Genesys Quality Management 8.1

Pre-implementation Guide

About Genesys

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

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

Notice

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

Your Responsibility for Your System's Security

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

Trademarks

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

Technical Support from Genesys

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

Ordering and Licensing Information

Complete information on ordering and licensing Genesys products can be found in the Genesys Licensing Guide.

Released by

Genesys Telecommunications Laboratories, Inc. www.genesyslab.com

Document Version: 81gqm_preimp_4-2013_8.1.511.00

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

This document describes how to prepare the call center equipment for the implementation of GQM. It contains all the pre-implementation tasks for the most common scenarios.

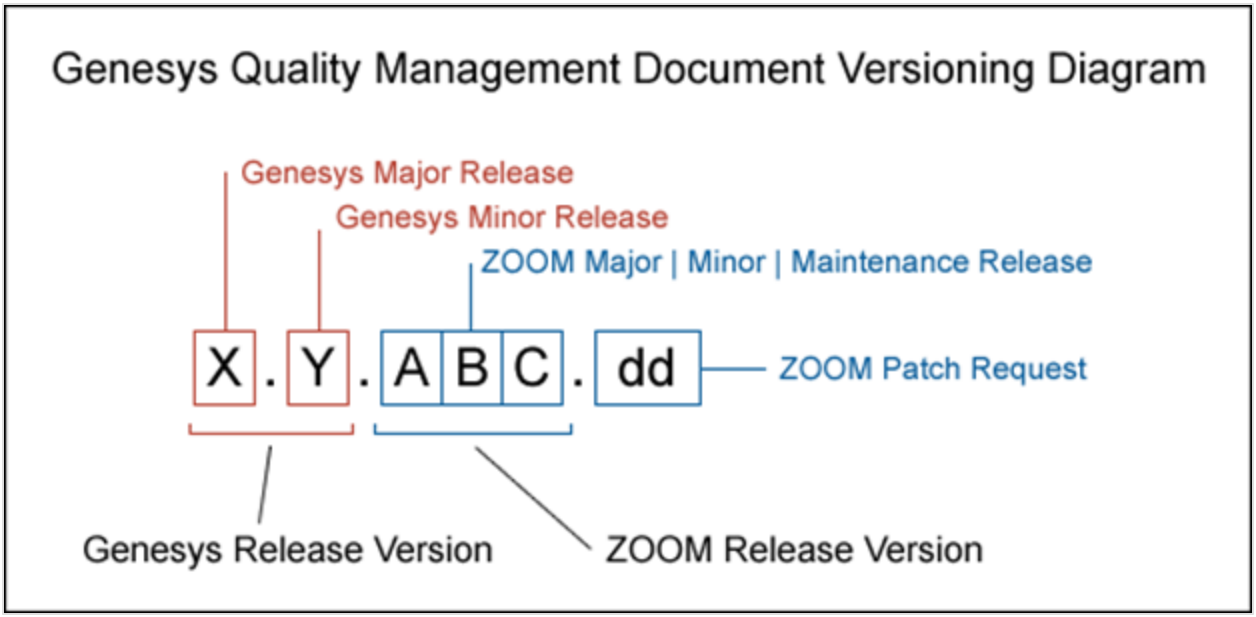
Audience

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

Document Version

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

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



Typographical Conventions

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

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

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

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

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

Expected Knowledge

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

- Basic knowledge of the Genesys Call Recording system features and functionality
- Unix system administration skills
- Network administration skills

Chapter

2 Important Pre-Installation tasks

Before installing GQM prepare the equipment and call center to interface with GQM. Follow the link that corresponds to the scenario that corresponds to the call center environment:

Preparing For Passive (SPAN) Recording on CUCM.

Preparing For Active Recording on CUCM.

Preparing For Genesys GIM.

Preparing For Genesys Active Recording Ecosystem and Genesys EPR

Preparing For Passive (SPAN) Recording on CUCM

To prepare for Passive Recording on CUCMthe Network Administrator must:

- Assign the IP address and Net mask for the eth0 Network Interface Card (NIC) on the GQM server.
- Provide network connectivity between the soft switches and the GQM server.
- Assign Gateway, Primary, and Secondary DNS addresses for the GQM server.
- Assign a hostname for thee GQM server. Create a fully qualified domain name for monitoring purposes.

For passive recording on CUCM:

1. Complete both tasks in Configuring CUCM for all Types of Recording.
2. Pre-configure the SPAN ports. Ensure that there is a second NIC connected to the server (eth1) and that eth1 is connected by cable to the Network with connectivity to the SPAN ports. (SCCP sniffer) Call Recording has to receive both signaling and RTP traffic on the SPAN port. Refer to Cisco documentation Configuring SPAN and RSPAN for more details on SPAN port configuration on Cisco switches. If using VMware then see VMware SPAN Port Configuration.
3. Install the operating system. See Installing the OS and Installation Files.

Preparing For Active Recording on CUCM

To Prepare for Active Recording on CUCM the Network Administrator must:

- Assign the IP address and Net mask for the eth0 Network Interface Card (NIC) on the GQM server.
- Provide network connectivity between the soft switches and the GQM server.
- Assign Gateway, Primary, and Secondary DNS addresses for the GQM server.
- Assign a hostname for the GQM server. Create a fully qualified domain name for monitoring purposes.

Important:

Recorded phones using Active Recording must support Active Recording (silent monitoring).

For an up-to-date list of all Cisco phones that support Active Recording see Unified CM Silent Monitoring Recording Supported Device Matrix.

To configure for active recording on CUCM:

1. Complete both tasks in Configuring CUCM for all Types of Recording.
2. Complete the tasks in Configuring CUCM for Active Recording. Note some steps are optional
3. Install the operating system.See Installing the OS and Installation Files.

Preparing For Genesys GIM

To prepare for Genesys GIM:

- Assign the IP address and Net mask for the eth0 Network Interface Card (NIC) on the GQM server.
- Provide network connectivity between the soft switches and the GQM server.
- Assign Gateway, Primary, and Secondary DNS addresses for the GQM server.
- Assign a hostname for the GQM server. Create a fully qualified domain name for monitoring purposes.

The following must be available:

- The T-Lib Primary server address.
- The T-Lib Backup server address.S
- The Config Primary server address.
- The Config Backup server address.

To configure for Genesys GIM:

1. Pre-configure the SPAN ports. Ensure that there is a second NIC connected to the server (eth1) and that eth1 is connected by cable to the Network with connectivity to the SPAN ports. Please refer to Cisco documentation Configuring SPAN and RSPAN for more details on SPAN port configuration on Cisco switches.
2. Add the CallREC_GIM Application Template into the Configuration Manager.
3. Add a new user (username and password) for Call Recording to communicate with Genesys in the Genesys Configuration Manager.

When the above are completed go to: Installing the OS and Installation Files.

Preparing For Genesys Active Recording Ecosystem or Genesys EPR

To prepare for Active Recording or EPR the Network Administrator must:

- Assign the IP address and Net mask for the eth0 Network Interface Card (NIC) on the GQM server.
- Provide network connectivity between the soft switches and the GQM server.
- Assign Gateway, Primary, and Secondary DNS addresses for the GQM server.
- Assign a hostname for the GQM server. Create a fully qualified domain name for monitoring purposes.

The following must be available:

- The Config Primary server address.
- The Config Backup server address.Genesys Labs, Inc.

Preparing Genesys Active Recording Ecosystem

To configure for Genesys Active Recording Ecosystem:

1. Add the CallREC_GIM Application Template into the Configuration Manager.
2. Add a new user (username and password) for Call Recording to communicate with the Genesys framework in the Genesys Configuration Manager.

When the above are completed go to: Installing the OS and Installation Files.

Preparing for Genesys EPR

To prepare for Genesys EPR:

1. Add the CallREC_GIM Application Template into the Configuration Manager.
2. Add a new user (username and password) for Call Recording to communicate with the Genesys framework in the Genesys Configuration Manager.
3. Pre-configure the SPAN ports. For enhanced passive recording (JTAPI sniffer) it is sufficient to SPAN only RTP traffic. Typically it is sufficient to configure one SPAN session that provides all necessary traffic to CallREC on one port (eth1). However if this is not possible there is option to connect multiple SPAN sessions to one server (of course more NICs is required). Refer to Cisco documentation Configuring SPAN and RSPAN for more details on SPAN port configuration on Cisco switches.
4. Set the rtp-info-password in the GenesysT-server configuration.

