the Decoder

Where 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 (normal gain). One step in value equals +- 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 will be affected.

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 1: 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.

Decoder Server Communicator

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

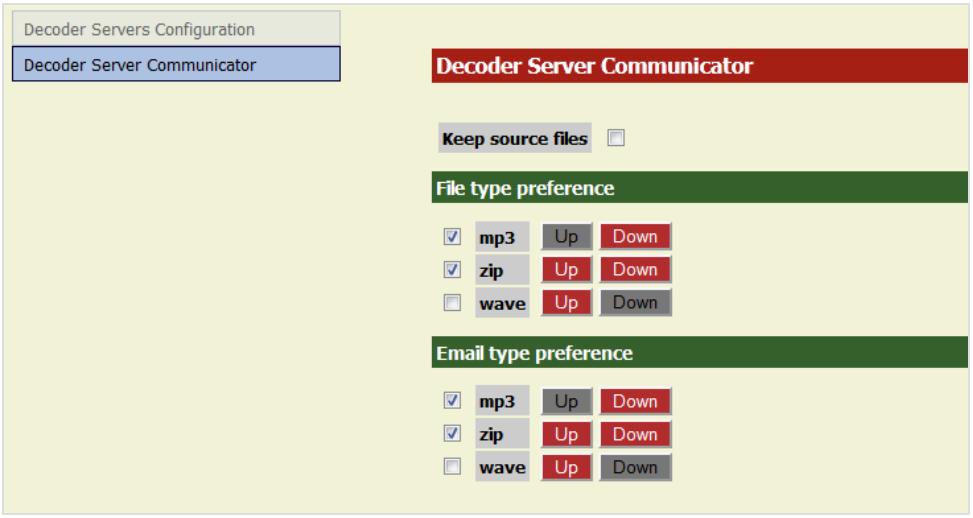


Figure 25: Decoder Server Communicator Settings

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 you deselect a format, this file type will not be available.

Important:

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

Web UI - Web Interface Administration

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

Call Recording uses the web browser for the user interface. Web Interface Administration allows you to change the settings of the web interface.

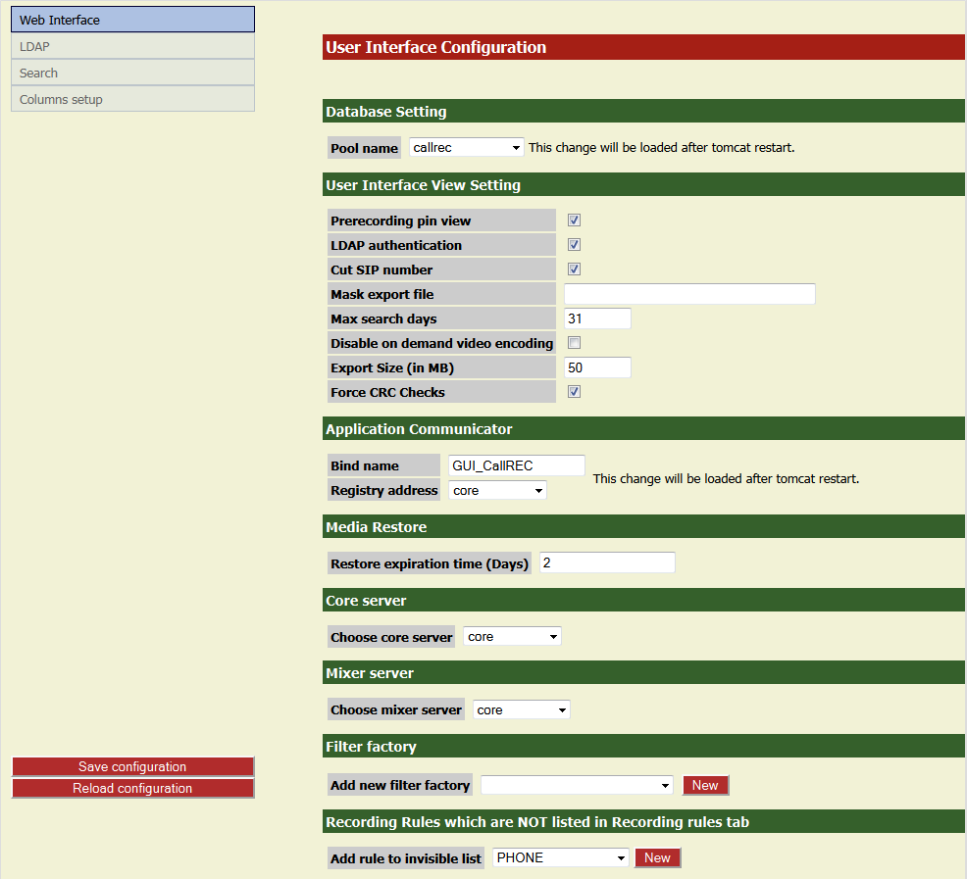


Figure 26: Web Interface Configuration

Important:

If you change the Pool name or Bind name you must restart your Tomcat web server.

User Interface Configuration

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

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

Database and User Interface settings

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

In most cases, you do NOT need to change the Pool name. The default is “callrec”.

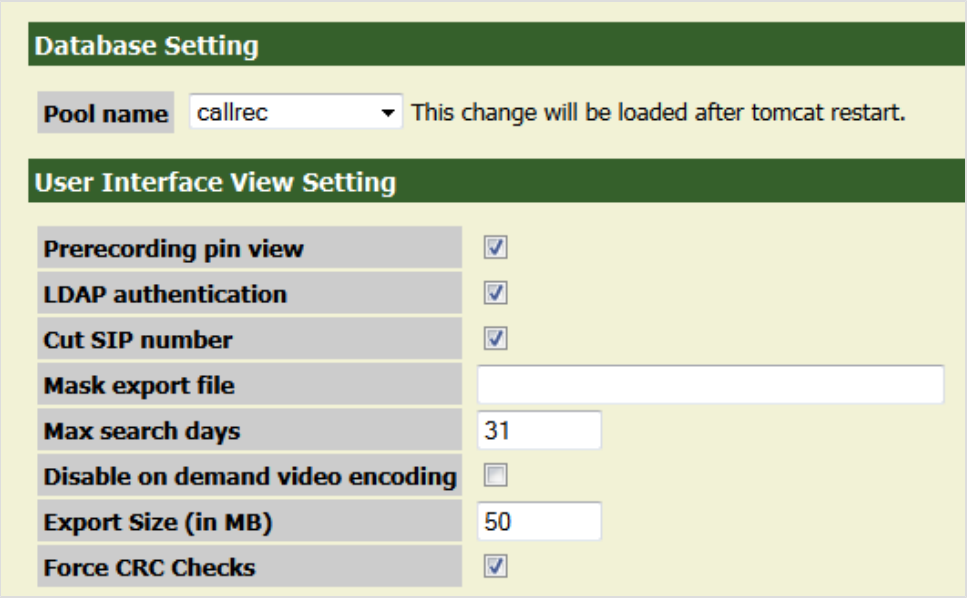


Figure 27: DB and User Interface View Settings

The Pool name drop down list shows 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 are displayed in the user interface:

- **Prerecording pin view** – Show pre-recorded calls with a special icon that looks like a pin.
- **LDAP authentication** – Use LDAP to authenticate users.

Important:

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 will 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. Disabling this feature will still allow the Media Encoder to work in batch mode, improving overall performance.

Export Size (in MB): For customers wishing 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 will be displayed, and the file will not be played. 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** scroll down.

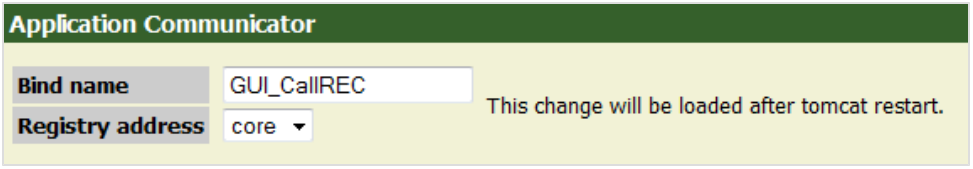


Figure 28: Application Communicator Settings

The Application Communicator contains RMI bind options. Changing the Bind name or Registry address requires restarting your 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** 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.

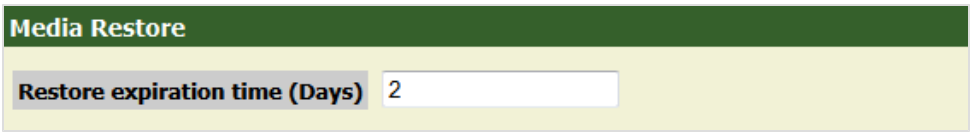


Figure 29: Media Restore Settings

Core server

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

Figure 30: Core Server Settings

- Choose core server – allows you to change 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** scroll down.

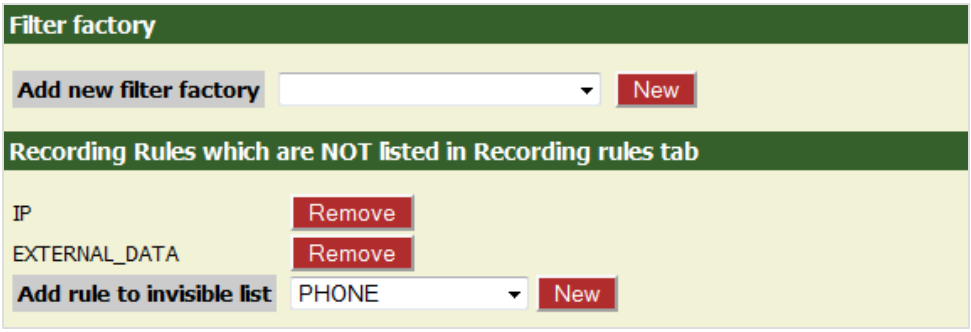


Figure 31: Filter Factory Settings

The Filter factory allows you to predefine 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 which 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.

Important:
This does not affect pre-existing rules.

Password Configuration

Navigate to **Settings > Configuration > Web UI > Web Interface** Scroll to bottom

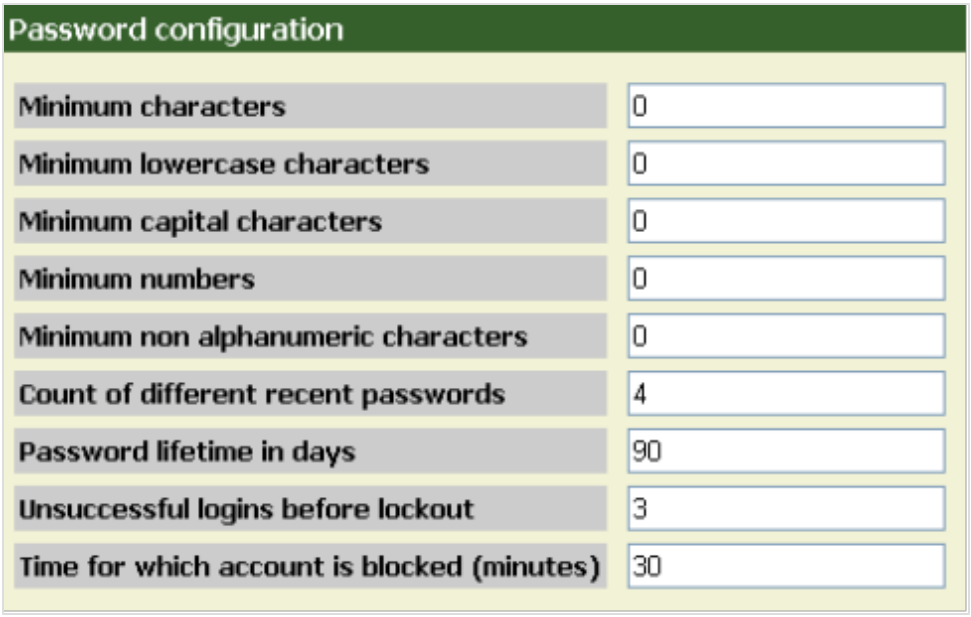


Figure 32: Password configuration

One of the most important sections on this configuration tab is **Password configuration**. The security of your Call Recording system can be improved (or alternatively degraded) by settings here. For a secure password policy, ensure you 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)

Setting	Description	Values
Minimum lowercase characters		
Minimum capital letters		
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 2: Password Properties

Enabling LDAP Authentication

LDAP Configuration allows you to identify and enable one or more LDAP servers, and Group Filtering.

You must enable LDAP Authentication before you can configure the settings in LDAP Configuration.

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

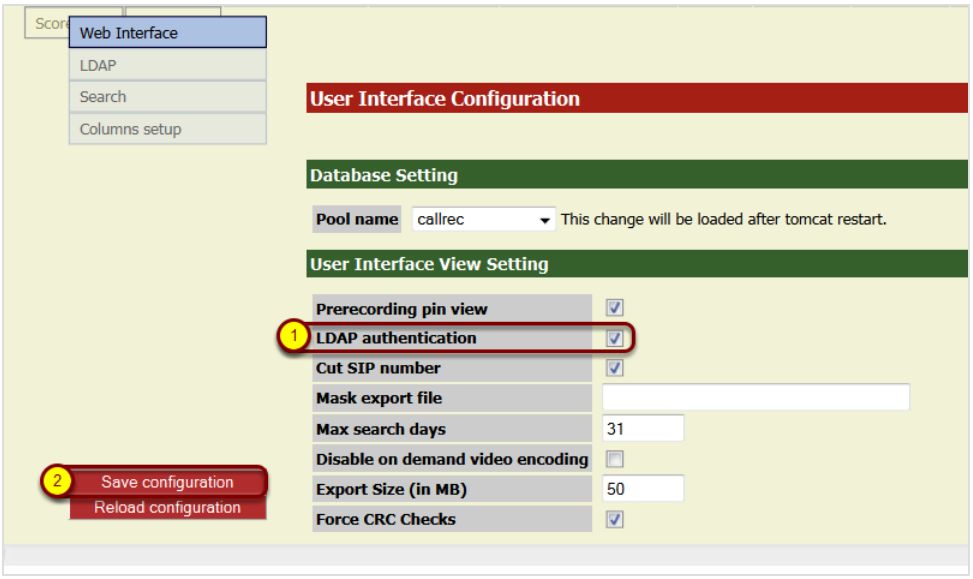


Figure 33: Enable LDAP Authentication

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

For more information concerning LDAP integration, configuration and maintenance please contact Genesys Support at http://genesyslab.com/support/contact.

LDAP Configuration

Navigate to **Settings > Configuration > Web UI > LDAP > LDAP Configuration**

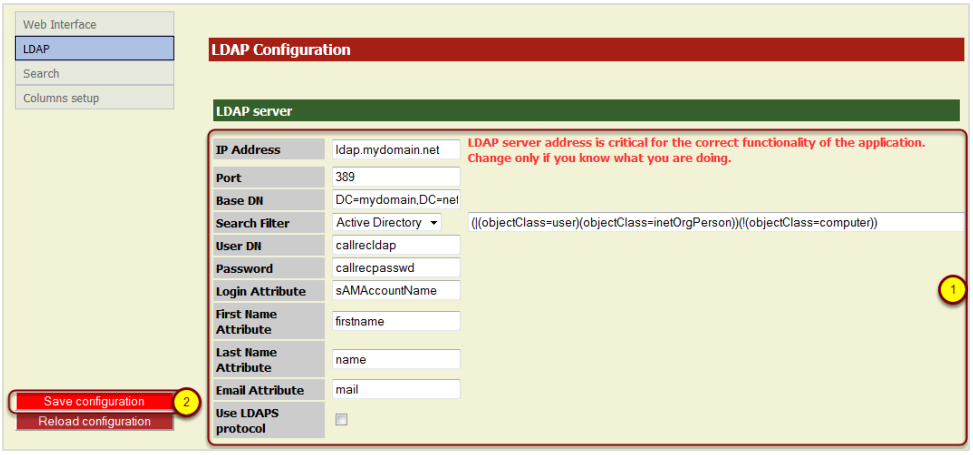


Figure 34: LDAP Configuration

1. Configure all settings according your LDAP server configuration.
2. Click **Save configuration**.

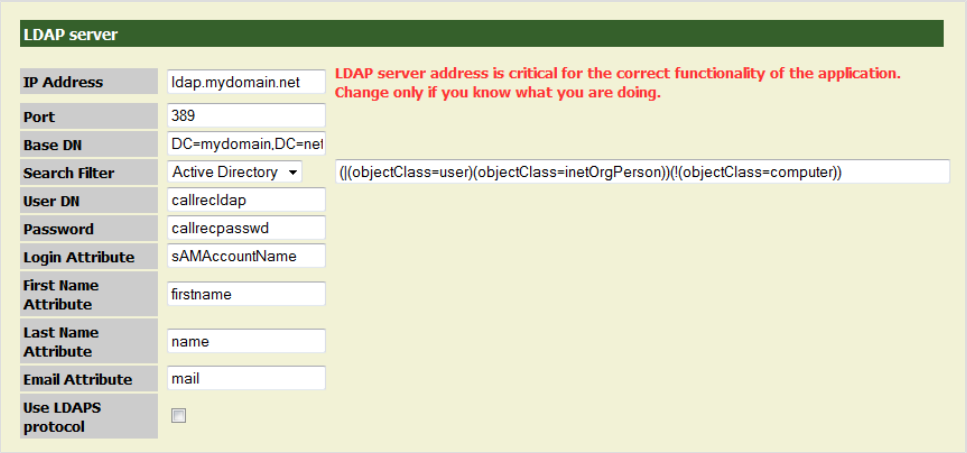
Settings are divided into two groups and you can also define Backup LDAP server. The **LDAP server** sectionis compulsory, in Group filtering is possible to enable this feature, but you may leave it unchanged – if you don't plan to use group filtering (will be explained later in text).

LDAP user account

You will also need to create user account for accessing LDAP data from Call Recording. It is not recommended to use user account with full access rights. Instead full access is better to grant read-only rights to newly created account.

This LDAP connection is used only for initial importing of users into Call Recording.

LDAP server:



LDAP ID

- **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 will lead to disabling LDAP authentication.

- **Port**: Port number for connection with your 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 dropdown. The choices are Active Directory, Open LDAP or Custom LDAP. The field on the right hand side allows you to modify the filter.
- **User DN**: User ID access into LDAP database – listing of users – Case sensitive.
- **Password**: Password of user – Case sensitive.
- **Login Attribute**: Name of LDAP key with user's login name.
- **First Name Attribute**: Name of LDAP key with user's first name.
- **Last Name Attribute**: Name of LDAP key with user's last name.
- **Email Attribute**: Name of LDAP key with user's email address.
- **Use LDAPS protocol**: Enable the LDAP over SSL protocol. See the Security Guide for more information.

Tip:

Typical key values for Microsoft Active Directory are as follows:
First Name Attribute = `givenName`
Last Name Attribute = `sn`

Group filtering:

- Click **New** to add additional filters.
- Use the **Up** and **Down** buttons to change the order of multiple filters.

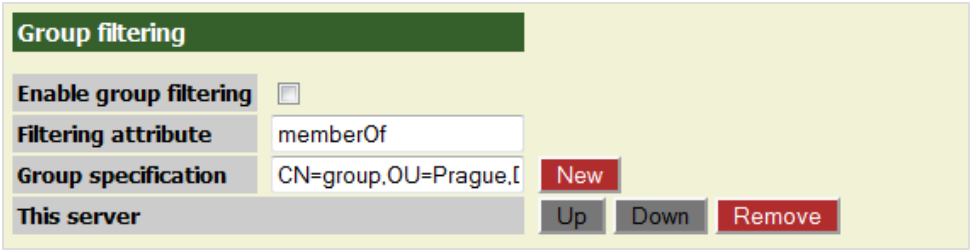


Figure 35: Group Filtering

- **Enable group filtering**: Check this 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:

Select only staff from Prague's call center. The common name is Prague, which 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** scroll down.

To add or edit the configuration of a backup LDAP server, follow the same steps as above.

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 your backup LDAP configuration.