When the above are completed go to: Installing the OS and Installation Files.

Preparing for Avaya Communication Manager

To prepare for integration with Avaya Communication Manager the Network Administrator must:

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

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

There must be sufficient Medpro, DMCC and TSAPI licenses available.

See the *Avaya Whitepaper* for more information.

When the above are completed go to: Installing the OS and Installation Files.

Chapter

3 Installation Types

There are three types of Genesys Quality Management installation:

This chapter contains the following sections:

Cluster Installation

Cluster installation enables recording of large telephony installations, load balancing, and the ability to record geographically distributed networks.

The installation of a cluster solution requires:

- Solution design, description of the roles of particular servers.
- Scaling the solution, scaling the individual server parameters based on anticipated call loads.
- Description of individual server properties – installed components, partitioning, network connections, file system sharing.
- Installation of individual servers.
- Configuration of individual servers, network connection setup, files system sharing setup.

Please refer to the *Planning Guide* for the pre-installation and design steps.

Individual servers are installed using the procedure described in this document. Contact Genesys Labs, Inc. at http://genesyslab.com/support/contact for additional information on configuration and integration of a cluster installation.

High Availability Installation

High Availability installation is a special kind of cluster installation. Genesys GQM is installed on several servers in order to provide a High Availability solution. In case of failure of one of the servers there are backup servers which will continue providing recording capability, usually with no impact on recording functionality and recorded calls availability.

The High Availability installation is similar to a cluster installation. Please refer to the Planning Guide for pre-installation steps and to the Call Recording Administration Guide for post-installation and configuration steps.

Single server installation

Standalone installation means that Genesys GQM is installed on only one server.

This basic type of installation is described in this document.

Chapter

4 VMware SPAN Port Configuration

For SPAN and combination recording, the server must have one or more SPAN ports connected to the second NIC. The SPAN port must provide all the RTP packets related to the calls being made. If the data is not available, the system shows that the call was made, but does not contain any audio data.

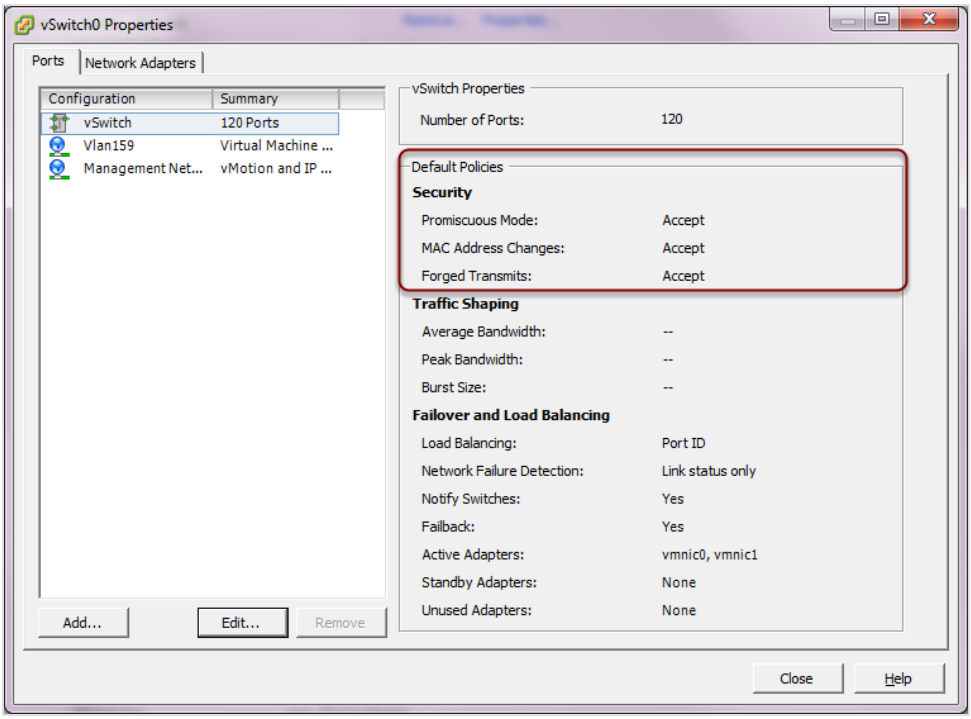


Figure 1: Vswitch Properties

Navigate to the control for the vSwitch and ensure that the following in **Default Policies** are all set to **Accept**.

- **Promiscuous Mode**
- **MAC Address Changes**
- **Forged Transmits**

Navigate to the Virtual Machine Properties

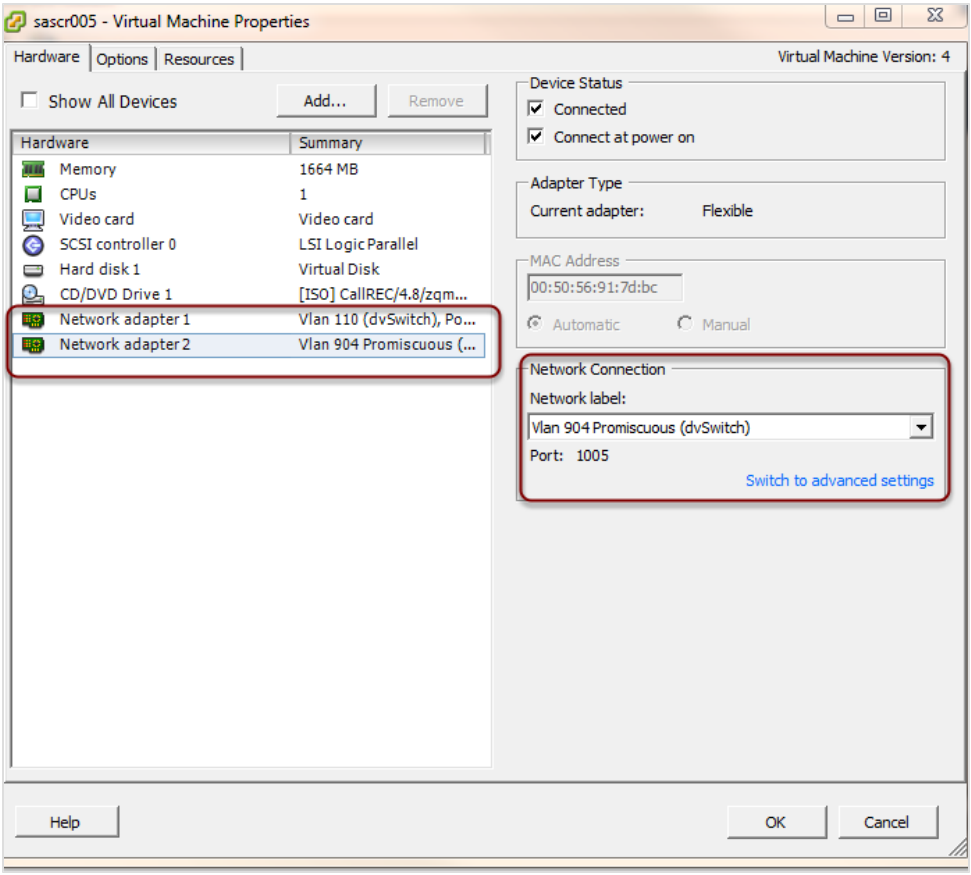


Figure 2: Virtual Machine Properties

1. Ensure that there are two network adapters
2. Ensure that each adapter is set to the correct Vlan

Please refer to Cisco documentation Configuring SPAN and RSPAN for more details.

In a non-virtual network environment by default eth0 is connected to local Intranet network and eth1 is connected to the Span-port of the switch. This Span-port mirrors the voice traffic that we should record.

Important:

If deploying an Active recording solution, SPAN ports are not required. Combination solutions, require both Passive (SPAN) and Active configuration.

Chapter

5 Configuring CUCM for All types of Recording

To configure CUCM for all types of recording:

- Create an Application User and password for JTAPI communications with the GQM server.
- Add Groups and Roles Permissions to the Application User.

Creating an Application User CUCM 6.x upwards

The creation of an Application User will enable Call Recording to observe “controlled devices” (phones). Include a device in Controlled Devices only for phones to be recorded. The omission of a phone in controlled devices will result in a “No streams recorded” error in Call Recording.

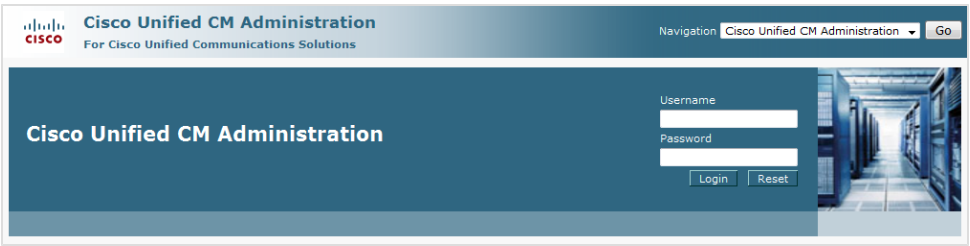


Figure 3: CUCM Logging In

Log in to Cisco Unified Communications Manager Administration.

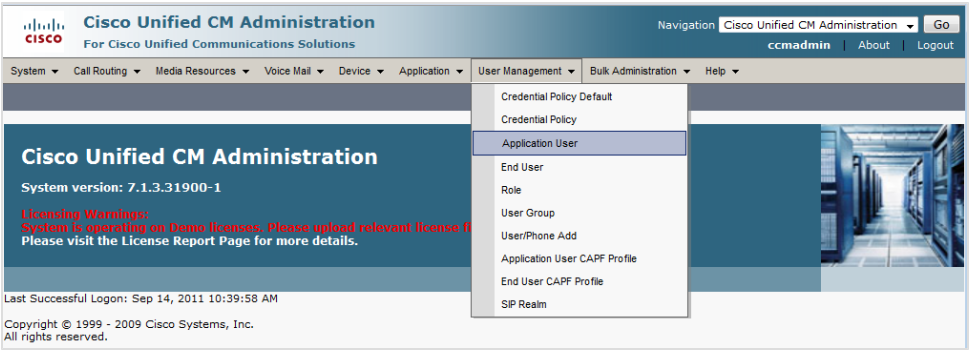


Figure 4: CUCM Application User Menu

Navigate to **User Management > Application User**.

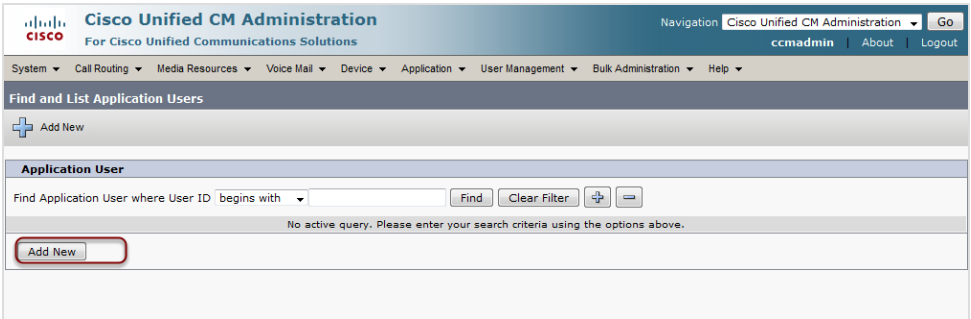


Figure 5: CUCM Add New

Select **Add New** the dialog below displays.

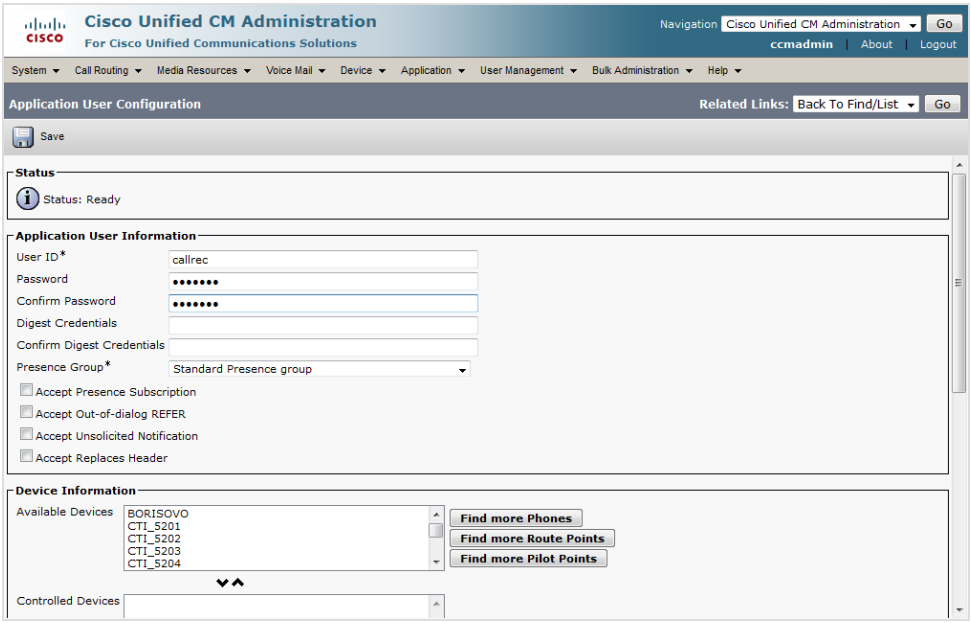


Figure 6: Enter Application User Credentials

1. Type a **User ID**, for example, callrec.
2. Type a password, for example callrec, in the **Password** field and type the same password in the **Confirm Password** field.

Write down the login name and password. Enter the same username and password when installing the JTAPI Client Library.

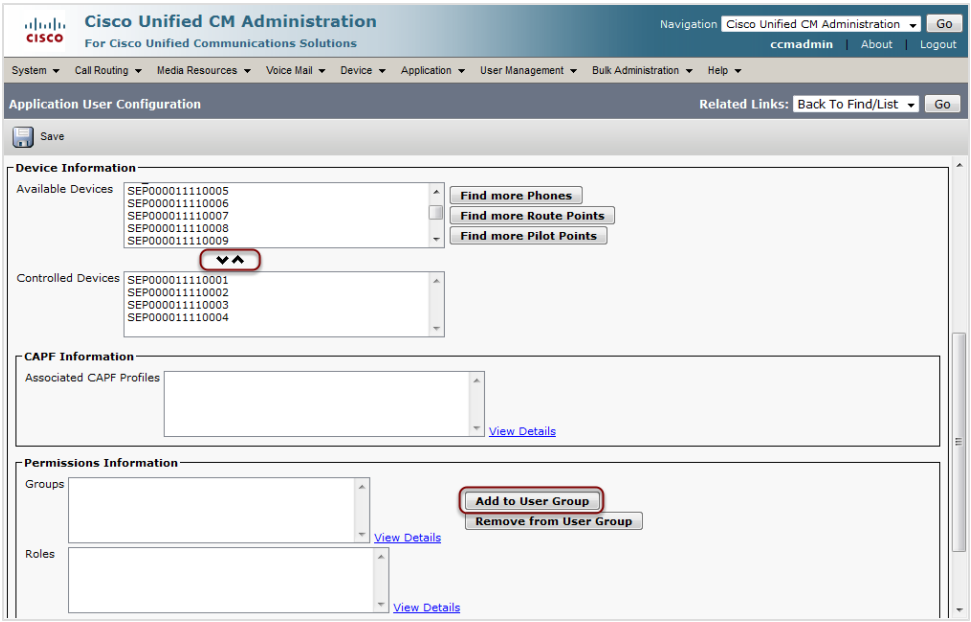


Figure 7: CUCM Assign Devices to Application User

1. Select the **Available Devices** to record using the arrows.
2. Click **Add to User Group**.The Find and List dialog box opens.

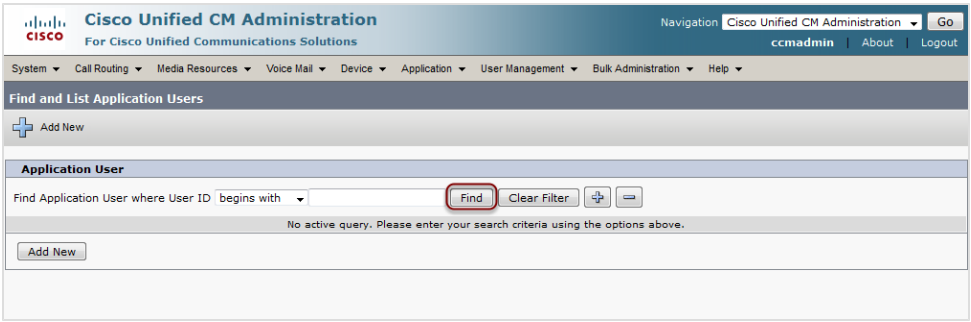


Figure 8: CUCM Find and List

Click **Find**. The Find and List dialog opens.