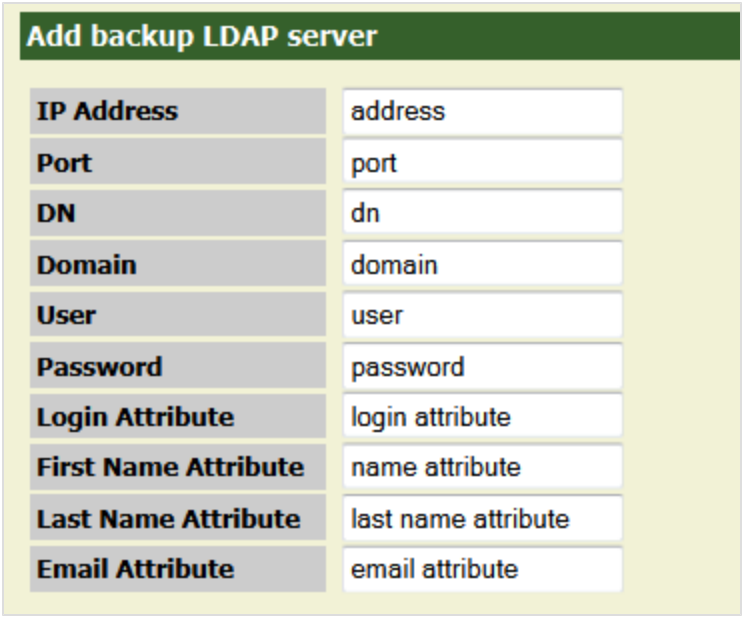


Figure 36: Add Back up LDAP Server

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

Adding LDAP users

When LDAP is configured correctly and your LDAP directory is running, you can import users (according to the entered criteria) into Call Recording. The import process will add into Call Recording database only user names and emails and password will be checked against the LDAP on every login. The following flowchart demonstrates the user authentication process.

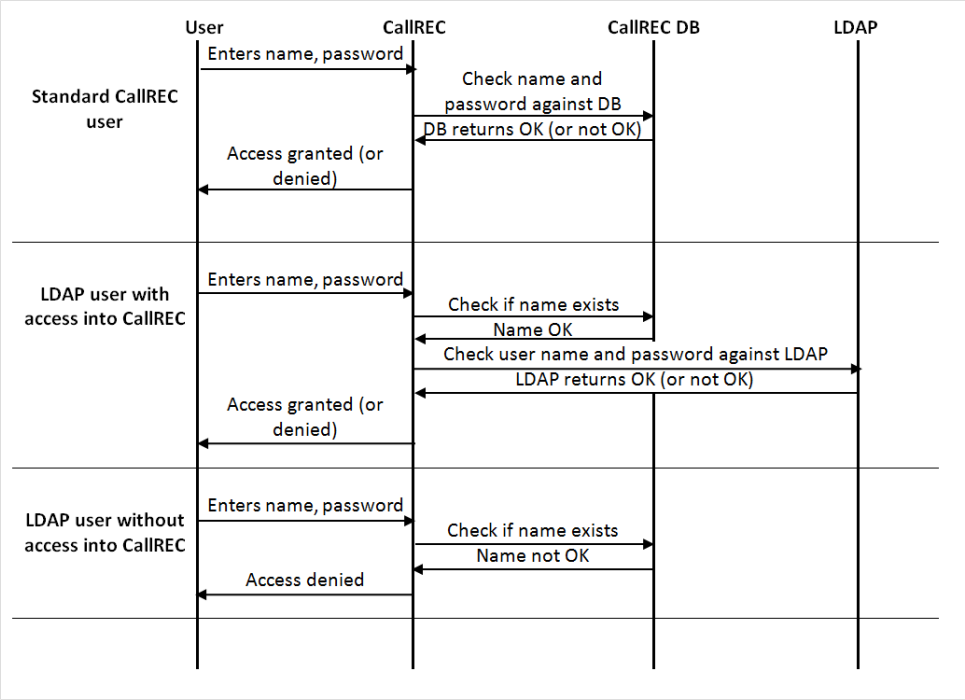


Figure 37: LDAP Add User Flow Chart

Importing LDAP users

To import users from LDAP, login into the Call Recording web interface and navigate to the **Users** tab. Here select a group or create new group for all LDAP users (according to the defined group filter etc.) and click **Insert new user**.

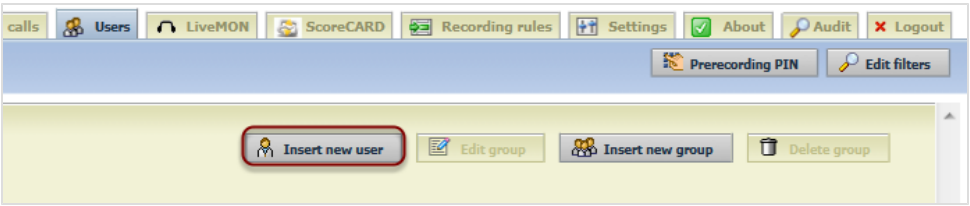


Figure 38: Insert New User Button in Users Tab

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).

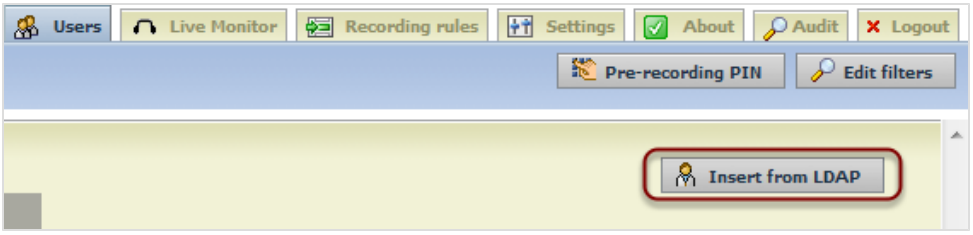


Figure 39: Insert from LDAP Button on Add User Page

In the **Insert LDAP user** list all LDAP users corresponding with the criteria entered in the configuration and you can select users for import.

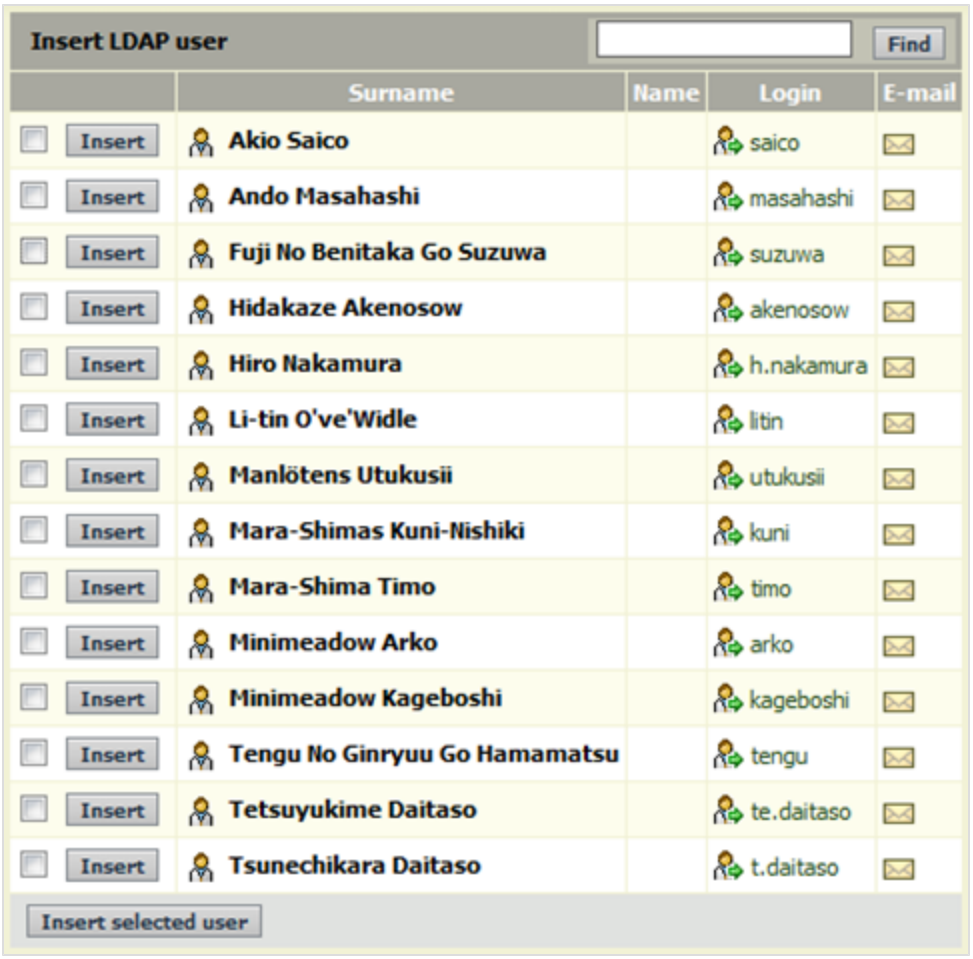


Figure 40: LDAP Users List

Users will be imported into the group currently open in Call Recording.

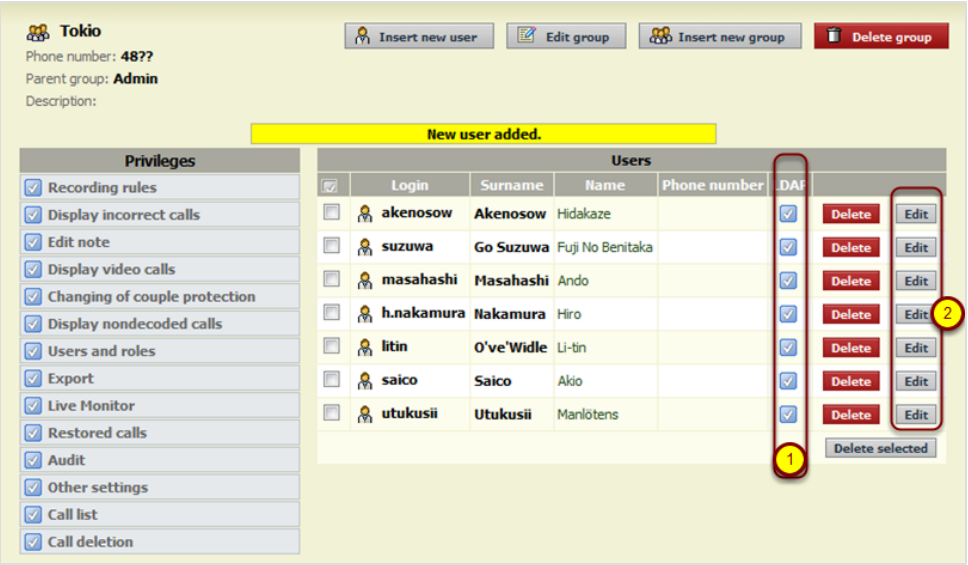


Figure 41: Newly Imported Users from LDAP

1. All imported users are marked with an LDAP user check-box on their User details page. If you uncheck the LDAP user check-box, the user will be no longer authorized against LDAP and will become 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 (therefore, if you want to change password for this user, you must change the password in LDAP).

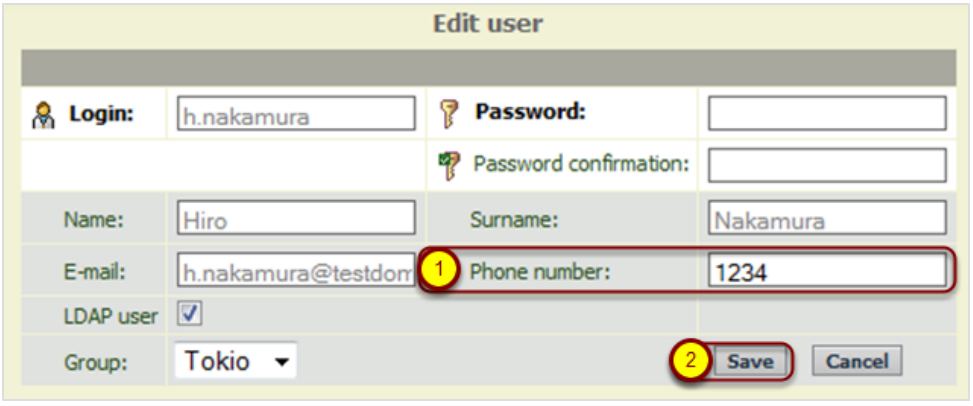


Figure 42: LDAP Imported User Detail

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

2. Click **Save**.

Advanced Search Setup

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

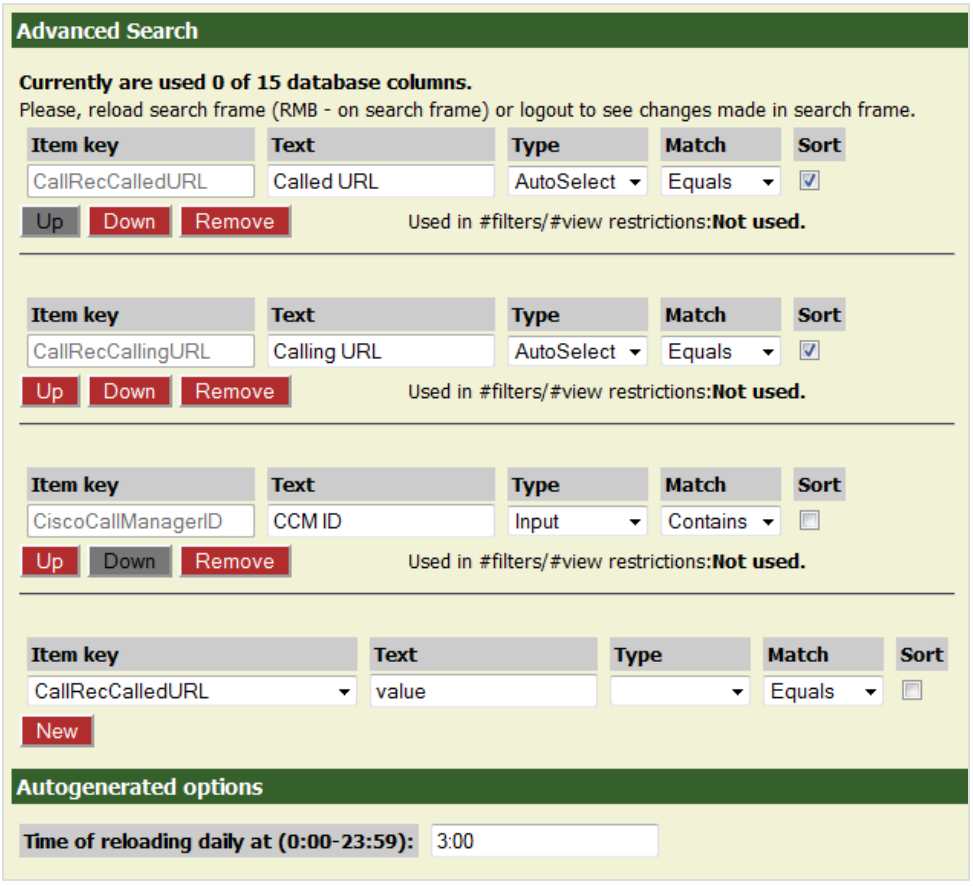


Figure 43: Advanced Search Definition

You can use up to 15 external data keys as advanced search criteria. The Advanced Search functionality allows you to set up and save common database searches, so they are available to your users in the web interface. The searches can be defined using any Call Recording external data, including data from Genesys Contact Center, or your own 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** dropdown list. Item key dropdown lists are re-generated once per day and entered into Auto-generated options.

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

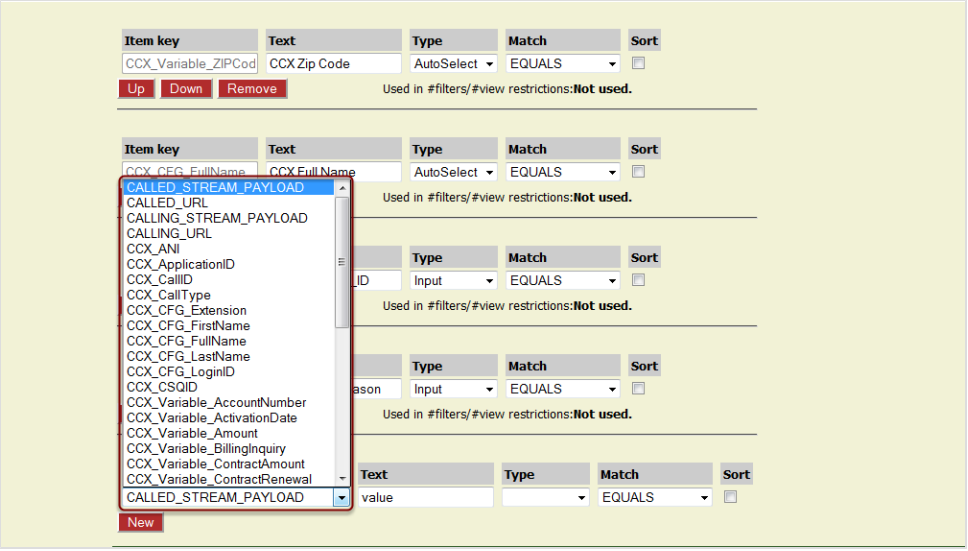
Important:

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

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



Selecting Data for Search Dropdown

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

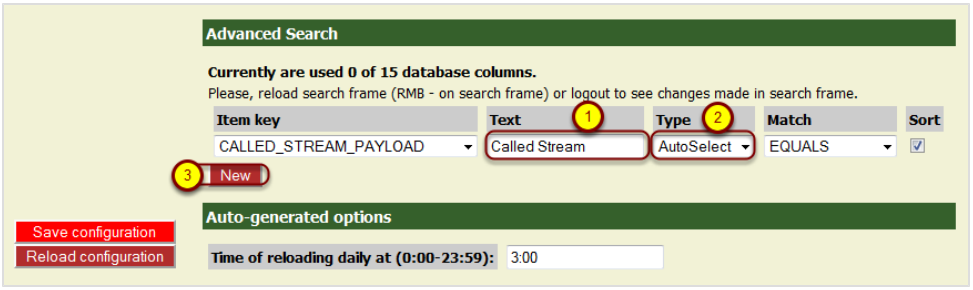


Figure 44: Advanced Search Showing Dropdown

1. Type a **Text** name for the search This is the name that will appear 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 will only be 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**(3) allows you to refine your search 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.

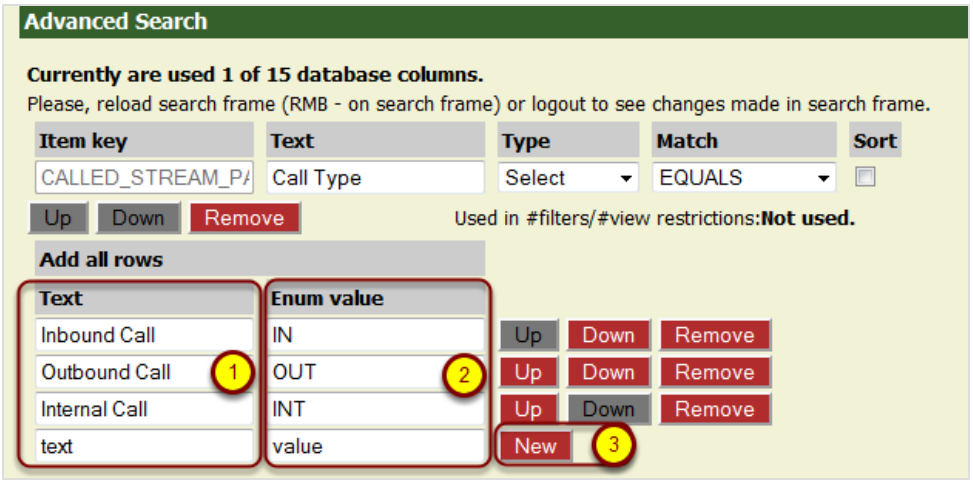


Figure 45: Add All Rows Dialog

1. In the **Text** field, type a description of the item.

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

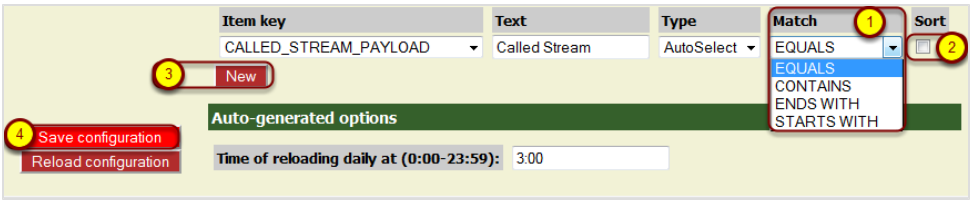


Figure 46: Select Match Value

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 your search and make it available to users.

Log out of Call Recordingand back in again. Navigate to **Recorded calls** and click **Search** The Search filter dialog opens.

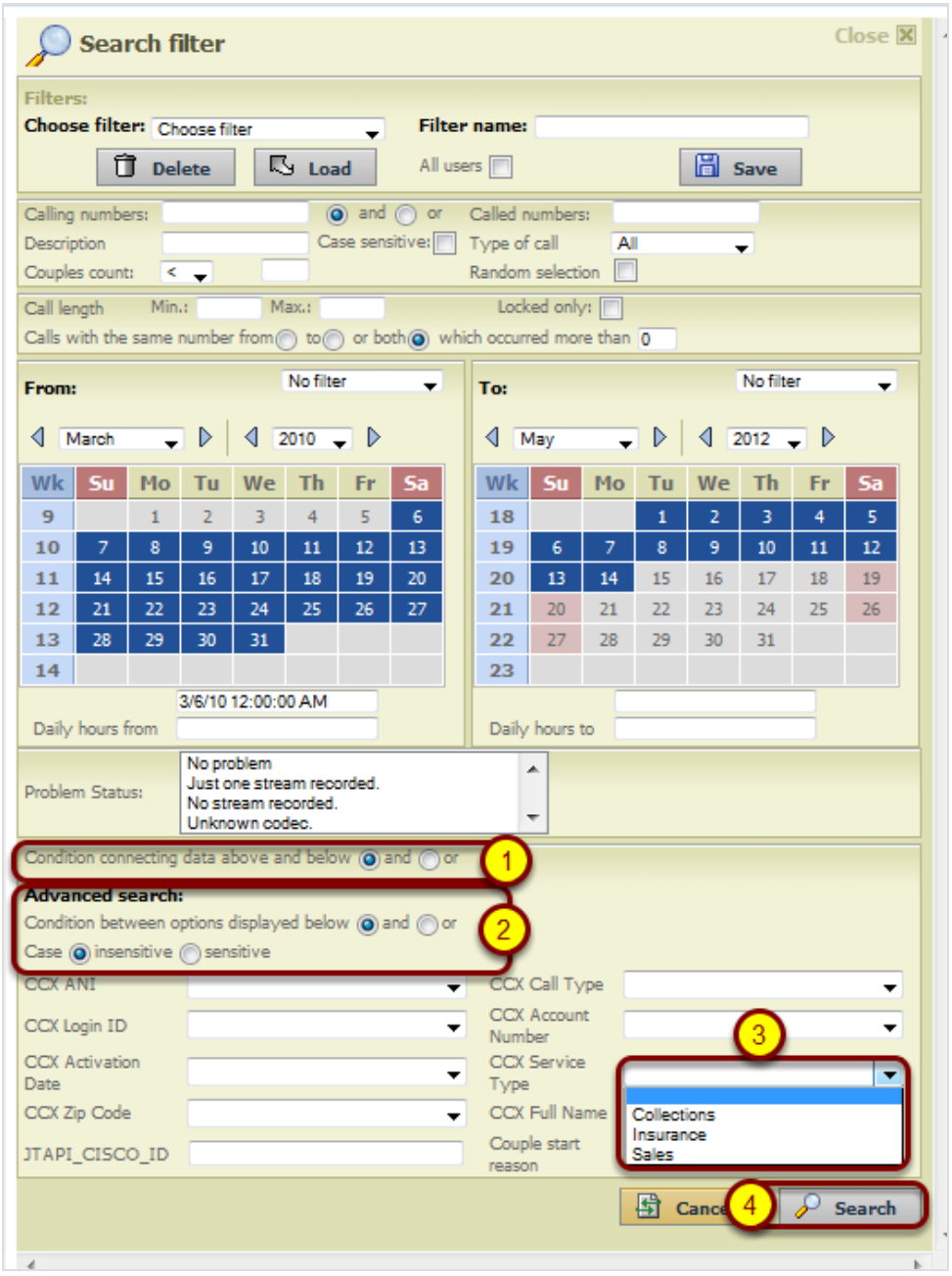


Figure 47: Search with External Data

These fields display in the Advanced Search area below standard searches. If the changes do not appear then try reloading 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 will only return calls that satisfy both the

criteria in the top of the form and the Advanced Search criteria.
Selecting **or** means that the search will return 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 will only return calls that satisfy all the elected criteria in the Advanced Search criteria.
   Selecting **or** means that the search will return 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 dropdown 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, you may have to wait several seconds between saving your changes and reloading the frame to see the changes in effect. To reload the frame right click inside the Search filter dialog select **This Frame** and then **Reload Frame**

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 you add requires additional user screen space.

Adding a New Column

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

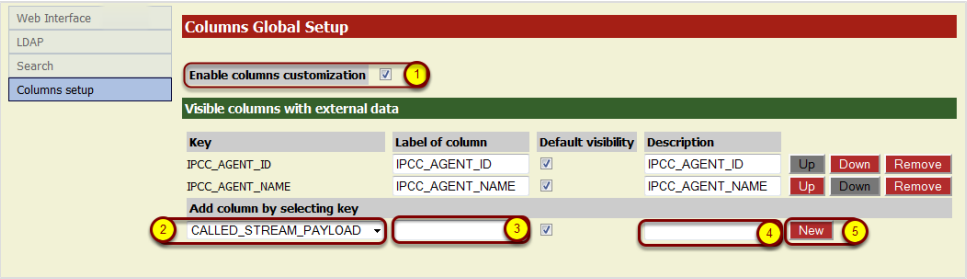


Figure 48: Columns Setup

1. Select the **Enable Columns customization** checkbox. This checkbox affects all users. If this checkbox is not selected then the customization will not be applied and the new column will 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 (optional).
5. Click **New**

Click **Save configuration** after you have added 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.
- Ensure you 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** .

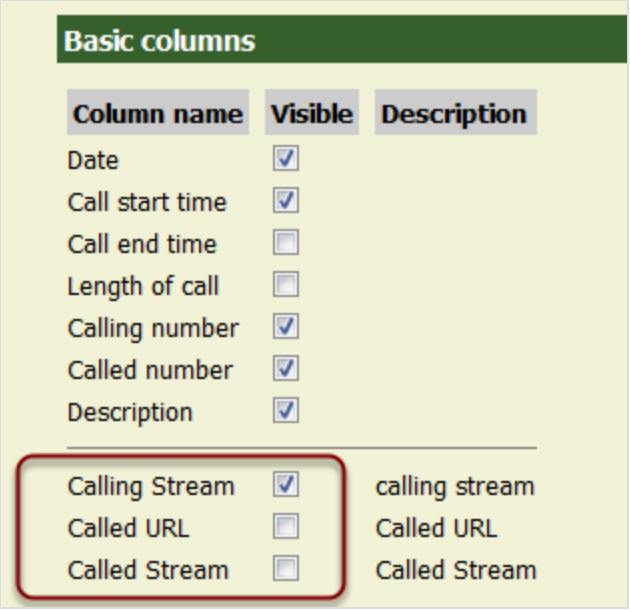


Figure 49: User Column Setup

Select the checkboxes for the columns required. The columns will be applied to their Recorded Calls and Restored Calls views.

Screen Capture

If the Screen Capture configuration module is visible, this contains the configuration items for the server components of the Screen Capture screen capture solution. More information on setup and configuration of Screen Capture can be found in the Screen Capture Administration Guide.

Integration

The Integration module, if visible, contains configuration sections for enabled integration modules, such as for Genesys contact center solutions. For more details on the setup and configuration of these modules, please refer to the Implementation Guide.

Extras

The Extras tab contains a configuration section for Call Recording Prerecording, a feature allowing agent-initiated call recording through a simple phone service on Cisco IP Phones. Please see the Prerecording chapter of this guide for more information on setup and configuration.

Key Manager

If a license has been loaded that includes the PCI DSS compliance license feature, the Key Manager configuration tab will be displayed. The Key Manager acts as a security authentication mechanism, ensuring that only authorized client applications such as Quality Manager and Screen Capture can communicate with the Call Recording core server. In addition, it provides advanced encryption facilities for securing recorded audio and video files. Navigate to **Settings >Key Manager**.

For more information about setting up the PCI DSS compliance license feature and GQM security, see the Security Guide.

Quality Manager

If Quality Manager has been enabled during setup, the Quality Manager configuration tab will be visible to the right of the Maintenance tab, enabling Quality Manager application settings to be modified. Please see the Quality Manager Administration Guide for more information on setup and configuration of Quality Manager. Navigate to **Settings > Quality Manager**.

User setup

User setup allows you to set call display options in the user interface. This is available to all Call Recording users. Navigate to **Settings > User Setup**.

Personal Setup

Language

The initial Call Recording Web UI login screen allows you to select a language. This language setting only controls the login page, and does not affect the display of the rest of Call Recording.

To change the default Call Recording language for the main application:

Log in to Call Recording.

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

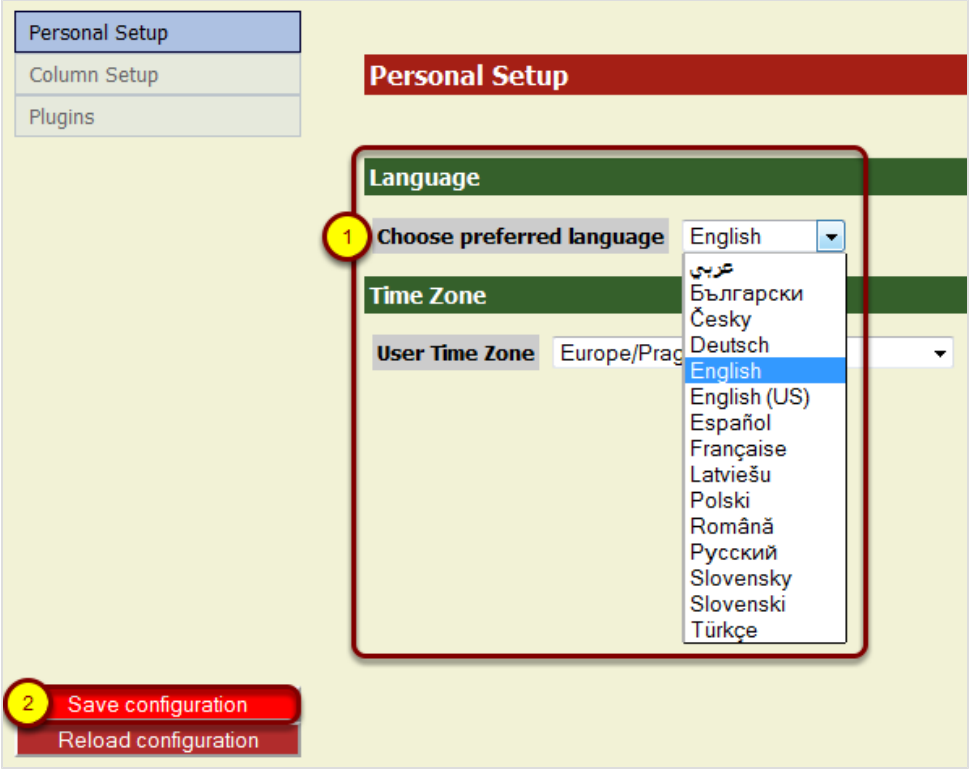


Figure 50: Changing the Default Language

1. Select the language from the **Choose preferred language** drop down list.

2. Click **Save configuration**.

Refresh the web page by clicking on another tab in Call Recording, or by clicking **Refresh** in your web browser.

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

Time Zone

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

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

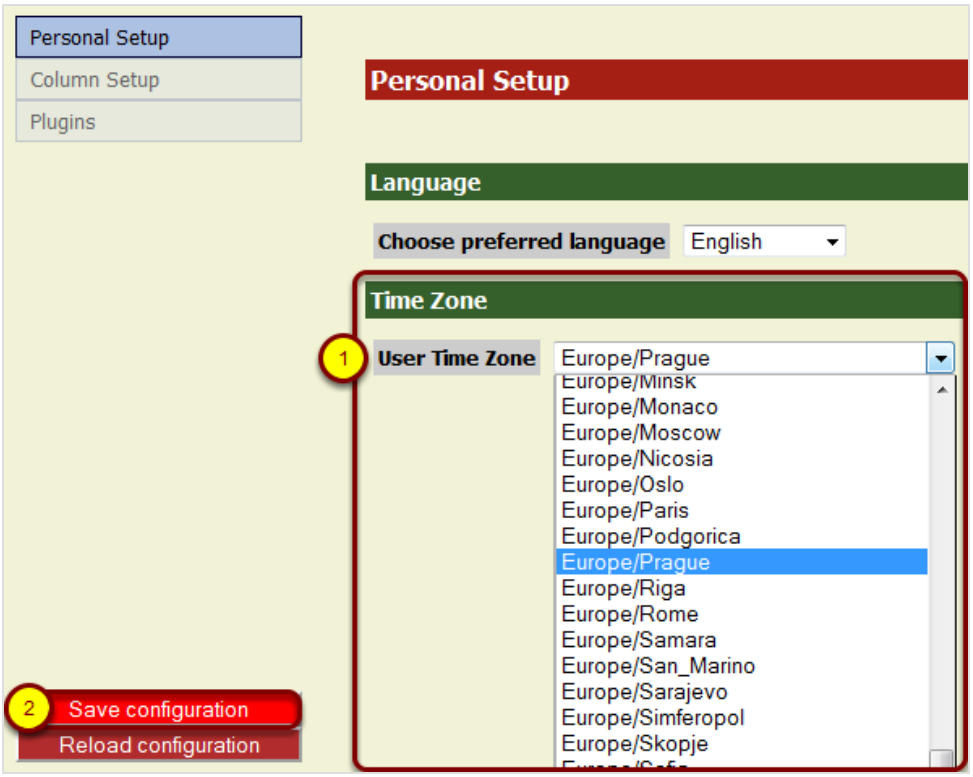


Figure 51: Changing the Default Time Zone

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

Refresh the web page by clicking on another tab in Call Recording, or by clicking **Refresh** in your web browser.

Important:

Changing the language and time zone only affects the profile of the logged in user. You can choose your own default language and time zone without affecting any other user.

Column Setup

This option is available only if the System Administrator allows users to change the column set-up. The current status of setup rights is shown below the **Setup rights** section on this screen.

The Call Recording **Recorded Calls** tab contains call information to help you select which calls to play. You can expand or reduce this view by adding or subtracting columns. Changing these selections only affects your own view of listed calls.

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

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

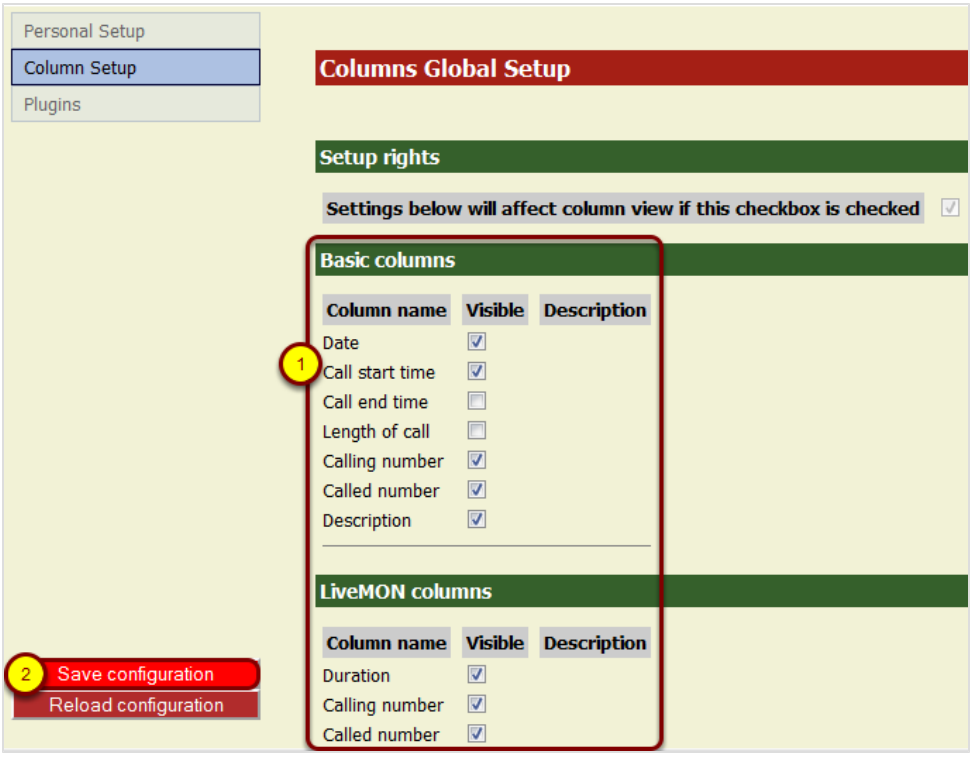


Figure 52: User's Setup - Columns

1. Select the columns to display in your **Recorded Calls** tab.
2. Click **Save Configuration**.

The columns you selected will now be displayed in the **Recorded Calls** tab.

Plugins

Some GQM features require programs to run as plugins on the local PC. These are available for download from the Call Recording Web UI for convenience; for example the Screen Capture Client installers.

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

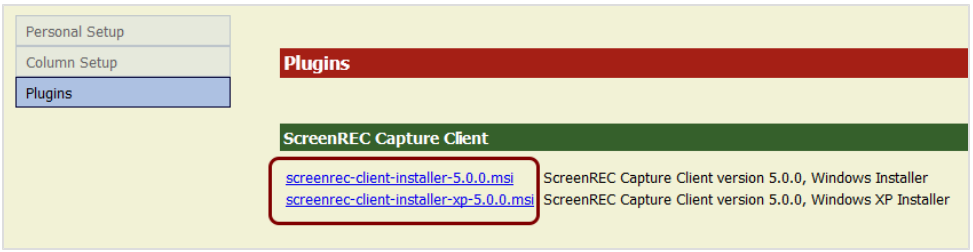


Figure 53: User's setup - Columns

Click a plugin link to download the plugin executable to your PC.

Depending on the plugin, you may need administrative permissions to run the plugin or setup wizard.

The Screen Capture Client is an MSI package to install the Screen Capture recording client on an Agent PC.
Please see the Screen Capture Administration Guide for more information.

Chapter

4 Maintenance

Use the Maintenance tab in the Call Recording web interface to perform standard maintenance on the Call Recording system, including Media Lifecycle Management. Additional specialized maintenance tools including manually executed shell scripts are available from the command line interface.

This chapter contains the following sections:

General Maintenance Configuration

It is important to remember that if you change the configuration of a tool then you must run a command line script to restart it. For example:

Restart one tool: in the example delete.

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

Restart all tools:

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

Important:

Since GQM 8.0.47x, calls that are not fully recorded because of insufficient storage space are now marked as incomplete (because of a recorder) in the database.

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 you must 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 enable you to make the most efficient use of your 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

These tools allow you to set up rules to store calls and screens. The tools are designed to be 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.

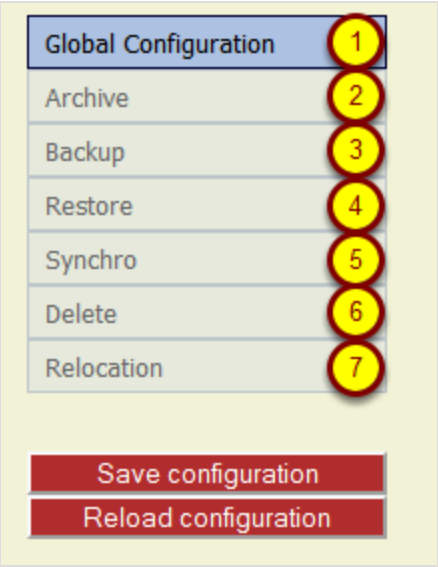


Figure 54: Global Configuration

1. Common parameters for all Maintenance tasks
2. Settings for Archiving of recordings and old database records
3. Settings for Backing up files and database records (usually for disaster recovery)
4. Settings for restoring files from backups
5. Settings for synchronization between Call Recording servers in a multi server environment
6. Settings for deleting files and related database records
7. Allows relocation of files with relevant database changes

Daemon

The following tasks may be **Run as a Daemon**, run manually (one-shot), or run each day using cron:

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

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

If you select **Run as Daemon** you cannot manually run tasks individually (one shot). To invoke the daemon, you must restart the tool you wish to activate.

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

Restore is always run as a daemon.

File Names

Only the first 6 characters of the prefix will form the file name.

Task Names

It is not possible to change a task name once it has been created.