Adding Groups and Roles to Permission Information

This user must have privileges to see all users to be recorded or monitored.

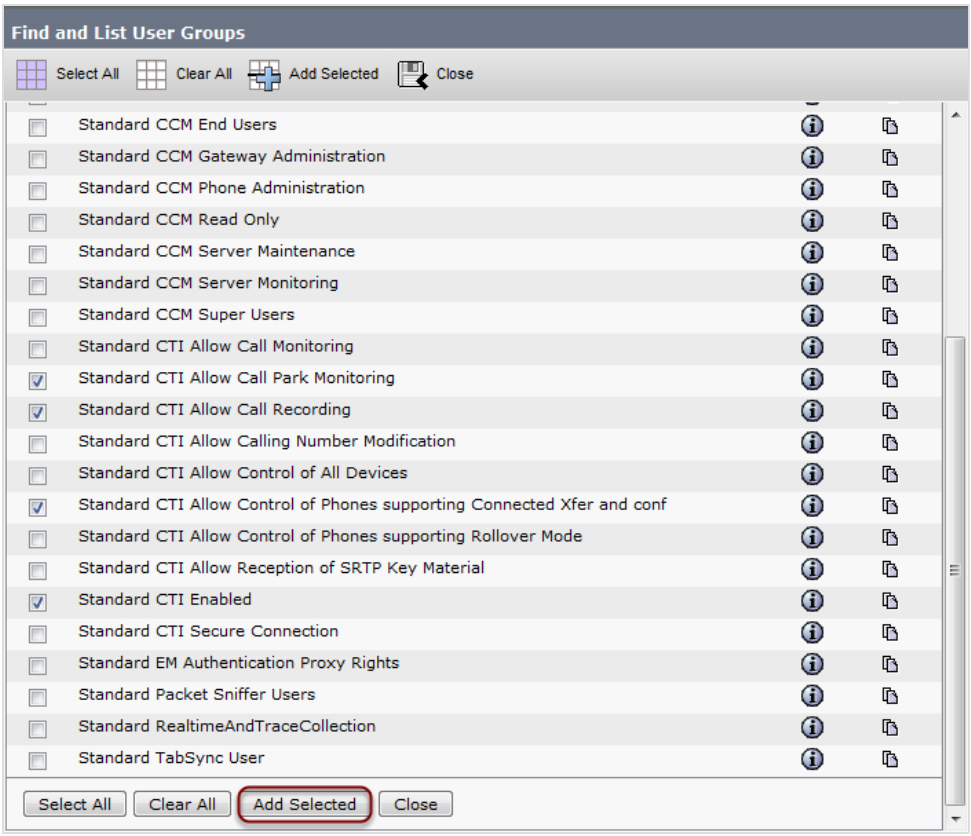


Figure 9: CUCM Find and List User Groups

Assign the Application user the roles

1. **Standard CTI Allow Park Monitoring**.
2. **Standard CTI Allow Call Recording** (For Active recording this step is not necessary for SPAN based recording).
3. **Standard CTI Allow Control of Phones supporting Connected Xfer and conf** (Cisco 89xx and 99xx series phones in CUCM 7.1 and above) by selecting their checkboxes.
4. **Standard CTI Enabled**.
5. Click **Add Selected**.

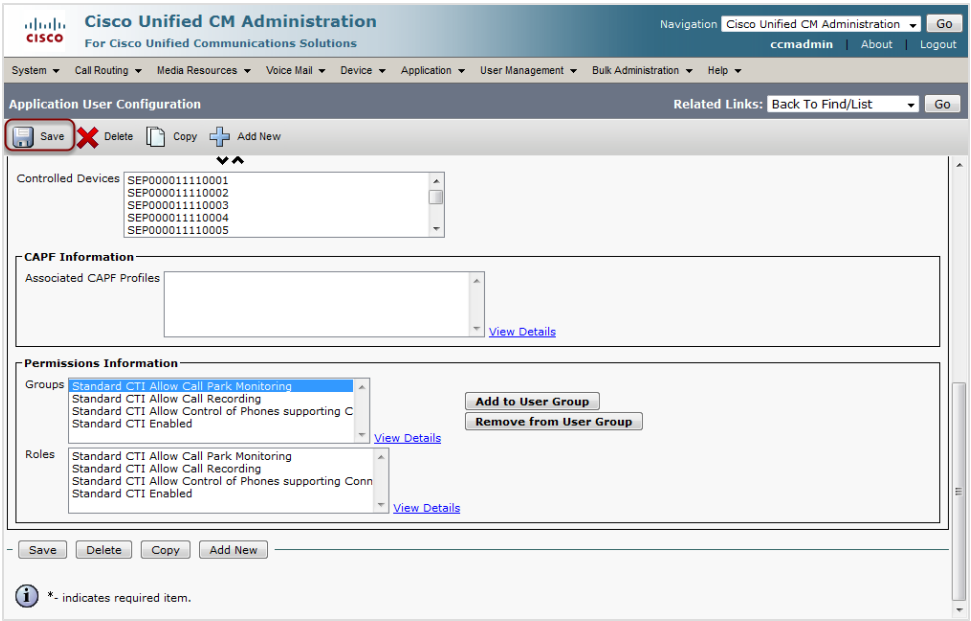


Figure 10: CUCM Application User Save Changes

Click **Save** On the Application User Configuration.

Chapter

6 Configuring CUCM for Active Recording

This chapter contains the following sections:

Configuring Tones for Recording (Optional)

Important:

Only enable warning tones if legally obliged to. These tones can be distracting or mistaken for a fault. Skip this step if an audible Recording Notification tone is not required.

1. Select **System > Service Parameters**.

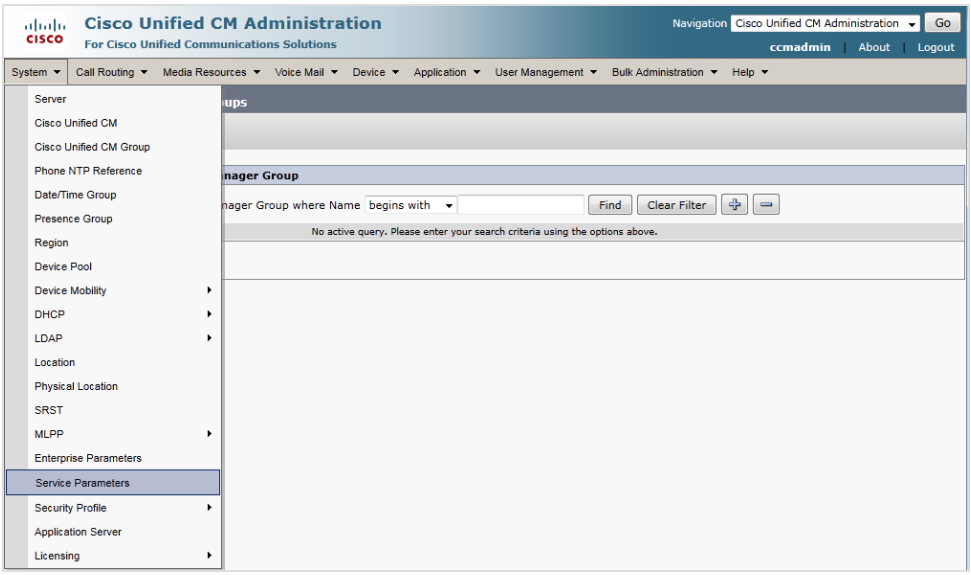


Figure 11: Service Parameters

The Service Parameter Configuration dialog displays.