Troubleshooting

`/opt/callrec/logs/tools.log` will show 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>
```

Enabling Tools

The tools must be enabled at all three levels for them to function:

1. Select the Tools service in Call Recording setup (callrec.conf).
2. 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.
3. By selecting the Enabled checkbox on each individual task level.

Setting the Global configuration

To configure Global configuration navigate to **Settings > Configuration > Maintenance > Global configuration**.

The Global configuration tool contains only one set of parameters: **Application Communicator Setting**.

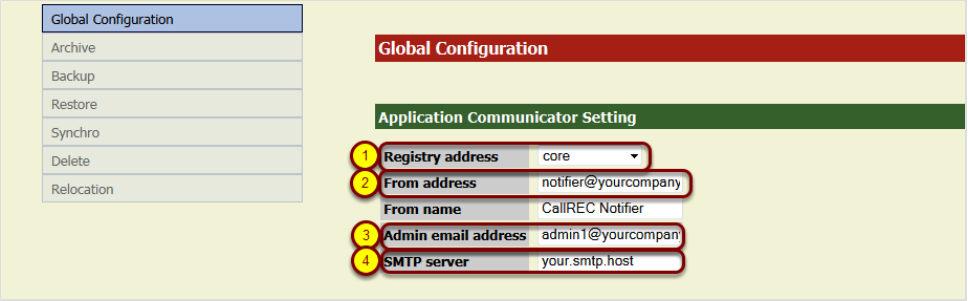


Figure 55: Maintenance Global Configuration

1. Select the Application Communicator used by maintenance tools (usually core) 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.

Click **Save** configuration.

Archiving

Archiving allows the retention of media files in different storage mediums. Archiving regularly ensures that there is always sufficient space locally to store your new calls.

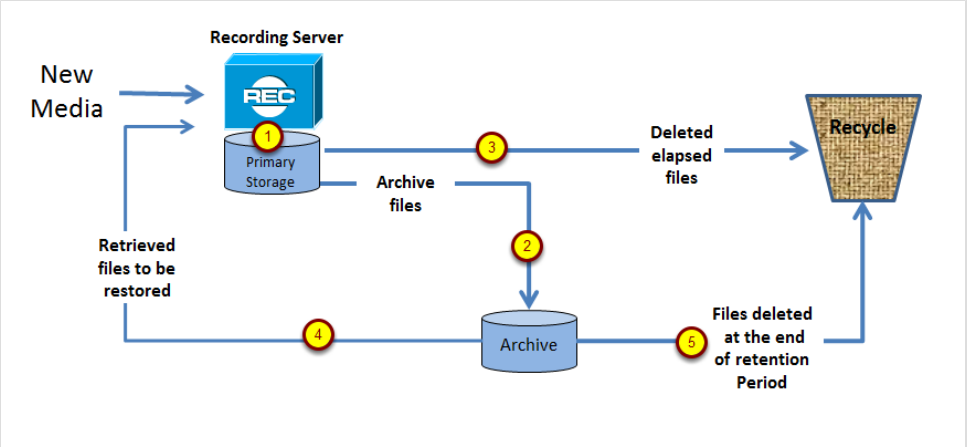


Figure 56: MLM Simple Archiving

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 also 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 will no longer be needed and can be deleted from the archive by an administrator.

Configuring Media Archive

To configure archiving navigate to **Settings > Configuration > Maintenance > Archive**.

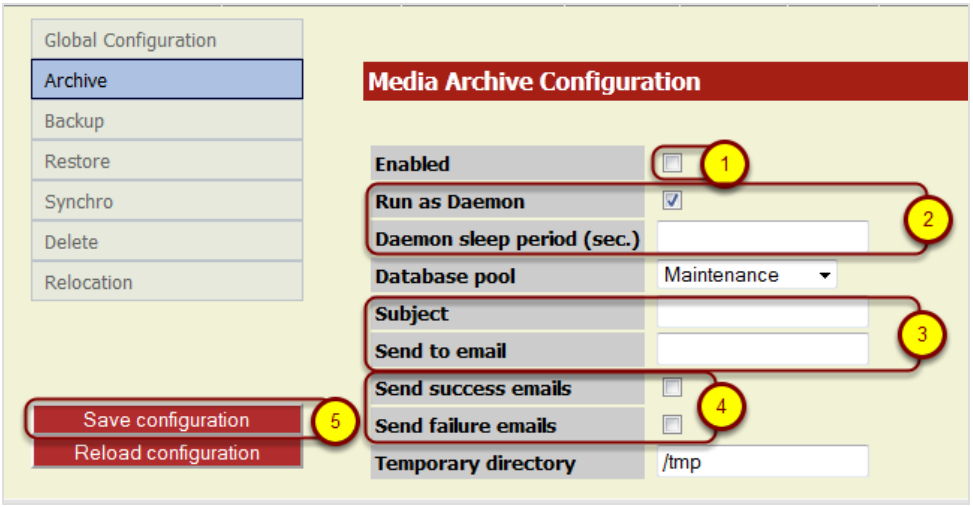


Figure 57: Configure Archive

1. Select the **Enabled** checkbox to enable the tool.
2. If you require the tool to run more frequently than once a day to even out performance, 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 will fail.
   If the tool is required to run once a day, deselect the **Run as Daemon** checkbox and the tool will run 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 will fail.
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. 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**.

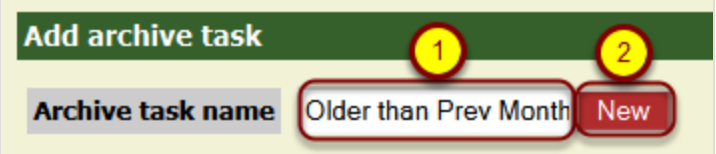


Figure 58: Add Archive Task

1. Enter a task name, each task name must be unique, the task name in the screenshot is `Older than Prev Month`.
2. Click **New** .

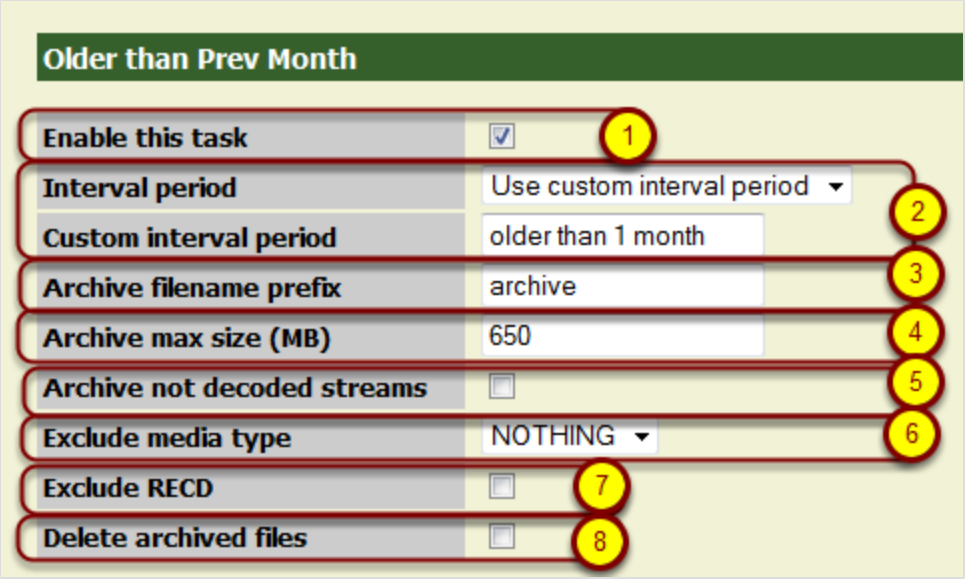


Figure 59: Enable Archive Task

1. Select **Enable this task**.
2. Select an **Interval period** from the drop down list or specify a custom period by selecting **Use custom interval period**.
   If you have selected **Use custom interval period** define your 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.

4. Set the archive maximum size in MB.
5. Optionally select **Archive not decoded streams** if you want to archive .pcap files the default is to archive MP3 files.
6. Optionally select which media type you wish 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 you cannot recover the original files you will only have the zipped archive version).

To test the validity click **Save configuration.**

Selecting an Archive

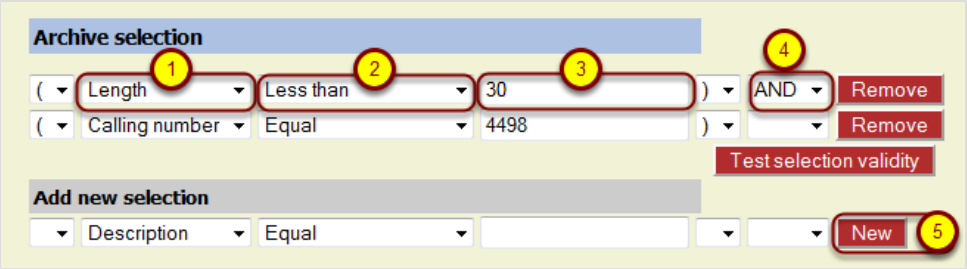


Figure 60: Archive Selection

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 dropdown 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**.

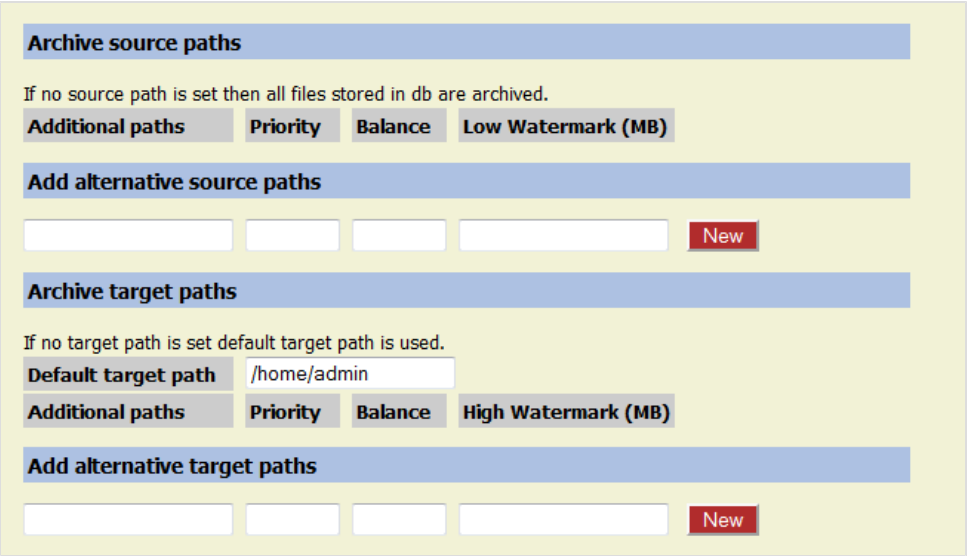


Figure 61: Archive Source Paths

Archive Source Paths: Allows you to identify alternative sources for identifying files to be archived during the task. Unless at least one path is set, the task will archive all files in the default database source path.

Archive Target Paths: Allows you to 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 Tools Manually One-shot

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

To start the tools manually (one-by-one) 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.

The most commonly used command:

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

Less common commands:

```
/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
```

Viewing Results

Linux

In `/home/admin` you can see 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 you have just archived. Open the file. You will see the MP3 files and associated details.

GUI

In the Recorded Calls view, you can see 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 is still displayed in Call Recording.
- When a call has been archived but not deleted, it behaves as a normal call recording.

Activating Deletion

Navigate to **Settings > Configuration > Maintenance > Archive**.

Scroll to an existing task.

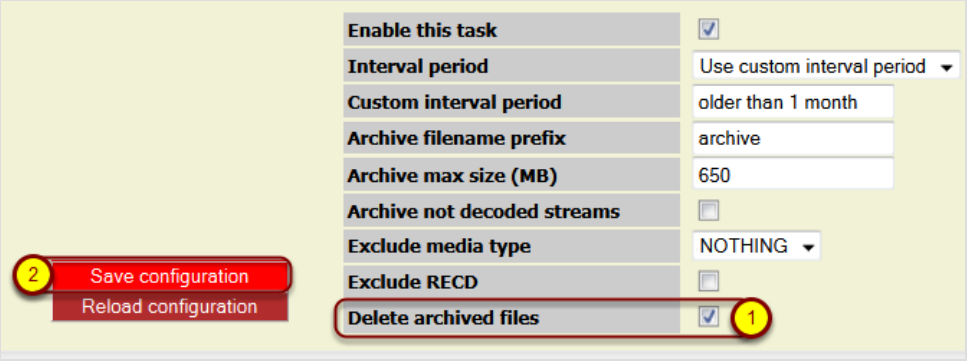


Figure 62: Activate Delete Archived Files

1. Select the checkbox to delete the archived files.
2. Save the configuration.

Viewing Results

Selecting the deletion of archived calls produces the following results:

Linux

In `/home/admin` there will be 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 will be empty.

GUI

In the **Recorded Calls** view, you can see all selected calls with the archived icon. An additional icon informs you 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.

Backup

With the Backup tool, all files are backed up if they are archived or not. A delete tool must be configured to delete any files which no longer need to be on the recording server.

Configuring Media Backup

Navigate to **Settings > Configuration > Maintenance > Backup**.

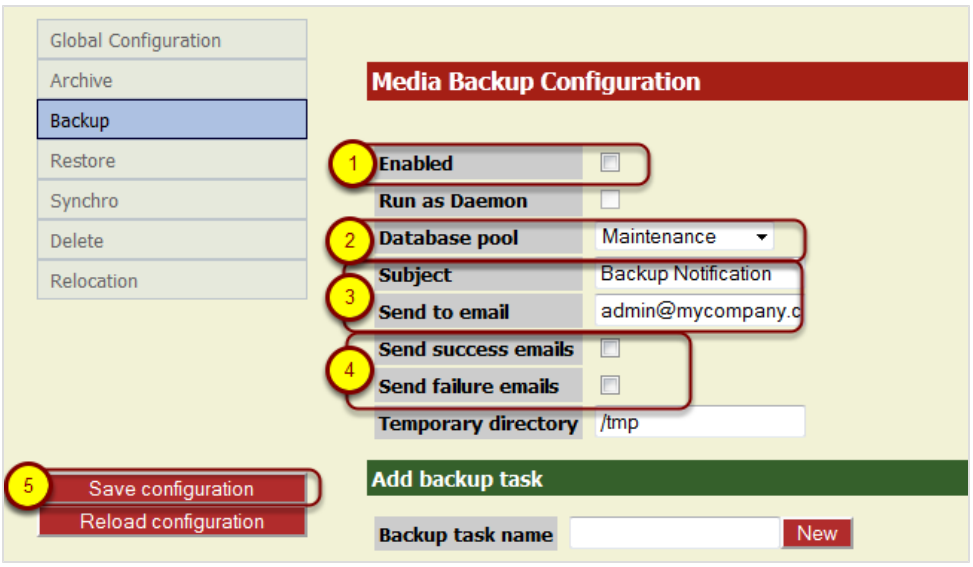


Figure 63: Configure Backup

1. Select the **Enable** checkbox to enable Backup.
2. Select a **Database pool** from the dropdown list.
3. Ensure there is a valid email address and set a subject for the email. If these fields are empty when you **Save configuration** then the validation will fail.
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. Click **Save configuration**.

You cannot run **Backup** as daemon.

Creating a Backup Task

Navigate to **Settings > Configuration > Maintenance > Backup**.

Figure 64: Add Backup Task

1. Enter a unique task name for the new task.
2. Click **New**. The form below appears.

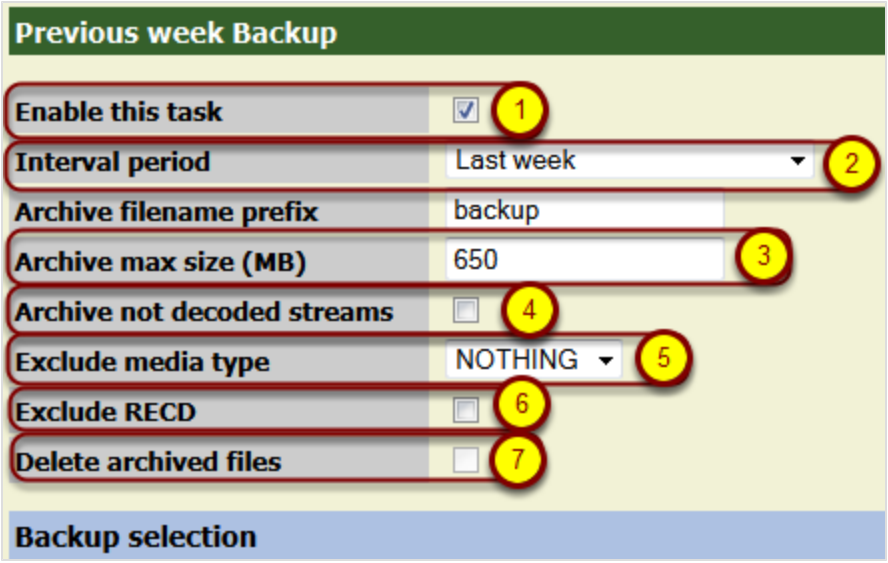


Figure 65: Enable the Backup Task

3. Select the **Enable** checkbox to enable the task.
4. Select an **Interval period** or enter a custom interval period.
5. Set the **Archive max size** (default value 650 MB).
6. If you want to archive .pcap files, select this box, the default is to archive MP3 files.
7. Select which media type you wish 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**.

Starting a Tool Manually

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

1. In the Linux console, enter the command: `/opt/callrec/bin/backup start`

One shot run:

```
/opt/callrec/bin/backup
```

Note that the Archive tool running in Cron (non-daemon mode) is most commonly used as backup doesn't 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 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.

Restoring

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.

Configuring Restore

Navigate to **Settings > Configuration > Maintenance > Restore**.

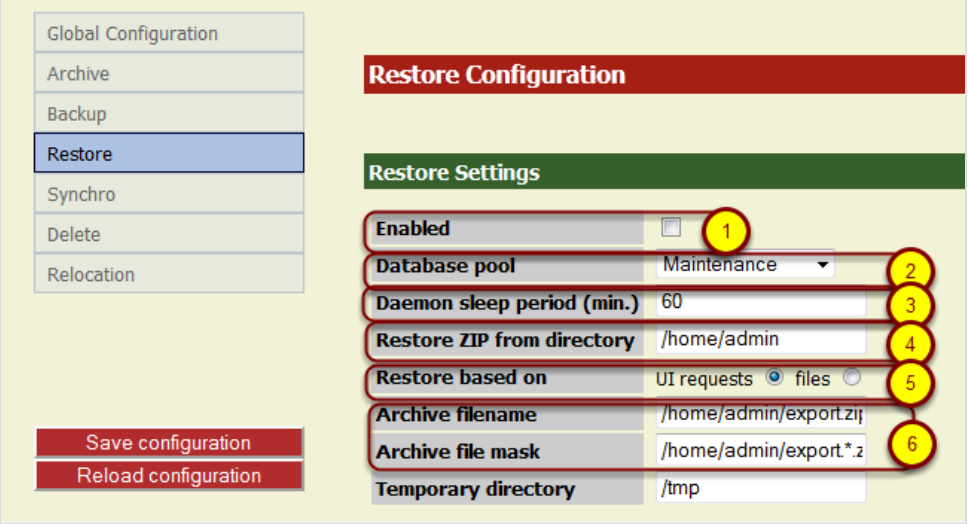


Figure 66: Restore Configuration

1. Select the **Enabled** checkbox.
2. Select the correct **Database pool** from the dropdown list.
3. Set the **Daemon sleep period**. If this field is empty when you **Save configuration** then the validation will fail.
4. The **Restore ZIP from directory** location should be the target location of the Archived files.
5. There are two options you can select in **Restore Based on**:
   - Restore Based on **UI requests**: Once you have archived the file then the file displays an icon in the Recorded Calls list  . Click  and it will be replaced by  indicating that the file is being restored. If selected, Restore Based on**UI requests** will process 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 will not be restored). Once restored the Recorded calls list will display showing that the call is restored and available for playing.

- Restore Based on **Files**: You must provide a list of files to be restored (all files contained in the zip files containing the requested files will be restored even if they have not been requested).
  Enter the **Archive filename** and **Archive file mask**.

Configuring Requests

Figure 67: Restore Request

1. Ensure there is a valid email address and set a subject for the email. If these fields are empty when you **Save configuration** then the validation will fail.
2. Calls will be restored to the default restore directory unless another has been created.
3. Click **Save configuration**.

Starting a Tool Manually

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

In the Linux console, enter the command:

```
/opt/callrec/bin/restore start
```

Viewing Results

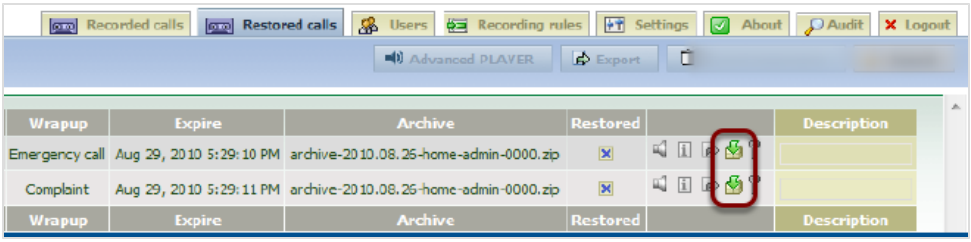
Linux

In `/opt/callrec/data/calls` select the associated date for the calls you have just archived. Open the file. You will see the MP3 files and associated details.

GUI

Once the archive and deleted calls have been selected for restore:

Restored calls



Restored Calls

The restored calls appear in the **Restored calls** tab.

The icon changes from informing you that the call is available for restore to the speaker icon which allows you to listen to the call.

Another icon appears informing you that the call has been restored.

Setting the Expiration Time

This sets how long the media file will be available for.

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

Set Expiration Time

Scroll to **Media Restore**

1. Enter a **Restore expiration time** for the media in Days.
2. Click **Save configuration**.

Notifying Admin of a 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**: Allows you 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.
  Watermark: Sets the capacity trigger for file storage.

Synchro

You only need to use Synchro if you have a replay server.

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 > Maintenance > Synchro**.

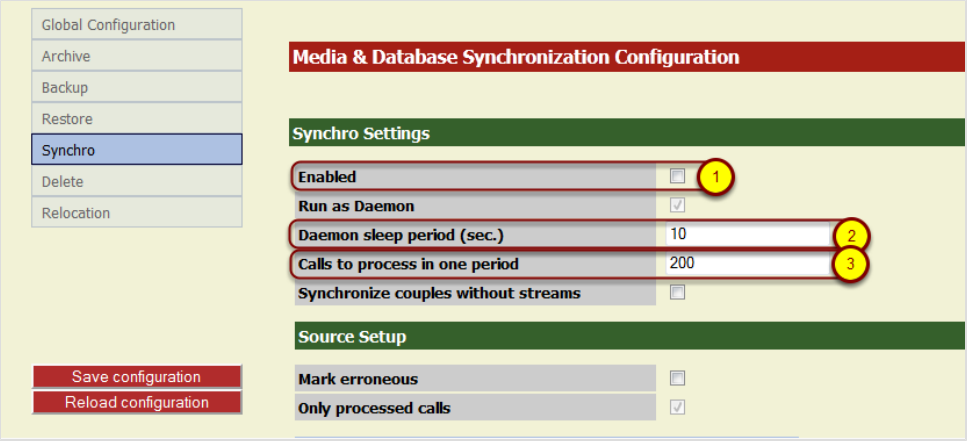


Figure 68: Synchro Settings

1. Select the **Enabled** checkbox to enable Synchro.
2. Set a **Daemon sleep period** in seconds. The default is 10 seconds. If this field is empty when **Save configuration** is selected, the validation will fail. 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:

Enabling the **Synchronize couples without streams** option is NOT recommended.

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 will attempt to synchronize calls before the MP3 is created, potentially causing major problems in operation.

Only enable **Mark Erroneous** if there are problems synchronizing. **Mark Erroneous** marks calls that failed during synchronization, and the daemon will ignore 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

You must add each recording server to be synchronized as a new source.

Figure 69: Add New Source

Type a unique name for the recording server in **Source Sysname**, for example `src1`.

Click **New**. A new section will open up as below.

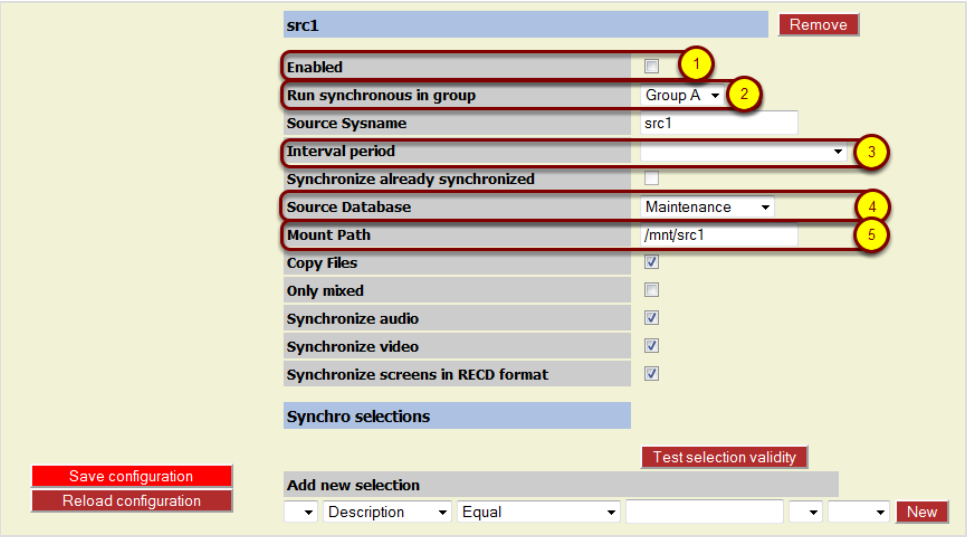


Figure 70: Synchro Source

To set the source parameters.

1. Select the **Enabled** checkbox to enable the source.
2. Select a group from the dropdown 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** dropdown list. The options are: **Yesterday**, **Last Week**, **Last Month**,
   or

   Use custom interval period. If **Use custom interval period** was selected,then type your **Custom interval period** in the field that appears. 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** dropdown 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 which will be used for additional archive storage for example.

Copy files default is enabled. When enabled, both files and database records will be copied to the replay server. If disabled, only database entries will be 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. It is defined in the web configuration interface.

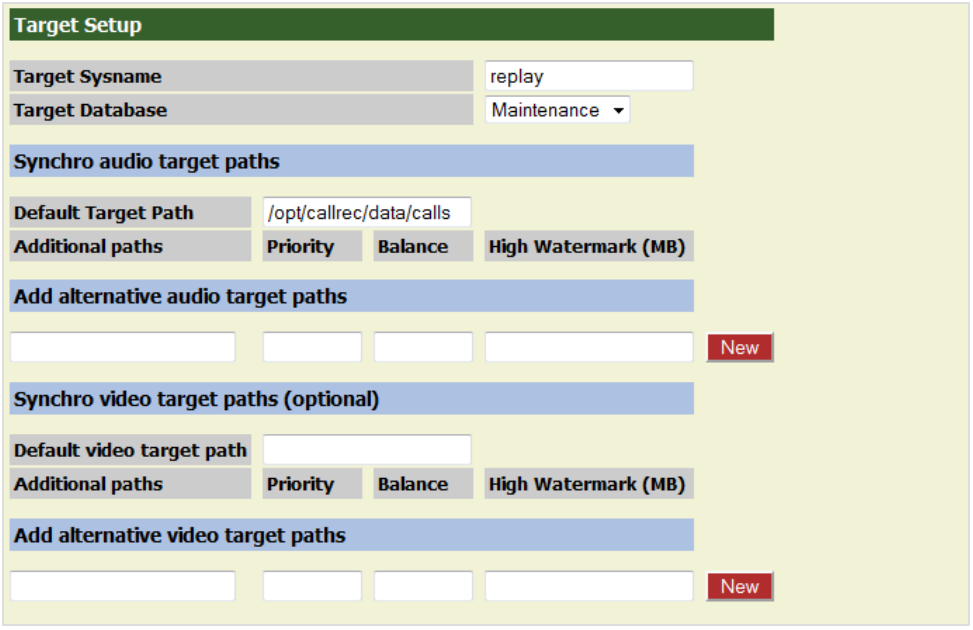


Figure 71: Target Setup

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 > Call Recording Core > Database** part of the configuration interface).
- **Default Target Path** : Where to store synchronized files.
- **Additional Paths**: Allows you to 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): Allows you to set default and additional video target paths for synchronization.
- **Important**: **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.

Configuring Delete

Call Recording allows users to set deletion parameters for the system to free up storage space after calls have been archived. Navigate to **Settings >Maintenance > Delete**.

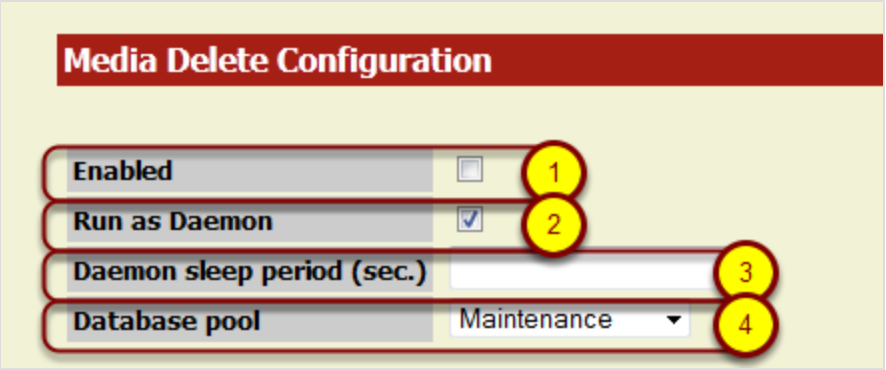


Figure 72: Deletion Parameters

1. Check the **Enabled** checkbox to activate the deletion function. If unchecked, the delete tool will be 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 dropdown list. Choose database pool, which will be used as the source for call related data (defined in **Settings > Call Recording Core > Database tab**).

Delete Calls, Recorded Screens, and Screens in Recd Format

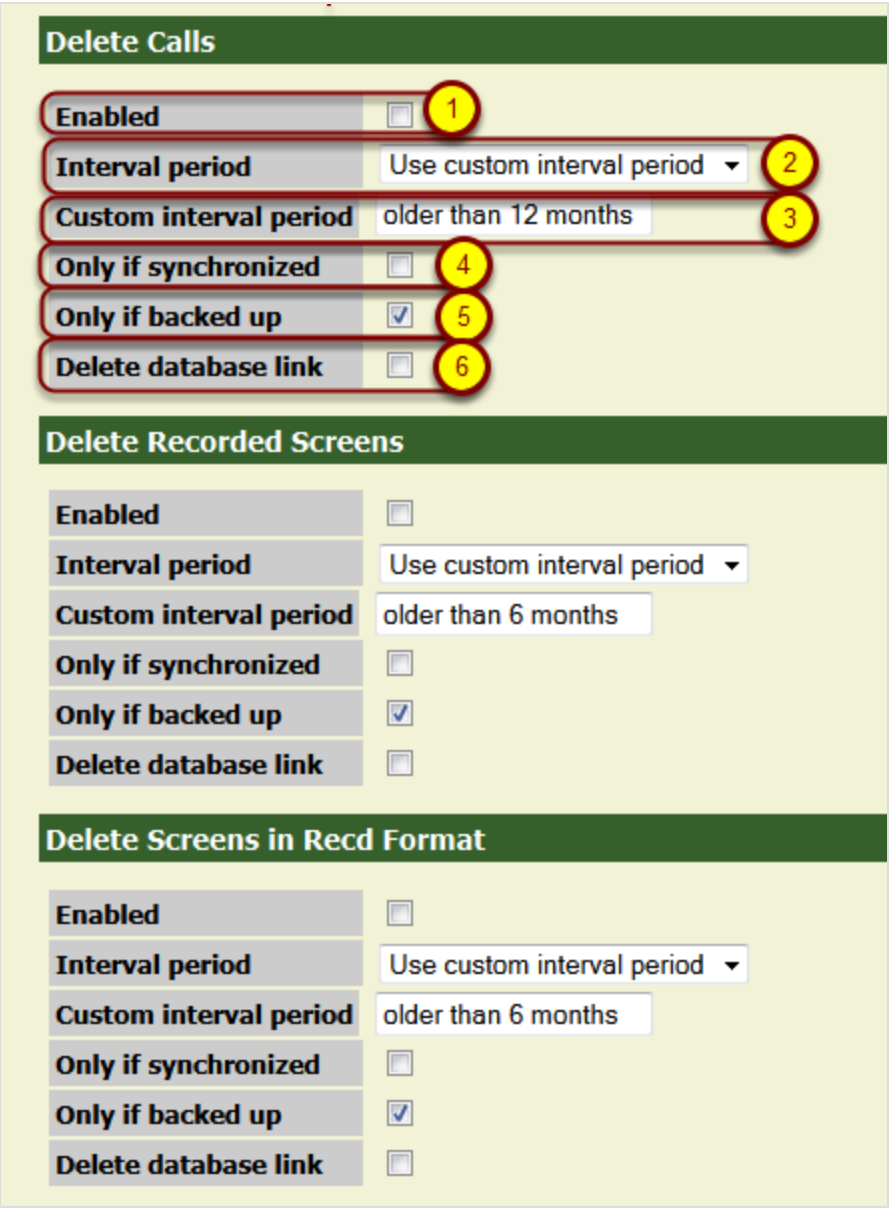


Figure 73: Delete Calls

There are three blocks identifying parameters for deleting Calls, Recorded Screens 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 you have selected **Use custom interval period**, define your 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

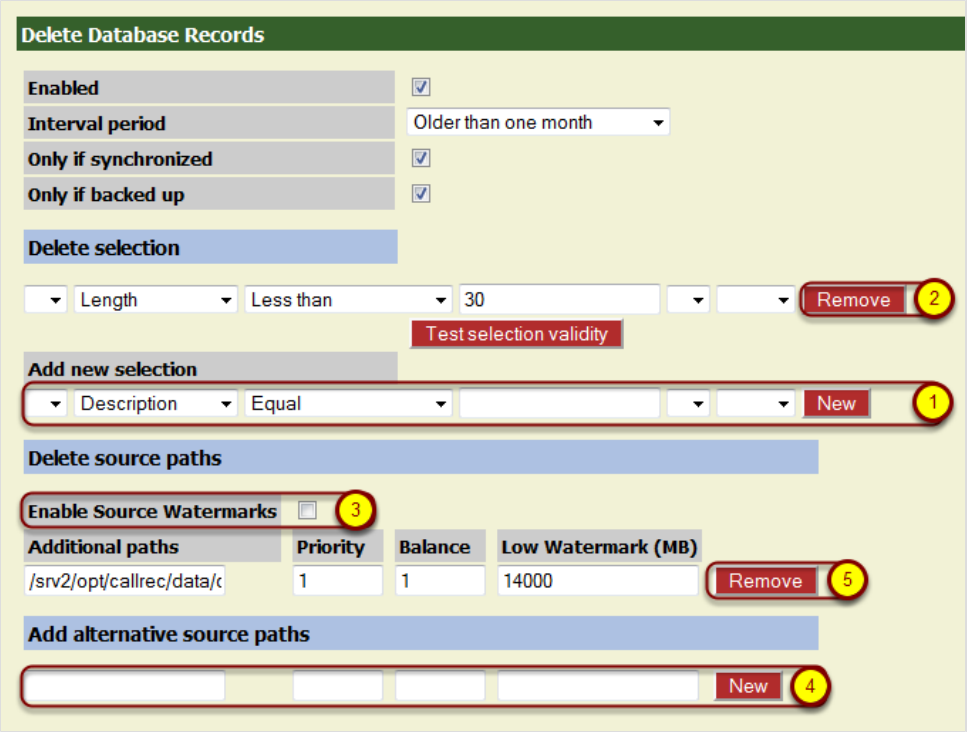


Figure 74: Delete Database Records

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 dropdown list.
2. To remove a selection, click **Remove**.
3. **Enable Source Watermarks**: Enables the watermark feature if checked. 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 will be triggered when less than this amount of free disk space is available.

Click **New** and the application will validate the entries. Any field that does not pass the validation will appear 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**.

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 >Maintenance > Relocation**.

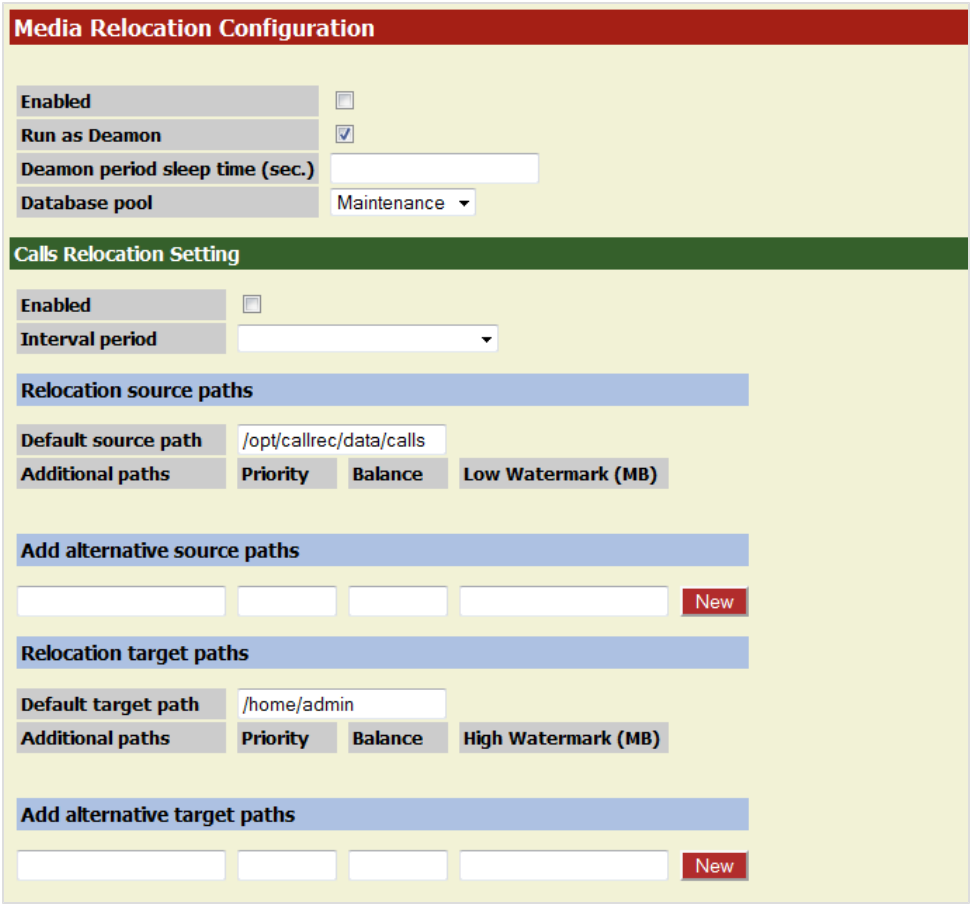


Figure 75: Maintenance - Relocation

- **Enabled** activates relocation function. If unchecked, the relocate tool will be disabled.
- **Run as Daemon** 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 which will 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 your 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** allows you to 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 allows Call Recording to access files for media playback.
- **Additional paths** allows you 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.

Custom Triggers Overview

Maintenance tools can be run based on custom event triggers defined by the administrator. You can 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 you specify Alternative Source Paths (ASPs), Call Recording ignores the default path, and instead applies the following rules:

- The highest priority ASP will be 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 allow you 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 you specify Alternative Target Paths (ATPs), Call Recording ignores the default path, and instead applies the following rules:

- The highest priority ATP will be 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 allow you 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

The time range for tools uses the following parameters:

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 should be included first, then the **to** variable

- `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)

Important:
These parameters for the time specification are case sensitive.

Chapter

5 Command Line Scripts

Many basic maintenance tasks in Call Recording can be executed directly from the command line. For each of the following tasks, you must log in as an Administrator with Root privileges.

This chapter contains the following sections:

Starting and stopping Call Recording

Use the service command for starting, stopping and restarting Call Recording services. The service command functions as a shortcut to the /etc/init.d directory. Please note that you have to switch to root from admin using su - to make relative path commands work:

```
[root@callrec ~]# service callrec
```

We suggest that you use the absolute path for these commands as these do not require you to change directory to issue these commands and avoids issues with directory permissions.

Usage: /etc/init.d/callrec {start|stop|restart|status}

Starting Call Recording

Use the command

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

to start-up the Call Recording application:

```
[root@callrec ~]# service callrec 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 command

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

to stop the Call Recording application:

```
root@callrec ~]# service callrec 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 command

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

to stop and restart the Call Recording application:

```
[root@callrec ~]# service callrec 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 start-up sequence of the server, run the command in root:

```
/sbin/chkconfig --add callrec
```

You can enable or disable automatic starting of Call Recording with the following commands:

```
/sbin/chkconfig callrec on
```

To enable

```
/sbin/chkconfig callrec off
```

To disable

Reloading the Configuration manager

If you restart Call Recordingwhile recording calls you will lose the recordings of the calls being recorded at the time that Call Recording is restarted. However Call Recording uses an independent configuration server to store configuration information for all the components of the system. This means you do not have to restart the entire Call Recording system 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, you can reset configuration in these components without restarting the system.

To reload the configuration, type:

```
/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 your sniffing method or encoding type needs a complete restart of the Call Recording system.

Checking Call Recording Status

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** – will show 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 the Server

Local Restart

To restart the server from the local console, press **CTRL+ALT+DEL** combination. The system will safely terminate all services and restart.

Remote restart

To restart the server remotely, log in as `admin` then type `su -` into the console (you will be prompted for the password) and enter the command `reboot`.

Shutting down the server

To shut down the server, log in as `admin` then type `su -` into the console (you will be prompted for the password) and then enter the command `halt`.

Restarting the services

Restarting the Call Recording Web Service

If the Call Recording GUI is not available, you may restart the Web service:

1. Log in as `admin` then type `su - root`
2. Type the command

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

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
callrec	All Call Recording components
callrec_archive	Archive Tool
callrec_callmonitor	Call Monitor
callrec_configmanager	Configuration Manager
callrec_core	Call Recording Core
callrec_delete	Delete Tool
callrec_ds	Decoder Server
callrec_genesys	Genesys Integration Module
callrec_instreamer	Audio Stream Recording
callrec_ipcc	UCCE Integration Module
callrec_ipccex	UCCX Integration Module
callrec_mixer	Audio and Video Mixer
callrec_naming	Naming Tool
callrec_relocation	Relocation Tool
callrec_restore	Restoring Tool
callrec_rmi	RMI Service
callrec_rs	Recorder Server
callrec_rts_jtapi	JTAPI Adapter
callrec_rts_sip	SIP Adapter
callrec_rts_skinny	Skinny Adapter
callrec_slr	Active Recorder
callrec_synchro	Synchronization Tool

COMPONENT_NAME	Component to be Restarted
callrec_screenrec	Screen Capture
callrec_tools	All Tool Components
callrec_web	Web Server (Tomcat5)

Table 3: Restarting Individual Call Recording Components

Restarting Call Recording in a Multi-Server Environment

Because Call Recording can be configured to support many different environments, the steps for restarting depend on your configuration.

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 your system administrator. Ensure you have written down all your custom settings so they can be restored.

To revert all your 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 Cisco CUCM, all the servers in the cluster should be time-synchronized (via NTP) with the same server as Cisco 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:

```
/etc/init.d/ntpd stop
```

Stop Call Recording and the Database:

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

Synchronize time manually:

```
ntpdate <timeserver IP address>
```

Write the current time to the system BIOS:

```
hwclock --systohc
```

Start the NTP daemon:

```
/etc/init.d/ntpd start
```

Check if the time/date is correct now:

```
date
```

Start the database and Call Recording again

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

The system will take a while before it is synchronized (usually around 15 minutes from when the NTP daemon was started):
Check the synchronization state.