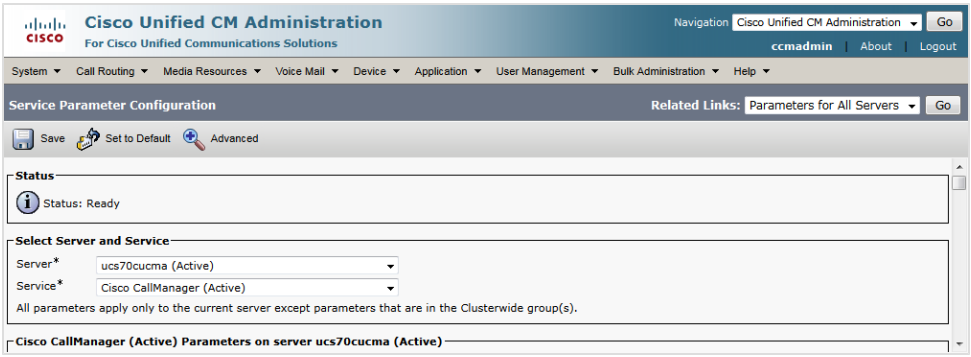


Figure 12: Service Parameter Configuration Select Server and Service

1. Select the Server from the dropdown list.
2. Select **Cisco CallManager (Active)** from the drop down list.
3. Scroll down to **Clusterwide Parameters (feature -Call Recording)** or use **CTRL+F** to find it quickly.

Set the values in **Play Recording Notification Tone to Observed Target** and **Play Recording Notification to Observed Connected Parties** to True if required.

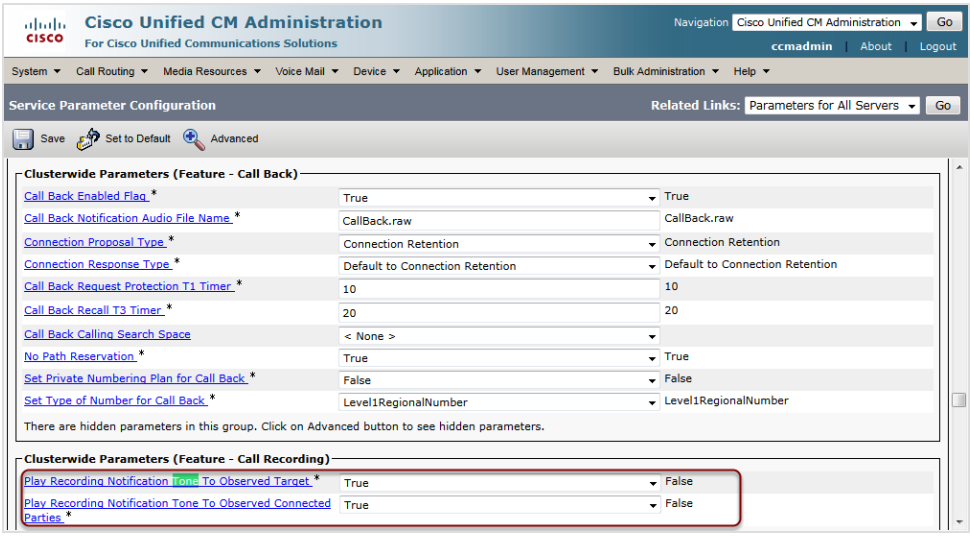


Figure 13: Service Parameter Configuration list

Creating a Recording Profile

The Recording Destination Address is NOT an IP address, it is a directory number, for example, 9105.

Refer to the numbering plan to select a number for the recording profile. Use an extension number that is not already assigned.

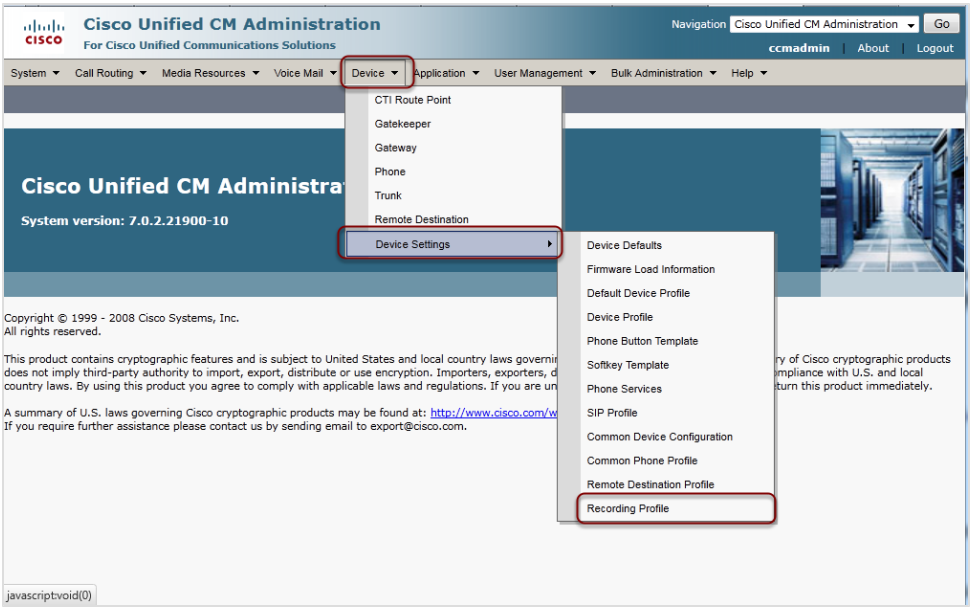


Figure 14: Select Recording profile

Select **Device > Device Setting> Recording Profile**.

The **Recording Profile** dialog opens.

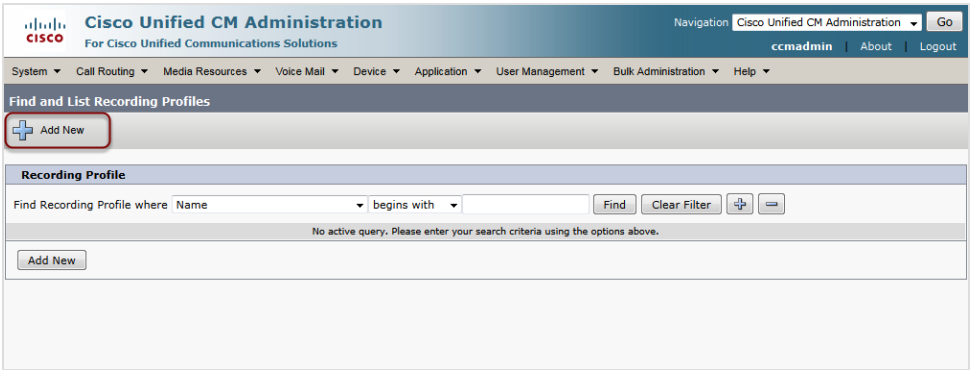


Figure 15: Recording Profile Add New

Select **Add New** the **Recording Profile Configuration** dialog opens.

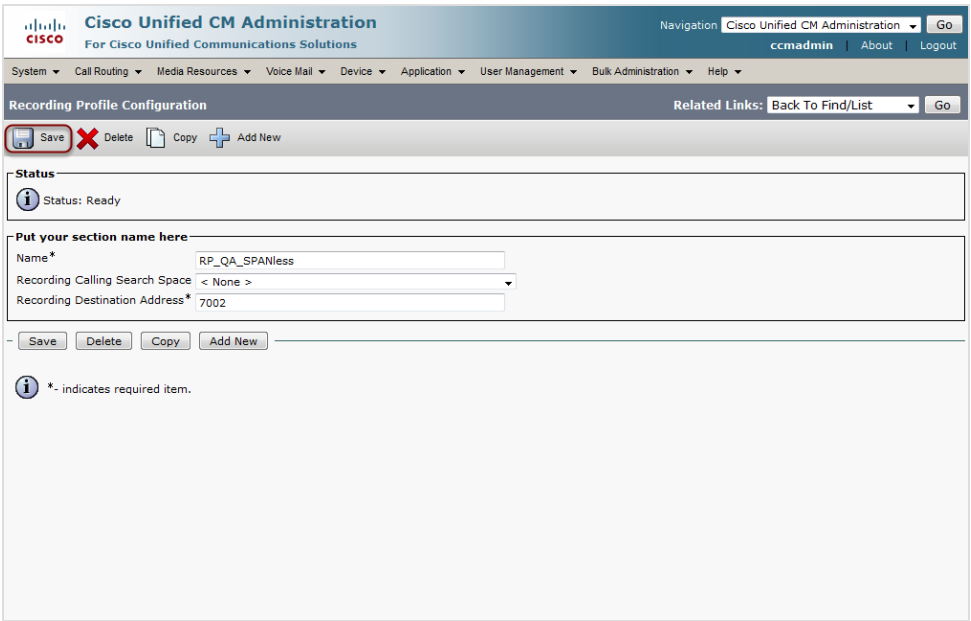


Figure 16: Recording Profile Configuration

1. Name the profile.
2. Type the **Recording Destination Address**.
3. Click **Save**.

Applying the Recording Profile to the Device

Select **Device > Phone**.

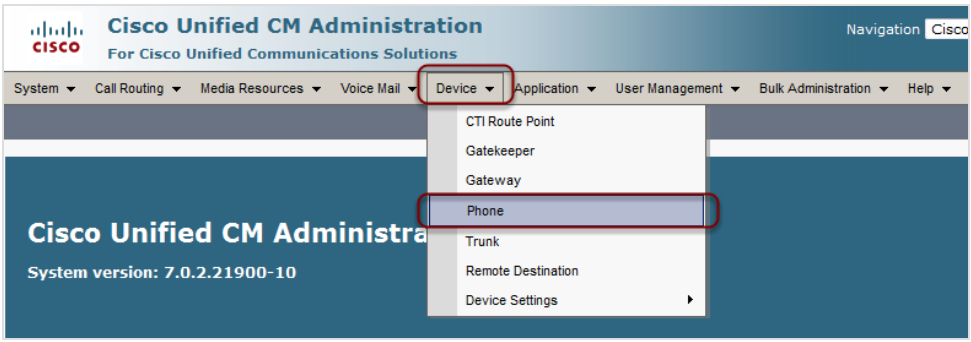


Figure 17: CUCM Select Device then Phone

The **Phone Configuration** dialog opens.

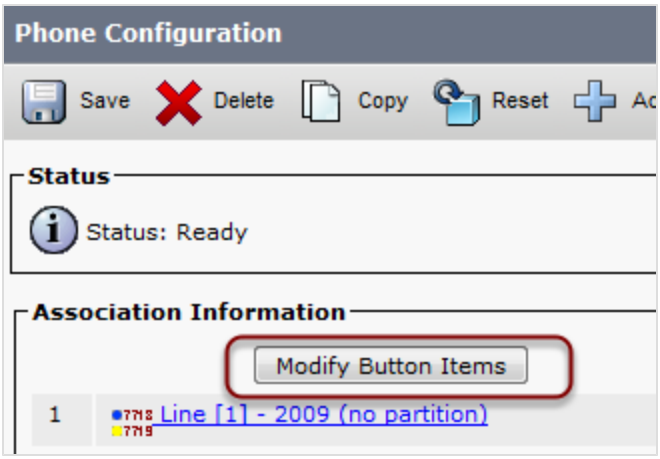


Figure 18: CUCM Modify Phone Configuration

Click **Modify Button Items**.

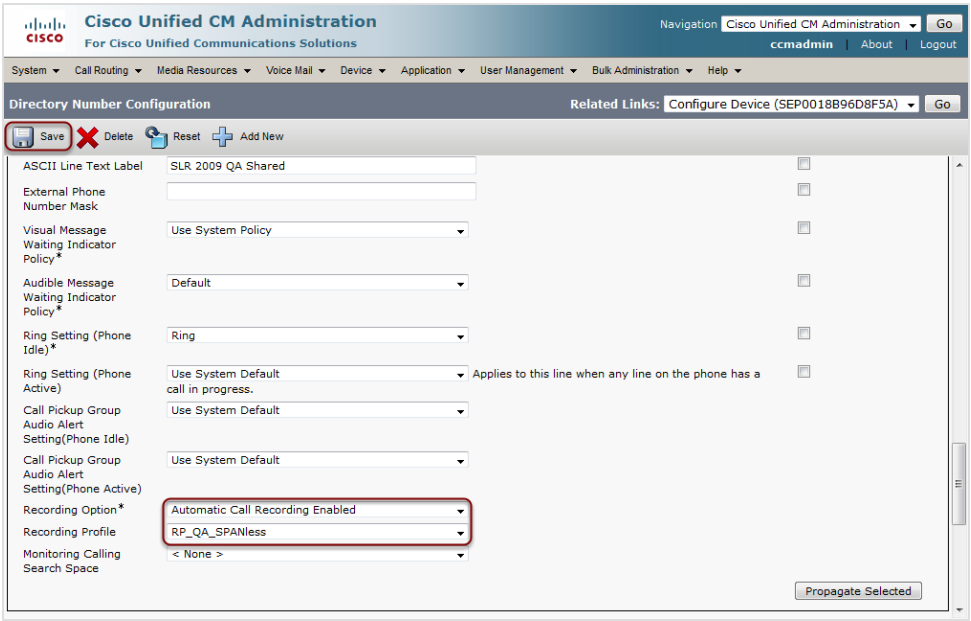


Figure 19: CUCM Assign Recording Profile to Phone

1. Select **Automatic Recording**.
2. Apply the configured Profile.
3. Click **Save**.

Creating a SIP Trunk to Point to the Recorder

The SIP Trunk points to the Recorder.

Create one Standard, Non Secure SIP Trunk for each Recorder (Destination Address = IP address of SLR Recorder).

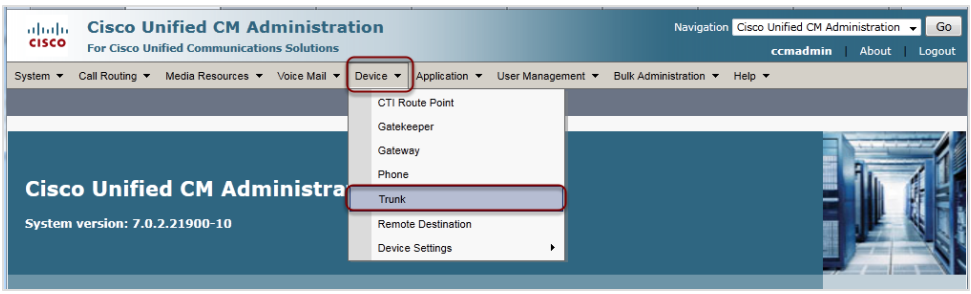


Figure 20: Select Device Trunk

Select **Device > Trunk**.

The **Find and List Trunks** dialog opens.

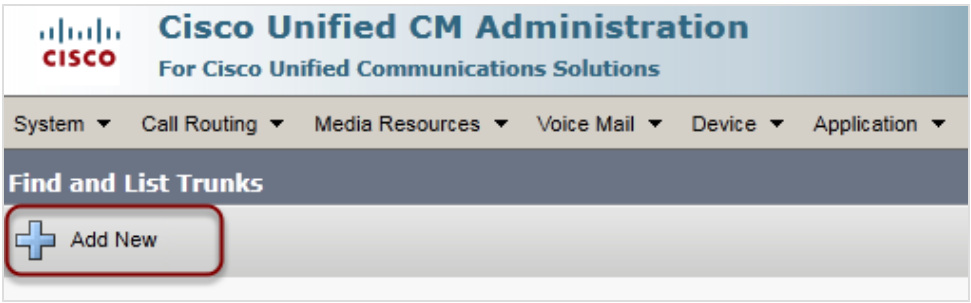


Figure 21: Find and List Trunks

Select **Add New**.