```
ntpstat
```

Mounting Windows File Shares

Connecting a Windows-based remote file storage facility to a Linux operating system can be tricky. If you wish to configure a connection to (or 'mount') a Windows file share for archive or backup media storage, for example, the following procedure is recommended:

1. Ensure you have the following information 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:

Should you later wish 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 will need 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, the Configuration Service and related components will need to be restarted. 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 isntance 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
`-A --accept <num>`	Accept payload num. can be specified as several options (`0,8,9,18,13,19`)
`-m --minpackets <num>`	Minimum packets representing not empty stream (default: `0`)
`-l --logger <name>`	File with log4cxx configuration (default: `slr.log4cxx.properties`)
`-e --sessionexpires <num>`	Timeout of SIP session expiration in seconds (default: `1800`). Valid range: `90 - 86400`
`-s --rejectedsessions <num>`	Max. rejected SIP sessions between 2 states (default: none)
`-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 --rtpportscount <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 4: 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 will handle 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 will still apply.

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
```

Chapter

6 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

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, you must enable SMTP within Call Recording so it can send email outside your 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 allows you to convert "raw" streamed data into audio files.

Use this script in the event an error occurred during encoding. Some streams may have remained un-encoded. The call2mp3 script allows you to select these un-encoded streams and encode them 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.

You can also 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 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 will stay 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.
- `-noupdatedb` – 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. Please note it will take a 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 allows you to specify additional backup parameters, such as UCCE or external data, through 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, `selectiveback` up splits it into multiple files.

`crc` allows you to 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` extention.

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`. Typically, you do not need to 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. You can 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 back up. You can identify any string within the call description, or standard Call Recording database entity.

Important:

You must use the format `&apos;string&apos;`

Example: To limit your 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 you have defined all your `selectivebackup` values, be sure to save your 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.

Chapter

7 Logs

Log files summarize the behavior of the system. Logs record all messages and exceptions generated by ZOOM 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:

Logs Overview

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.

You can access all log files from the Call Recording web interface. If you are logged in as Administrator, go to the log page under **Settings > Logs**. You can open individual log pages, copy them to the clipboard, or export them for further analysis.

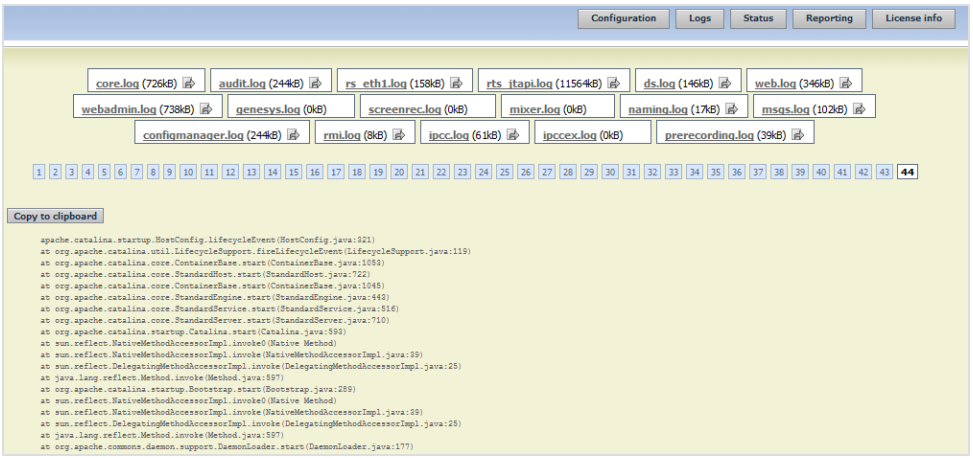


Figure 76: Working with the Call Recording Log Files

- To browse through log files, click the number icons to open log pages.
- 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 will be 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 are logged here. Allows you to determine which users performed which action.

Sending Logs to Genesys

Log files are particularly helpful for diagnosing problems with the system. You can either attach log files to emails to our Service and Support team (http://genesyslab.com/support/contact) or send the logs directly using the `bugreport` script.

Sending logs with the `bugreport` script (if SMTP is enabled and has internet access):

1. Log in with administrator privileges, then type `su - root`
2. Enter the following command:

```
/opt/callrec/bin/bugreport
```

Sending logs as an email attachment:

1. Log in as 'admin' then type `su - root`Genesys Documentation
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 your computer
5. Send the `log.tar` file as an email attachment to http://genesyslab.com/support/contact

DEBUG Mode

All Call Recording components use `log4j` for creating 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.

For debugging, you may have to change from `log4j` to debug mode.

Every component has its own configuration file for logging. These configuration log files are located in `/etc/callrec/`.

To switch between `log4j` and `debug` logging modes:

1. Locate configuration file belonging 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, and so on.

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. You can change 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 log page size

To change the number of log records displayed on a single page, you can 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 your 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, you can 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` identifying 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
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 5: 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>
```

Chapter

8 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

To generate a report, log in with administrator privileges and go to **Settings > Reporting**.

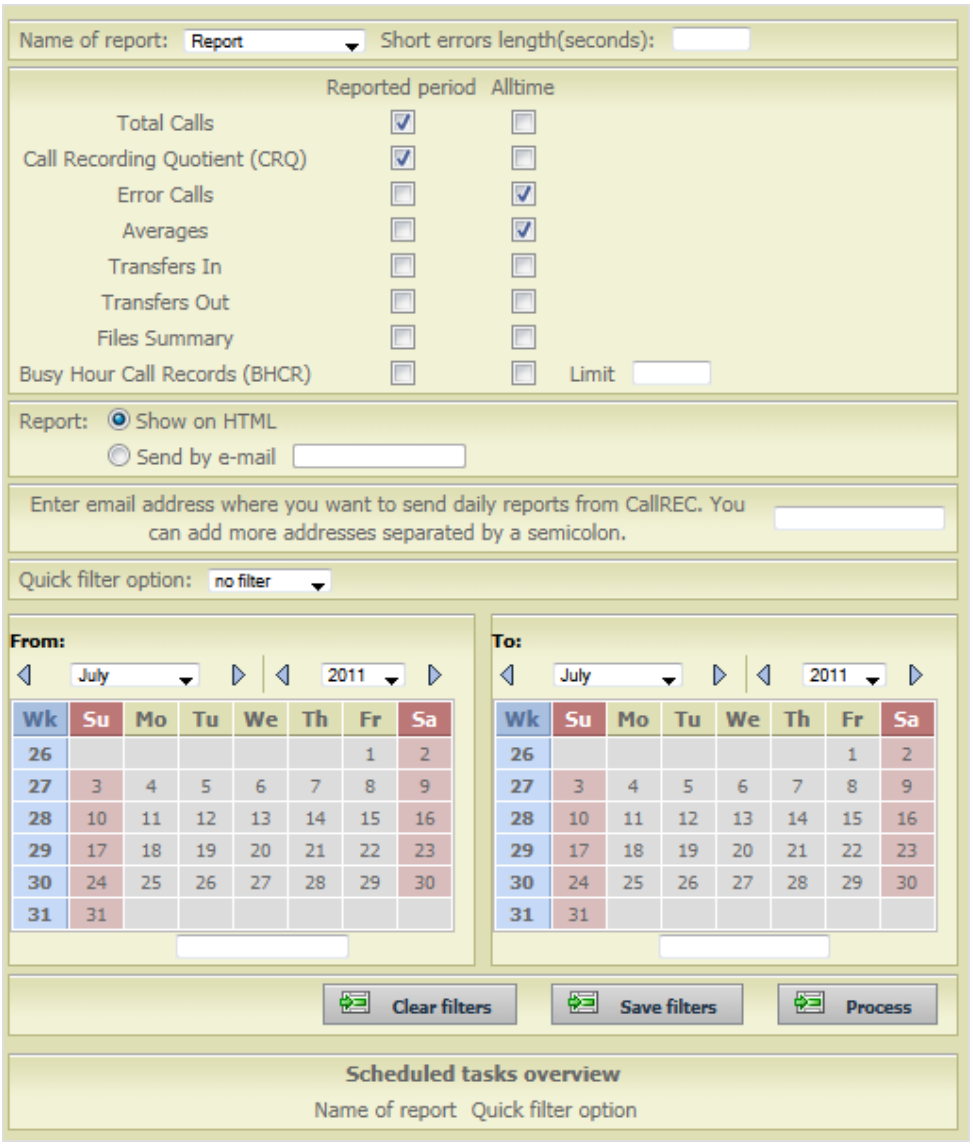


Figure 77: Reporting – Parameters

Name of report changes the options available for the report:

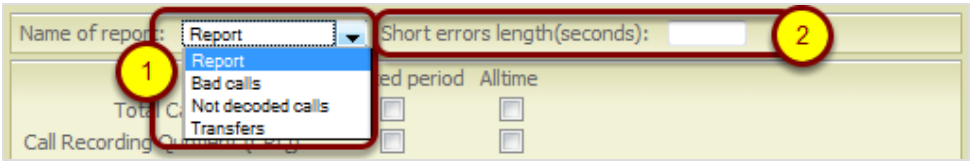


Figure 78: Reports Selection

1. **Report**: All reporting options are available. Bad calls – Limits the report to only calls that are incorrectly recorded or missing information in the database.
   Not decoded calls: Limits the report to only calls which 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 allows you to discard very short calls, not including them in your report.

Report Type

You can select two types of reports:

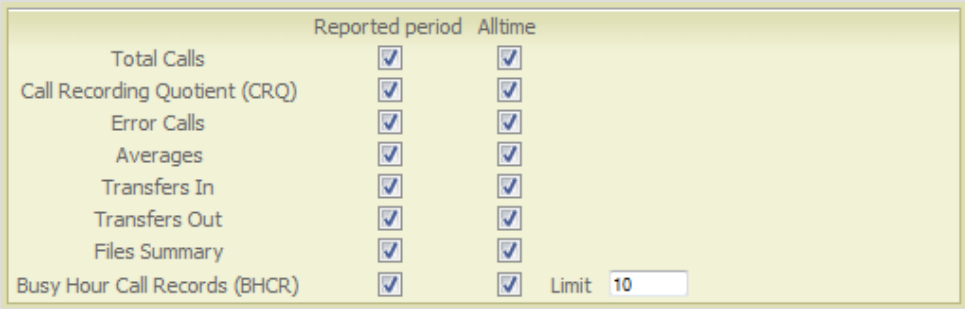


Figure 79: Report Parameters Selection

- **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 can be displayed in your web browser (select Show on HTML) or send to an email address.

Figure 80: Report Results Setting

Setting Up Periodical Reports with Quick Filter

To create an automatic periodical report based on a time range, you can use a Quick filter option. The Quick filter options pre-define a period for the report to be sent to the email recipients.

Figure 81: Daily Reporting

1. Select a time period from the drop down list.

Important:
It is recommended to use only (yesterday or last week).

2. Enter email address allows you to enter multiple recipients of email notifications. Use a semicolon ";" to separate email addresses.

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.

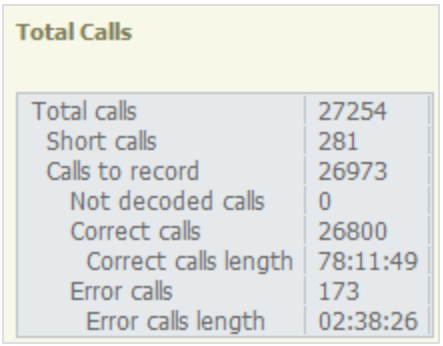


Figure 82: Total Calls Captured by Call Recording

Call Recording Quotient (CRQ): Shows the percentage of total calls that have been recorded.

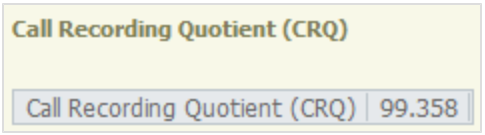


Figure 83: Percent of Calls Recorded

Error Calls: Generates a table of all error calls, listed by the type of error.

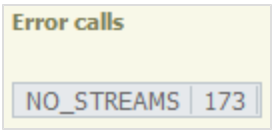


Figure 84: Error Calls

Averages: Shows the average number of daily calls and their average length in seconds.

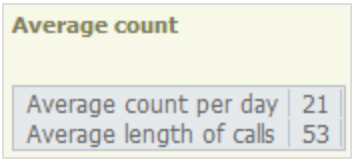


Figure 85: Average Count

Transfers-in, Transfers-out: Shows the total number of calls synchronized within Call Recording.

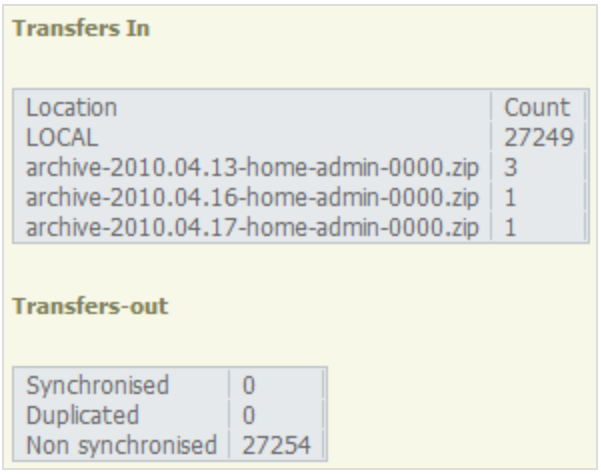


Figure 86: Synchronized Calls

- 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).

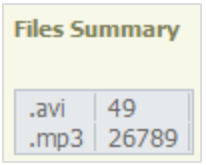


Figure 87: Total Number of Saved Files in Listed Formats

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 88: Recording Levels

Limit: Allows the number of events set to be displayed in the report.

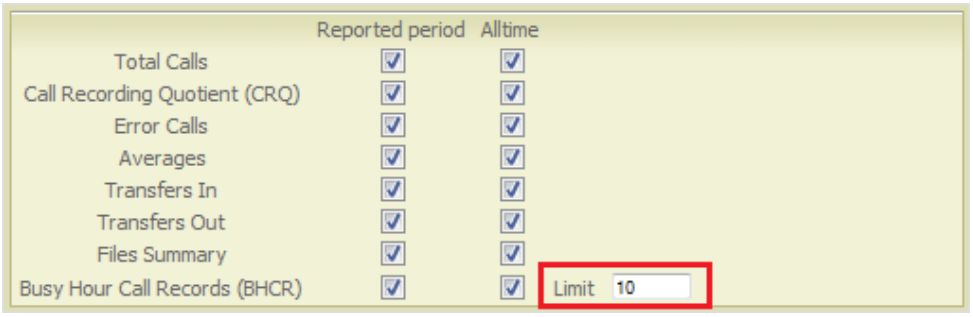


Figure 89: Recording Limit Selection

Time Range Setup for Selected Parameters

The time range for reporting parameters can be set by using the Quick filter option (see Setting Up Periodical Reports), or by selecting the time period using standard calendar controls. If no reporting period is specified, the whole database of calls is processed for reporting.

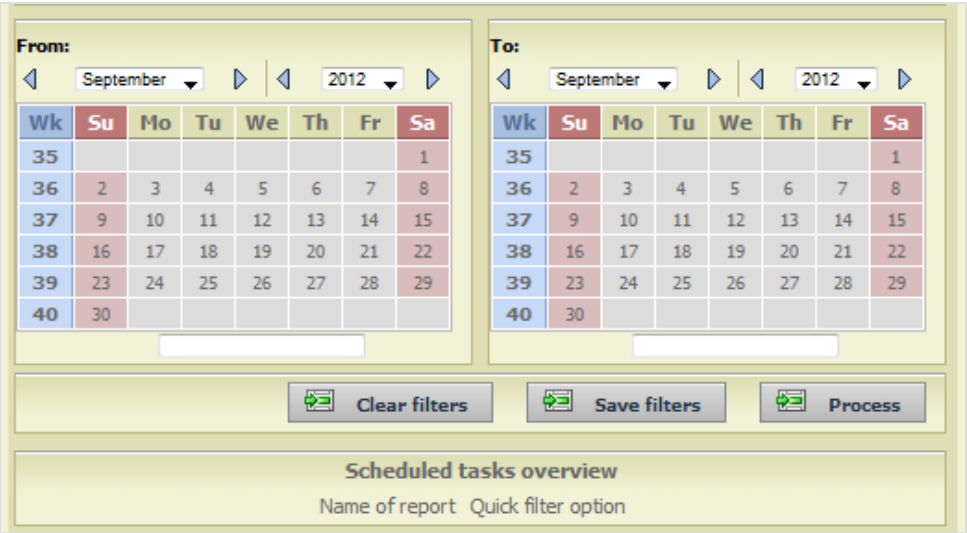


Figure 90: Selecting Time Period

To run a report, click **Process**.

Saved filters should only be set by the administrator.

Bad Calls Report

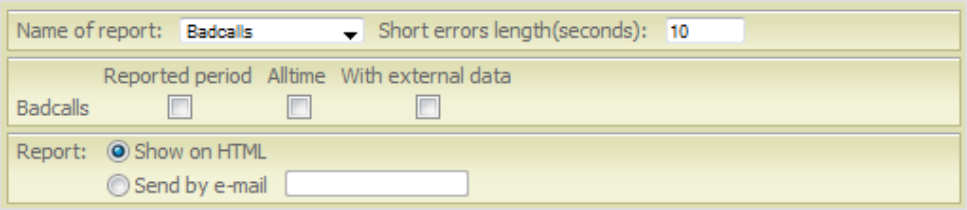
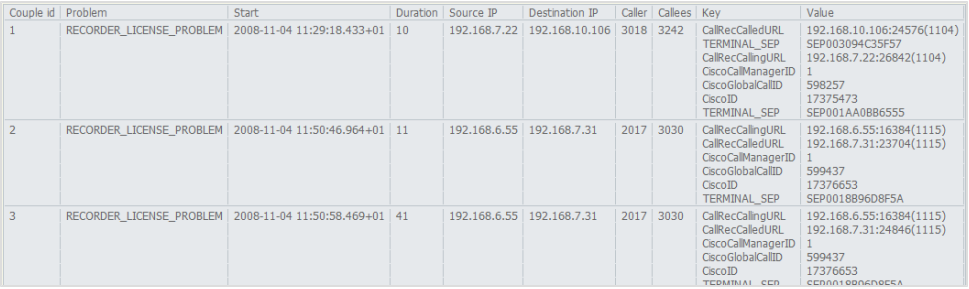


Figure 91: Error Report Setting

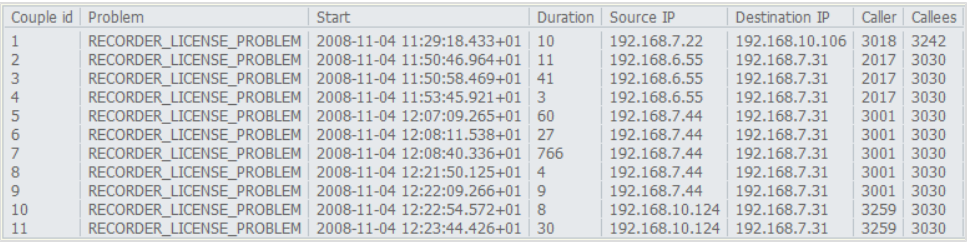
When you select **Bad Calls** from the Report drop down list, you can check the **With external data** box. This includes data from external databases in the Bad Calls report.



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 SEP001AA0BB6555
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 SEP0018B96D8F5A
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	192.168.6.55:16384(1115) 192.168.7.31:24846(1115) 1 599437 17376653

Figure 92: Bad Call Report with External Information

When **With external data** is selected, you can see additional information like **Key** and **Value**.



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 93: 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 allows visibility to potential overloads, creating queues before decoding.

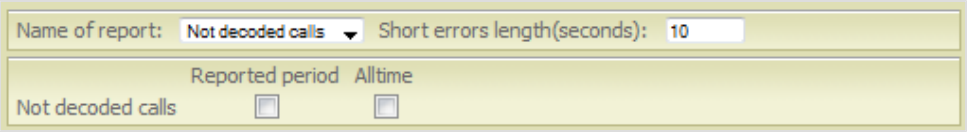


Figure 94: Not Decoded Call - Parameters

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 running on a distributed network, the Transfers report shows the performance of the system by analyzing whether calls were transferred within the system in the selected time range.

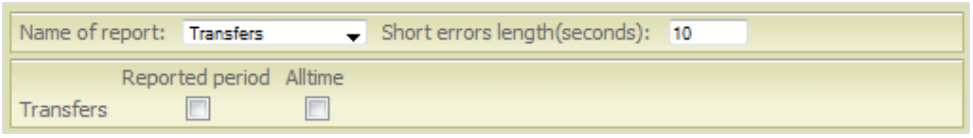


Figure 95: Transferred Recordings – Parameters

There are two parameters:

- **Outside** : Recordings which were recorded before the specified time range, but are processed in the selected time period.
- **Within**: Recordings which were processed in the selected time period.

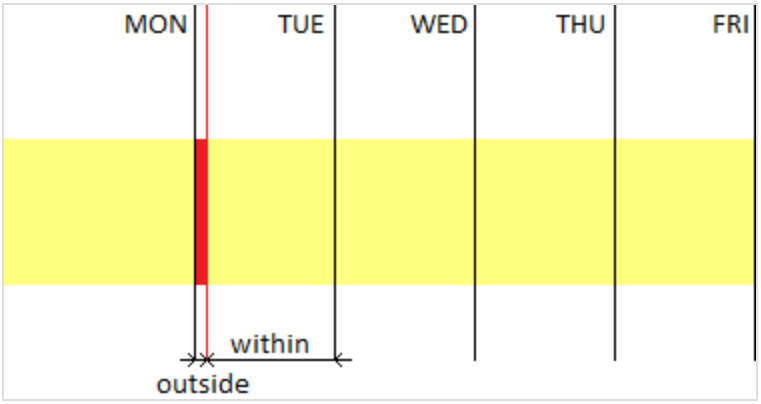


Figure 96: Transfers within and Outside the Specified Time Range

Chapter

9 SNMP

The Simple Network Management Protocol (SNMP) allows you to remotely monitor the parameters and functions of servers and applications.

Call Recording uses SNMP v2 messaging with an installed agent module, which supports SNMP GET (SNMP SET is not supported). This module is installed during GQM installation in a default configuration, which 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

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 6: 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.):

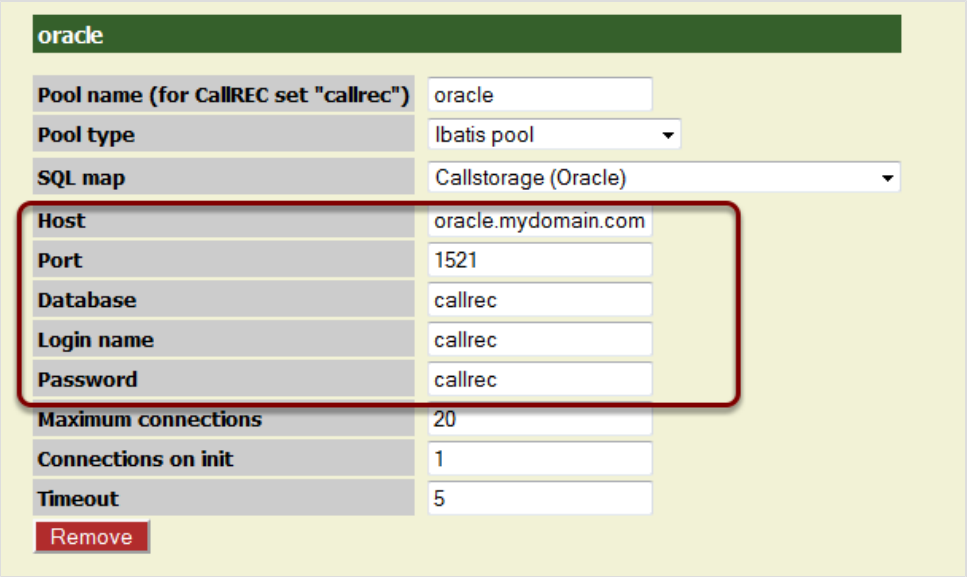
Node OID	Module Name
1.10.1	Core
1.10.2	Redlines
1.10.4	Observable Naming
1.10.5	Prerecording Server
1.10.6	Decoder Master Communicator
1.10.7	Config Manager Communicator
1.10.8	SRS Communicator
1.10.9	Remote NS
1.10.10	User Interface
1.10.11	Remote JTAPI
1.10.13	Mixer
1.10.15	Genesys Adapter

Table 7: 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 where the Oracle pool settings are.



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 and switch to the root account using the command :