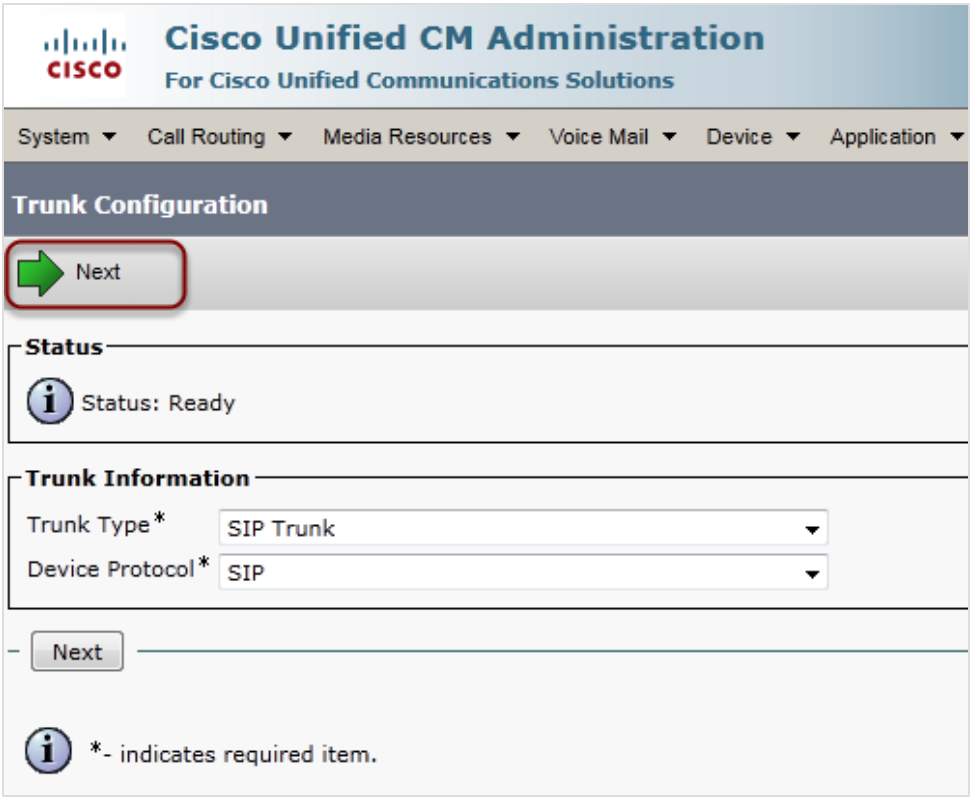


Figure 22: Trunk Information

1. Select the relevant **Trunk Information**.
2. Select **Next**.

Configuring the SIP Trunk

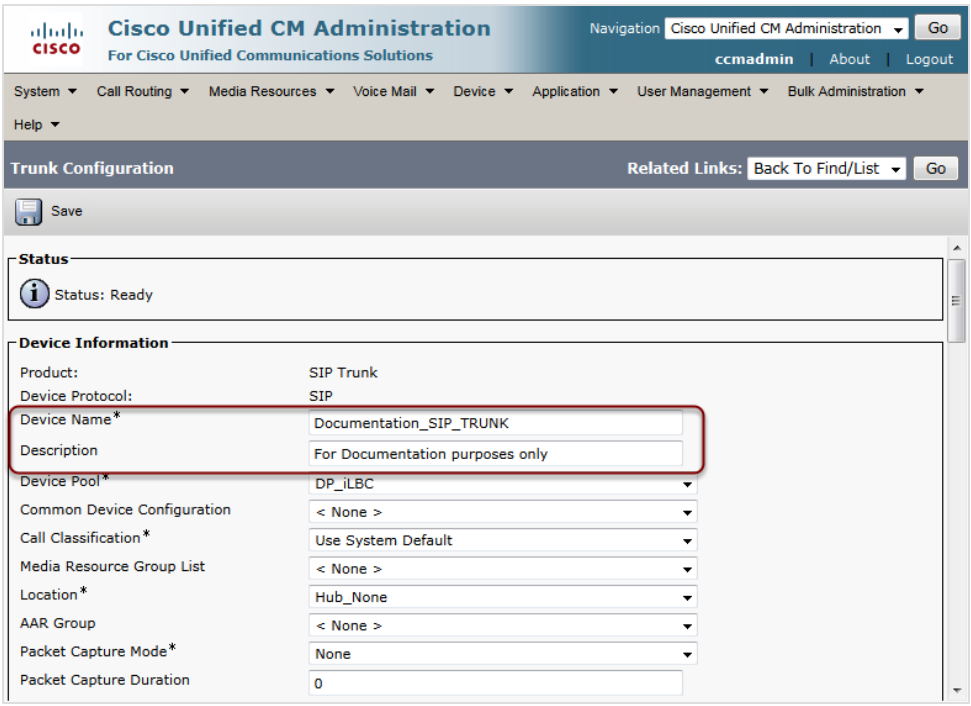


Figure 23: Add Device Name

Type a Device name and optionally a description.

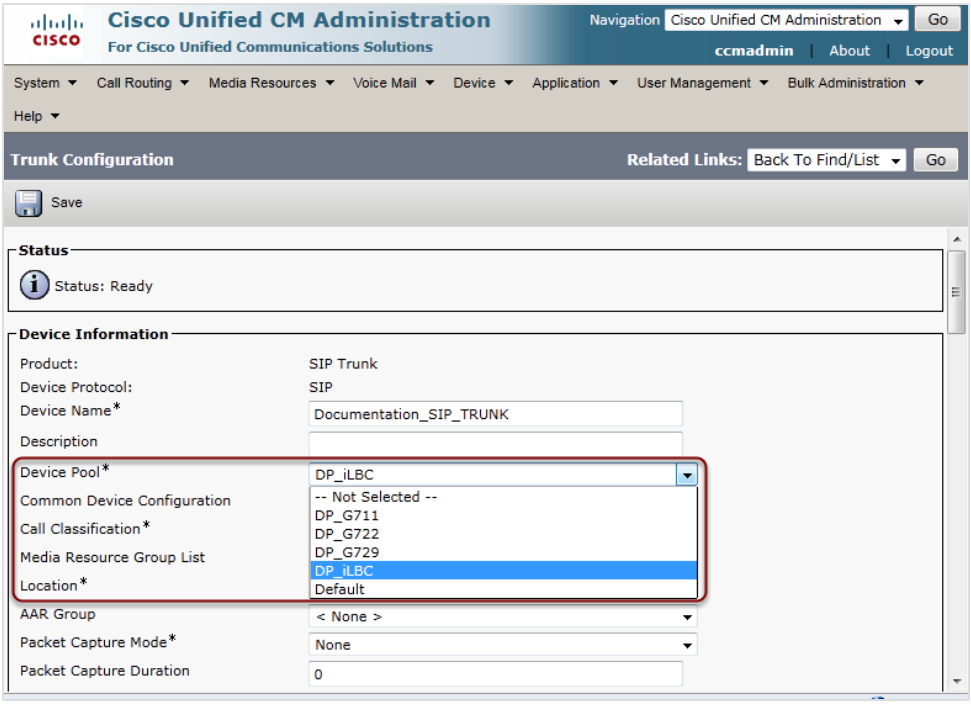


Figure 24: Select a Device Pool

Select a Device Pool from the dropdown list.

Scroll down to **SIP Information**.

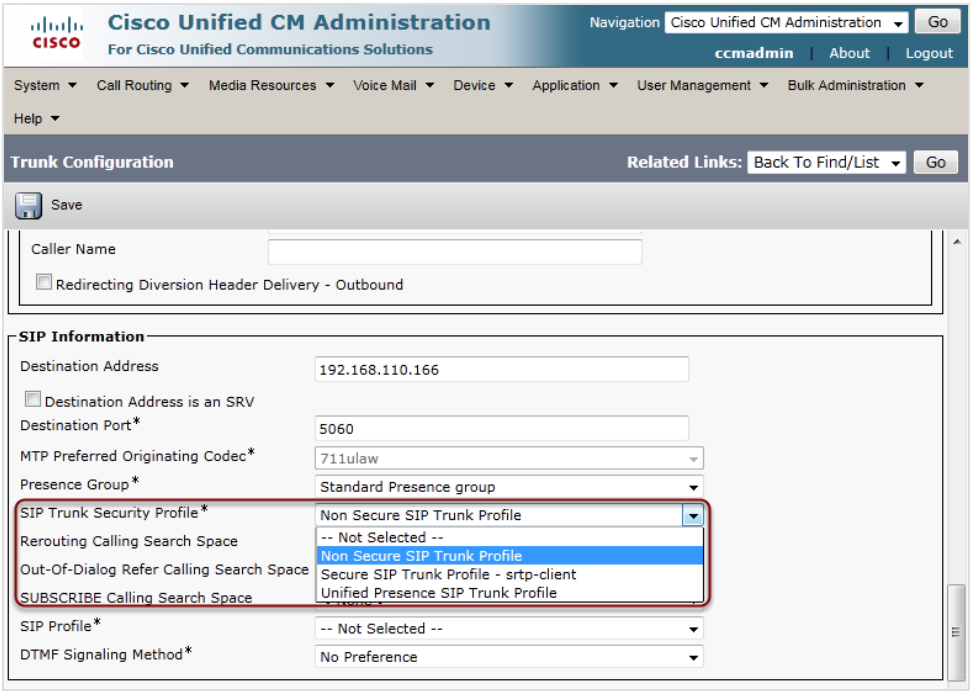


Figure 25: Select a SIP Trunk Security Profile

Select a SIP **Trunk Security Profile** from the dropdown list.