```
su -
```

Using vim or a similar editor modify the SNMP configuration file for example:

```
vim /opt/callrec/SNMP/src/deployment.cfg
```

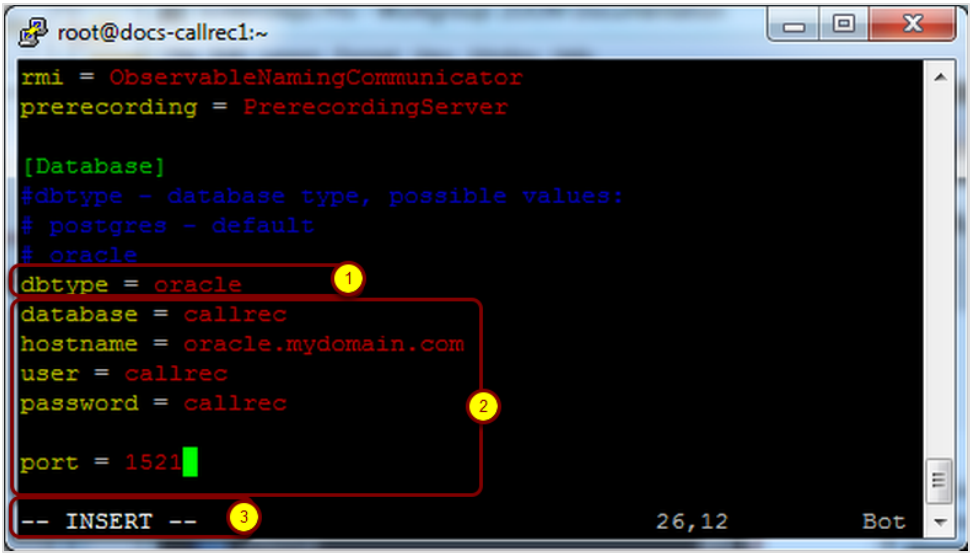


Figure 97: Database Settings in Config

Ensure that you are in **--INSERT--**mode by pressing the **i** key. 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

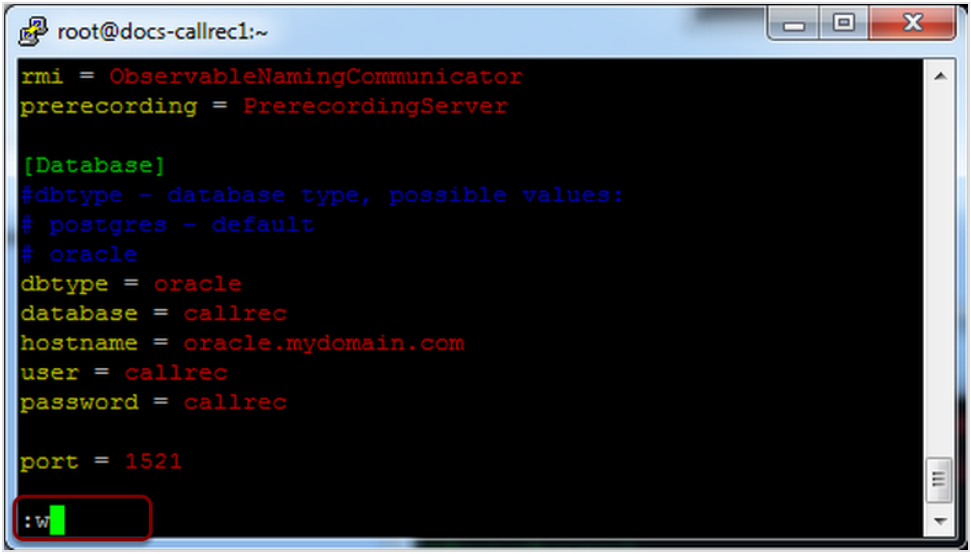


Figure 98: Image Caption

Press **Esc** to go into command mode. The **-- INSERT --** message at the bottom of the screen will disappear indicating that you are out of editing mode and enter the command `:w` to save the configuration. You should see a message to confirm that the config has been written for example:

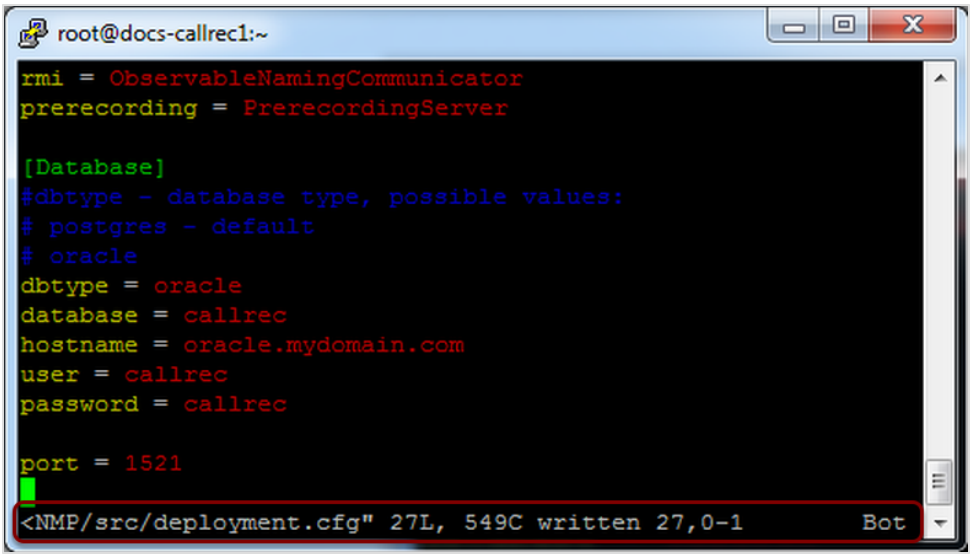


Figure 99: Confirmation Message

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, you should wait 5-7 minutes to allow SNMP to gather information.

Each object in your system listed in the Management Information Base (MIB) has its own error and information codes, allowing you to track the status of your system. Consult your SNMP documentation for further information.

Chapter

10 Prerecording

Prerecording allows users to selectively record calls. Prerecording saves all calls, but only temporarily. If a user wants to permanently save a call, they have an adjustable time period to identify the call so it will be converted to a file and saved. If a call is not identified by the user, it is erased from memory.

The call, which is 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. Postrecording (the call ends and recording is waiting).

Every stage has its own group of parameters in Call Recording and could be set different ways – for example, you may choose what users will be able to do with a call during every stage:

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

Important:

Prerecording cannot record calls made through secure HTTPS unless the http protocol is left enabled.

This chapter contains the following sections:

Configuring Prerecording in CUCM

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

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

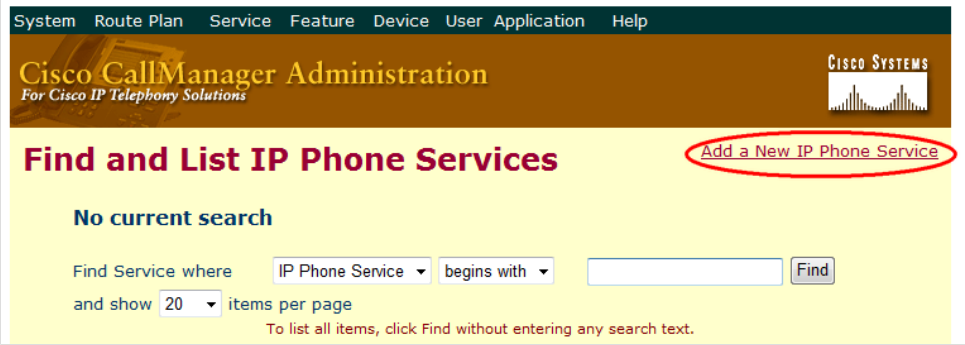


Figure 100: Adding a New IP Phone Service

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

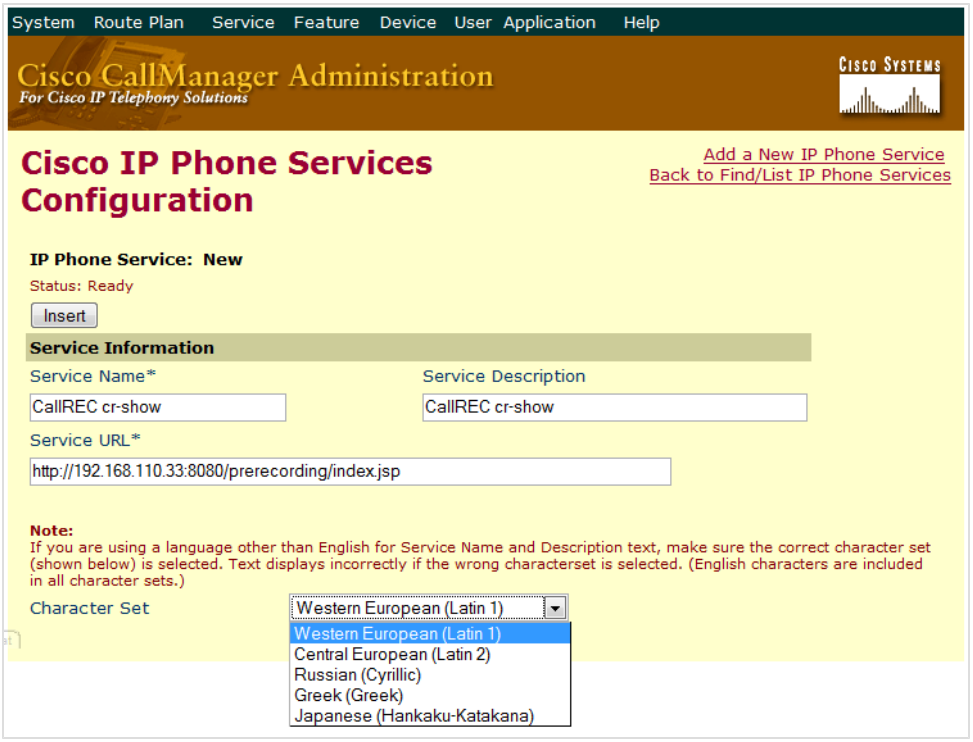


Figure 101: IP Phone Service Configuration

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 your Call Recording Core server
   - **Character Set** – choose a character set according to your preferred language
5. Click **Insert** to save your changes.

You will be returned to the **IP Phone Services Configuration** screen with a list of installed services.

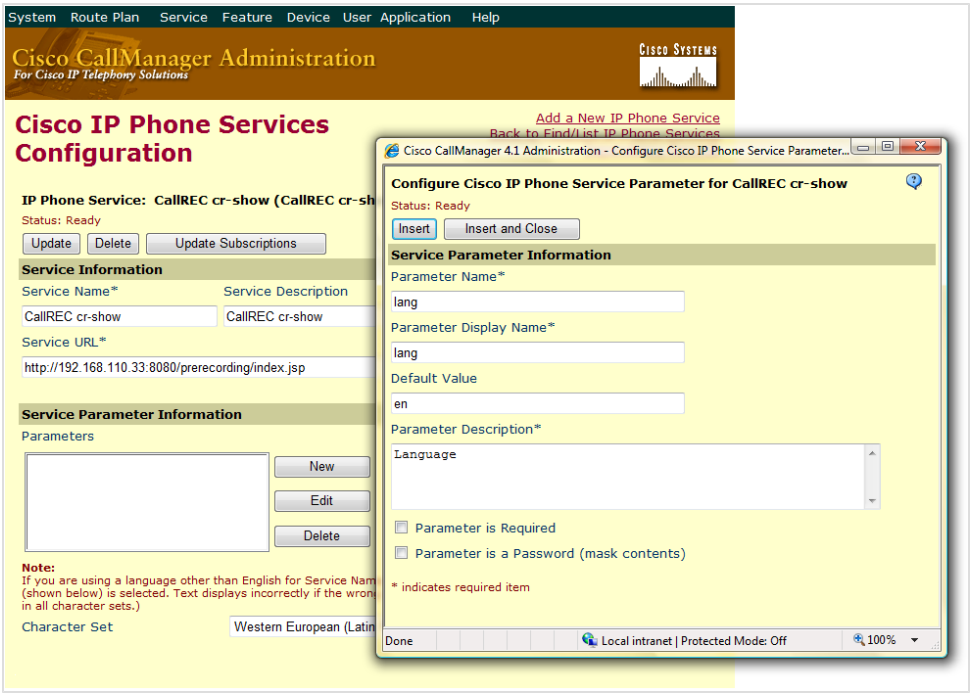


Figure 102: IP Phone Service Parameters

6. Select the Call Recording service from the list.

Important:

If your 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 your changes.

Making prerecording available for users

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

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

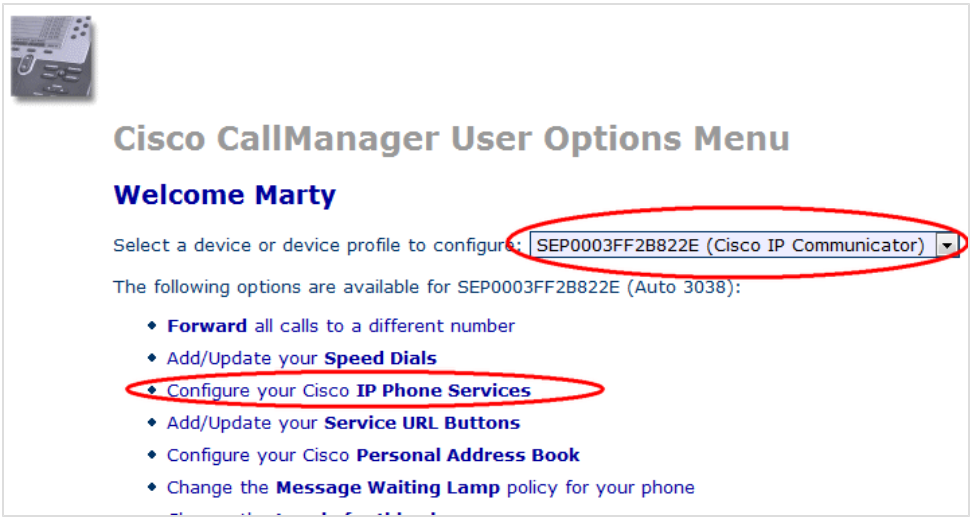


Figure 103: CUCM User Options

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

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

Figure 104: 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, please consult the CUCM Administration Guide.

Configuring Prerecording in Genesys Call Recording

After you have added Call Recording to the CUCM Configuration, you must specify available functions and prerecording settings within the Call Recording web interface. These settings add functions to all users' IP phone interface.

Log in to Call Recording with administrator privileges and navigate to **Settings > Configuration > Extras > Call Recording Prerecording**. Prerecording is listed in the additional installed modules.

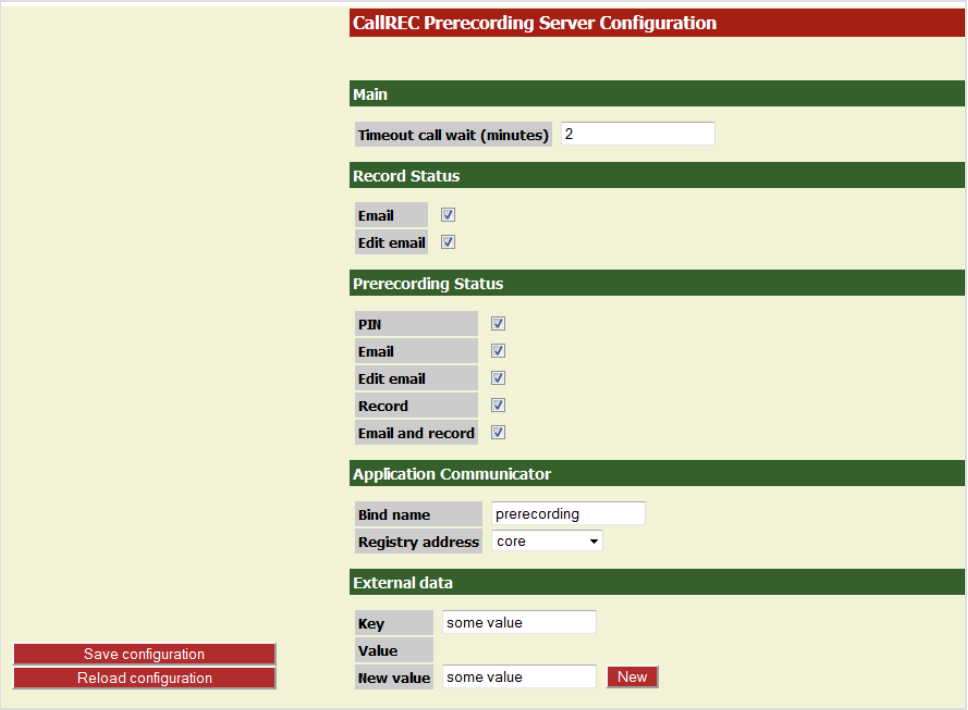


Figure 105: Prerecording Interface Options

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

Enter the following settings:

Main

Timeout call wait (minutes): Defines how long the user has after the end of a call to save that call recording. The default value is 2 minutes.

Record Status

Email: Enables the **Send by email** option in the service menu. The recorded calls will be 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.

Prerecording Status

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 will be 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.

Application Communicator

Bind name: Name of integration module for registering on RMI(for example, "Prerecording").

Registry address: Server with RMI service running. This is defined in the Servers part of configuration. (for example "core").

External Data

External Data (supplementary call information tagged to a call) can be added by a phone user during or after a prerecorded call (the same definable timeout applies 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 (saving).

To configure the External Data feature:
In the Prerecording External Data configuration section of the CallREC web interface, specify a Key (data name) and one or more New values (selectable

values), pressing the New button each time.
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 your CallREC Core server).
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 (saving).

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

Configuring Prerecording in CUCM 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 Cisco Unified Communications Manager 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 opens.

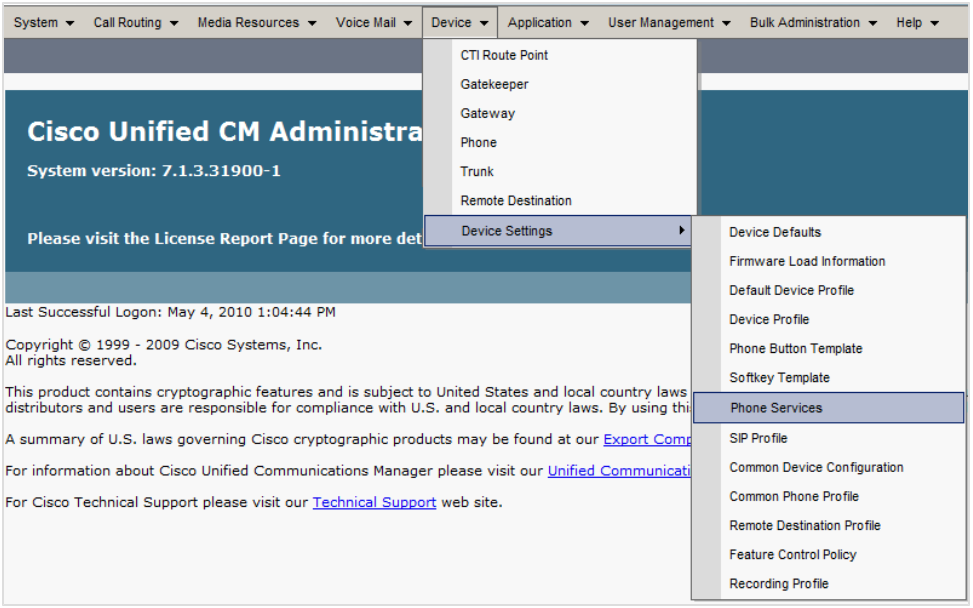


Figure 106: Phone Services Menu in CUCM 7

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

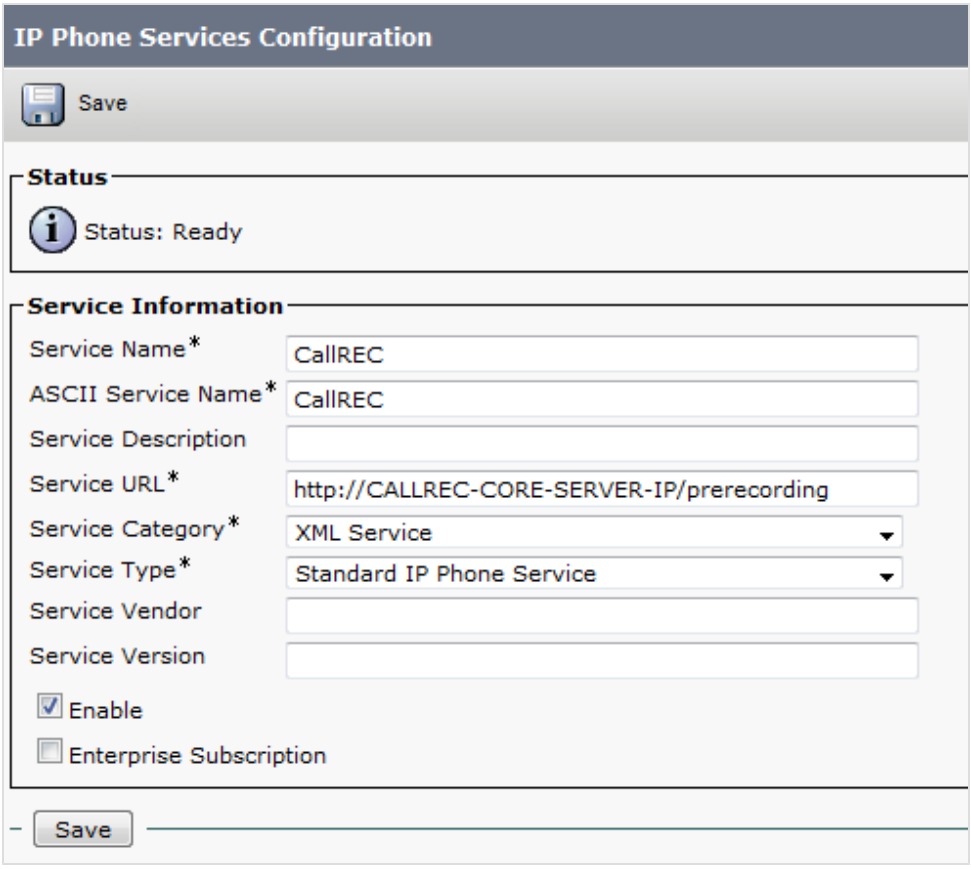


Figure 107: IP Phone Services Configuration in CUCM7

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 your Call Recording Core server.
   - Enable – check this option to enable the service (only for CUCM 7 and higher).

Important:
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 your changes.

Making Prerecording Available for Users

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

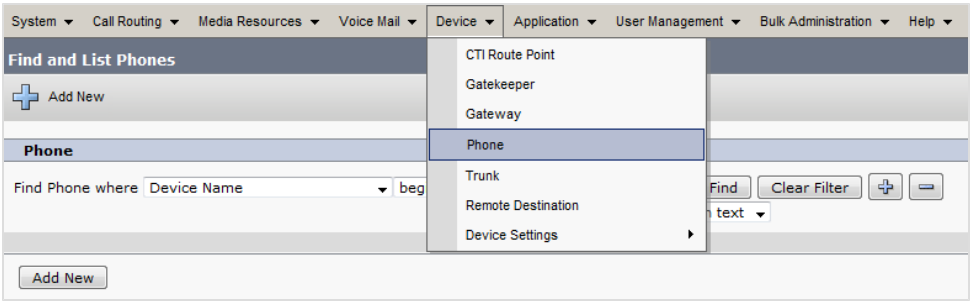


Figure 108: Phone Menu in CUCM 7

1. Select the device for which you want to enable prerecording via **Device > Phone**.

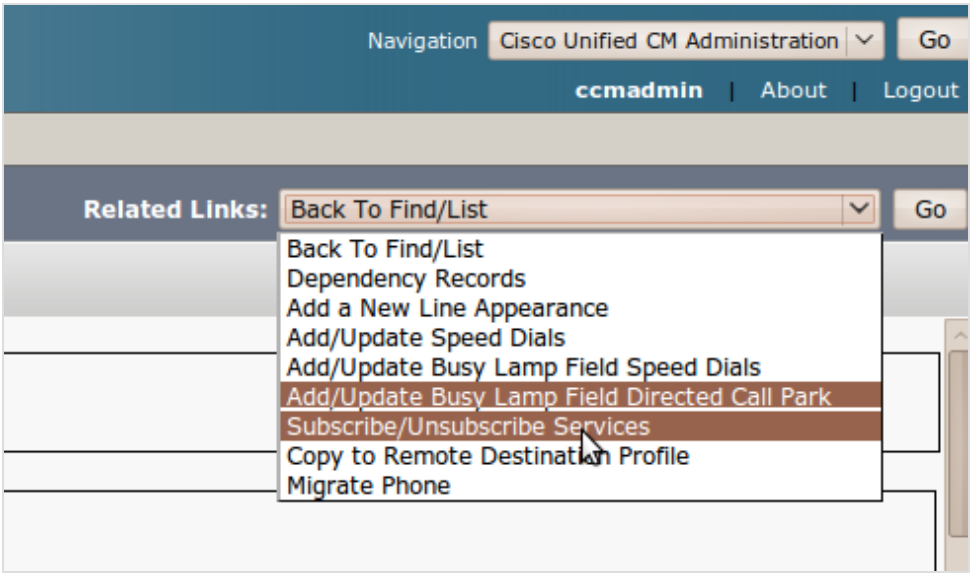


Figure 109: Related Links

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

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

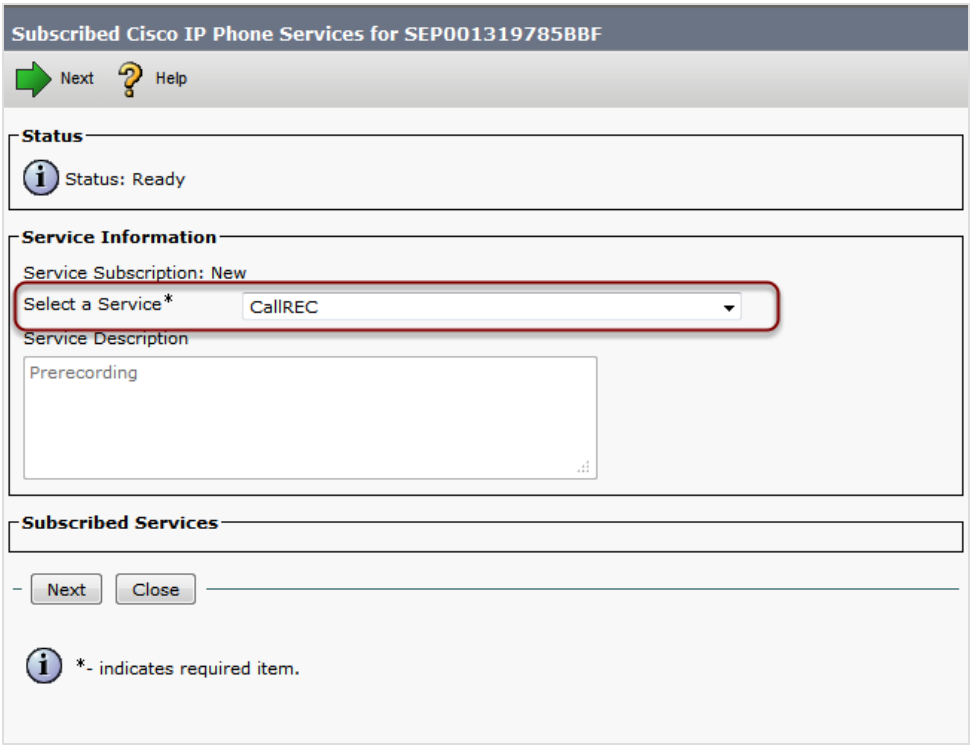


Figure 110: Select a Service Dropdown

3. Select the service from the **Select a Service** dropdown list and click **Next**.

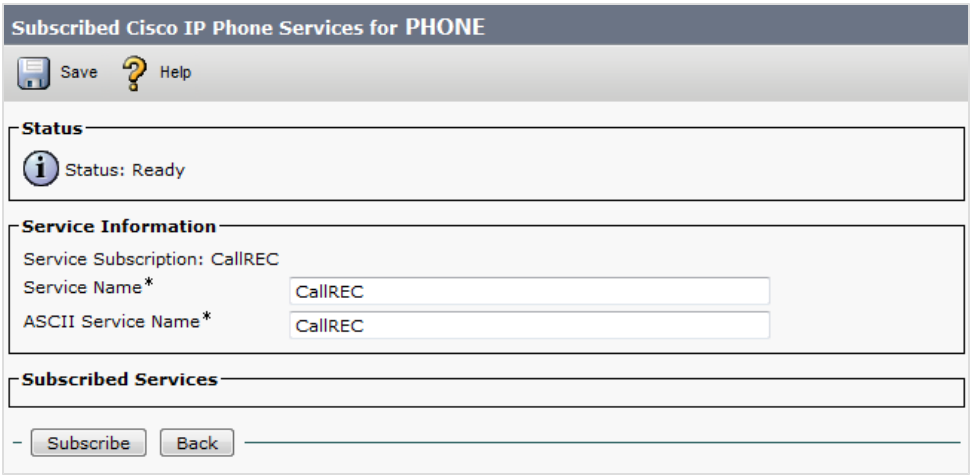


Figure 111: Subscribe to IP Phone Service CUCM 7

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

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

Important:

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 Cisco Unified Communications Manager Administration Guide.

Chapter

11 Live Monitor

Genesys Live Monitor (previously known as LiveMonitor) allows supervisors to listen to calls and add information as they happen. Live Monitor is a Java application that is launched when you click the Live Monitor tab in CallREC.

Live Monitor is normally installed along with Call Recording.

Important:
If you are using Network Address Translation (NAT), additional steps are necessary to enable Live Monitor – see below.

Important:
Live Monitor localization is based on the computer's regional settings that Live Monitor is initialized on. For example, In Windows 7 it is at **Control Panel > Region and Language > Keyboards and Languages**.

This chapter contains the following sections:

Configuring Live Monitor in Call Recording

To configure Live Monitor, log in to Call Recording with administrator privileges. Navigate to **Settings > Extras > Live Monitor** tab

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.

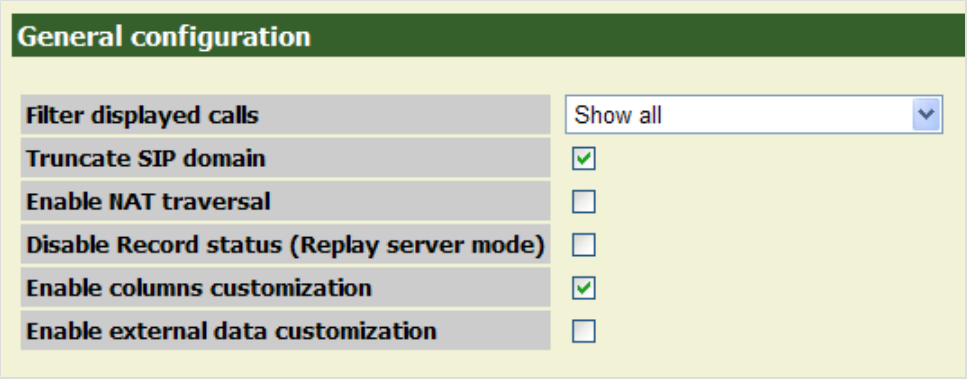


Figure 112: LiveMON Configuration

The following options are available:

Filter displayed calls: Allows the selection of what type of calls will be displayed. The options are as follows:

- **Show all** (default): All calls registered by Call Recording Core will be displayed, regardless of whether they are being recorded or not.
- **Recorded calls only**: Displays only these calls which are actually being recorded.
- **Recorded and prerecorded calls**: Displays all the calls which are either being recorded or which are being prerecorded and may be saved.

Truncate SIP domain: If enabled, SIP extension numbers will be 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: Allows users to choose which columns will be 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

From the Call Recording administrator's web interface, you can add external data options that allow supervisors to add information to Live Monitor. You can also restrict which types of calls 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 you can add to Live Monitor:

- **Text**: For supervisors comments.
- **List** : For choosing predefined options.
- **Checkbox**: For labeling calls with True/False values.

To add a new data row to Live Monitor:

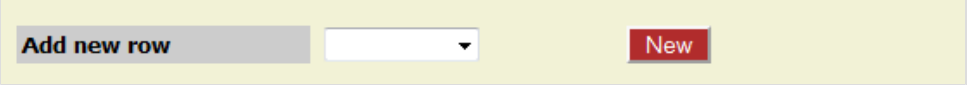


Figure 113: Adding a new row

1. Select a data type from the Add new row drop down list
2. Click **New**
   - Text:

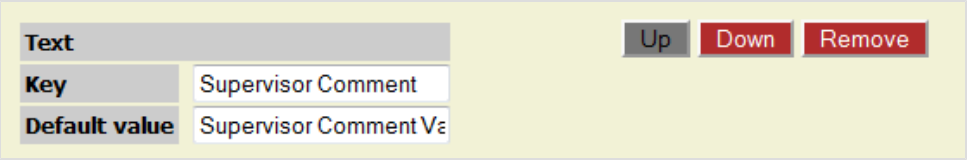


Figure 114: Adding a text field

- **Key**: Type the name of the text field.
- **Default value**: Type text that appears in the field by default.

Important:
This can be overwritten by users.

- Click **Save** configuration to save your new Live Monitor text box.
- List:

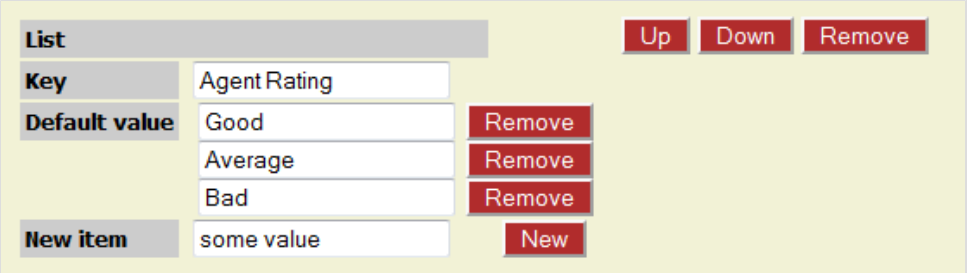


Figure 115: Adding a Selection List

- **Key**: Type the name of the list.
- **New item**: Type the value of an item then click **New**.
- **Items**: Displays the item values you have entered. To delete an item from the list, click **Remove**.

3. Click **Save configuration** to save your new Live Monitor list.
   - Checkbox:

Figure 116: Adding a checkbox

- **Key**: Type the name of the checkbox.
- **Default value**: Check this box to make the key a default value. If blank, the box is unchecked in Live Monitor.

4. Click **Save configuration** to save your 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 and click **Edit** .and modify the properties in the **Edit User** dialog field **Phone number**. You may set a range of phone number using ? as a wild card. For example 20?? will set 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, you must change your NAT settings and the open ports in your firewall for Live Monitor.

If you are using a strict firewall, you will need to open these ports in your firewall to allow 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**

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 8: 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 9: Genesys Default Ports for MSR/EPR/GIM

Tip:

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 it is better to change these settings through the Admin User Interface. Ensure you have a backup of all configuration files before changing port numbers.

Chapter

12 Known Issues

This chapter details the known issues.

This chapter contains the following sections:

CCM4 – Call Deregistration

There is a known JTAPI issue with Cisco Call Manager 4 installations, where terminals (phones) can be unexpectedly deregistered, preventing their calls from being recorded.

This state can be detected by running the following command with root permissions:

```
/opt/callrec/bin/callrec_status -name remoteJTAPI -state all -verbosity 5
```

All active devices configured for recording should have settings: `observed=true` and `in service= true`. If any have `in service=false`, they will appear to be registered but no calls will be recorded.

A workaround for this issue is to restart the JTAPI service:

```
[root@docs-callrec1 ~]# /opt/callrec/bin/rc.callrec_rts_jtapi restart
Stopping CallREC JTAPI: ..                                 [  OK  ]
Starting CallREC JTAPI:                                    [  OK  ]
```

Important:

Note that any active call recording sessions will be lost when the JTAPI service is restarted

This issue does not affect newer versions of CUCM (5.x+).

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 will be recorded as any other call. The calling extension (for instance, the customer) will be saved as the calling number, while the Hunt List Pilot Number will be saved as the called number. The extension number of the final Hunt List member who picked up the call (for instance the agent) will be saved in External Data as the key: `JTAPI_CALLED_TERMINAL_ADDRESS`.

Chapter

13 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.