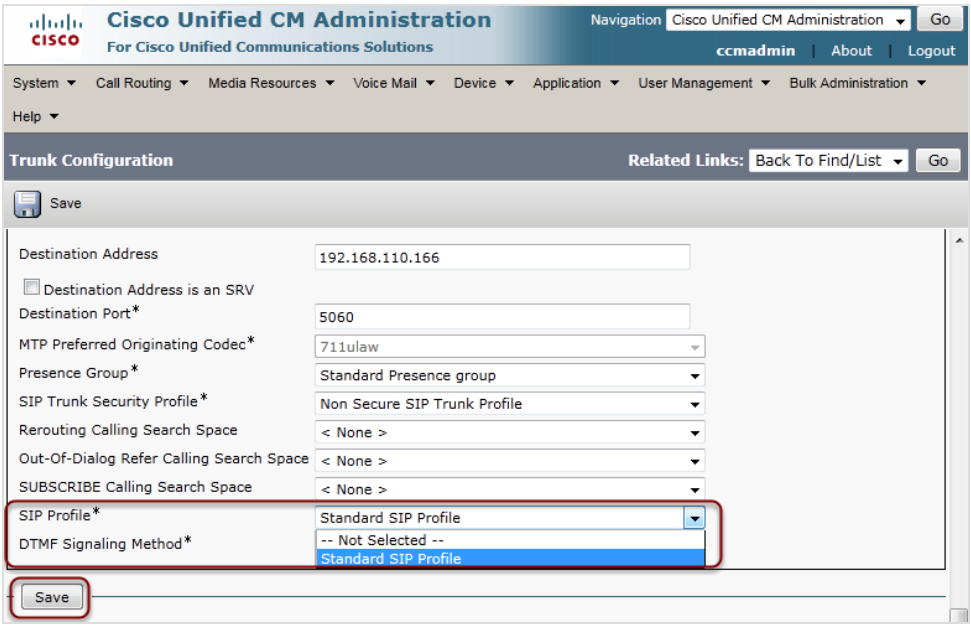


Figure 26: Select a SIP Profile

1. Select a **SIP Profile** from the dropdown list.
2. Click **Save**.

Creating a Route Group and Assigning the SIP Trunk

For High Availability. Skip this task if High Availability is not required.

For a single server installation, configure the Route Pattern SIP Trunk directly. Redundant installations require configuration of Route Groups and Route Lists.

The correct Distribution Algorithm is the Top Down method. Selecting the Circular method results in each stream being forwarded to a different recorder server, which is inefficient.

If there are 2 Recorders, configure 2 Voice Recording Profiles with two extensions 1111 and 2222. Route Patterns for these numbers will point to the Route List. The first route list will contain Route Group where Recorder1 will be the primary recorder and Recorder2, the secondary. The other route group will be configured in the opposite way:

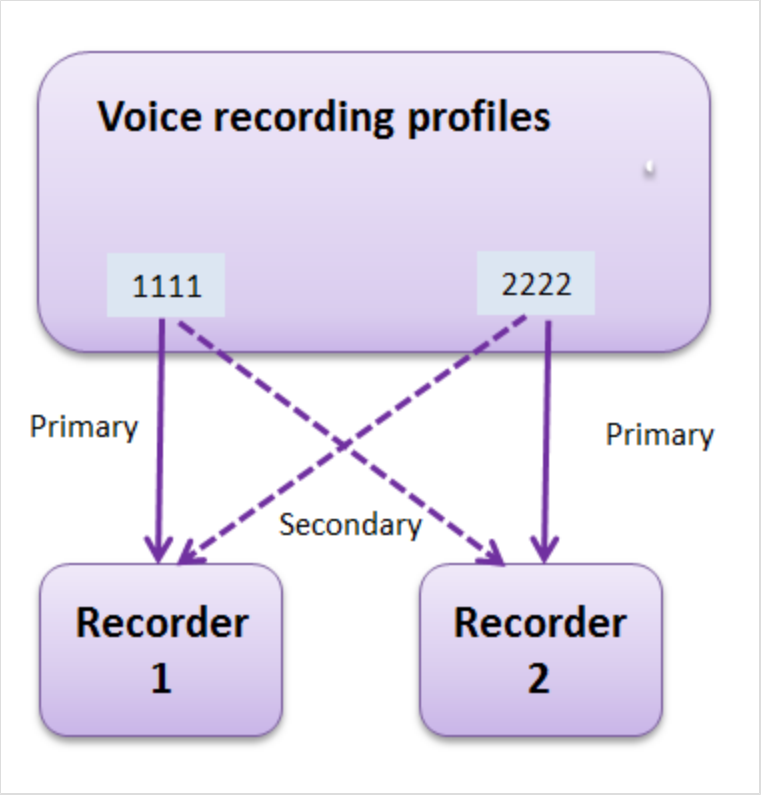


Figure 27: Showing Primary and Secondary Connections to Recorders

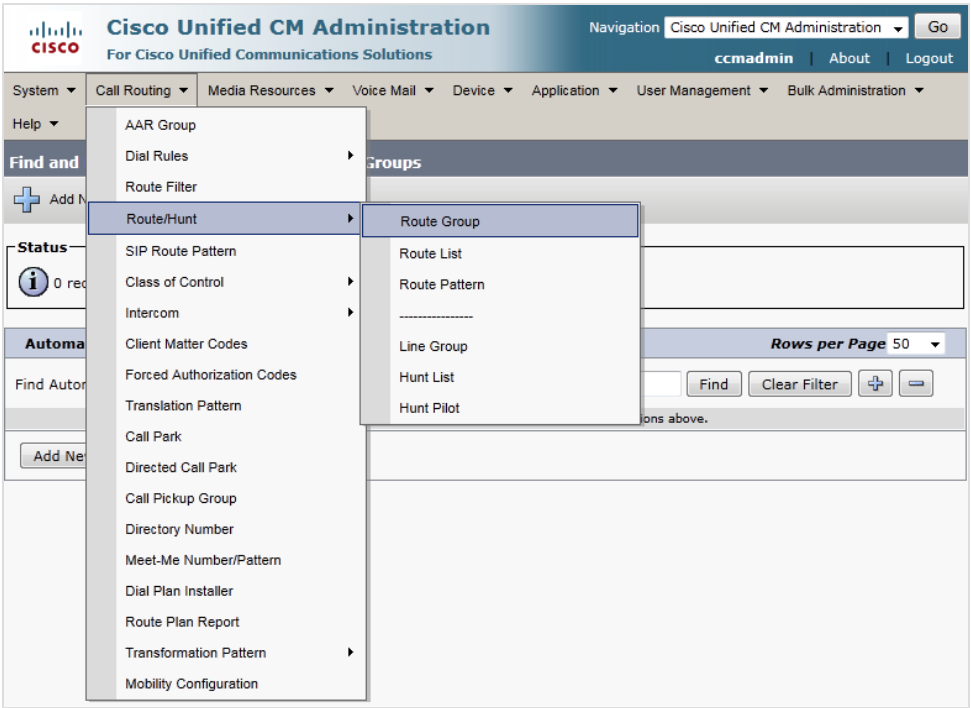


Figure 28: Select Route Group

Select Call **Routing > Route/Hunt > Route Group**.

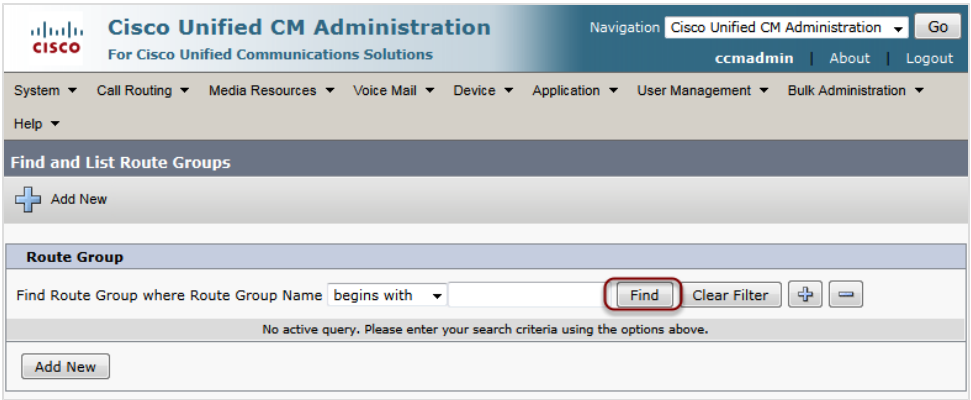


Figure 29: Find and List Groups

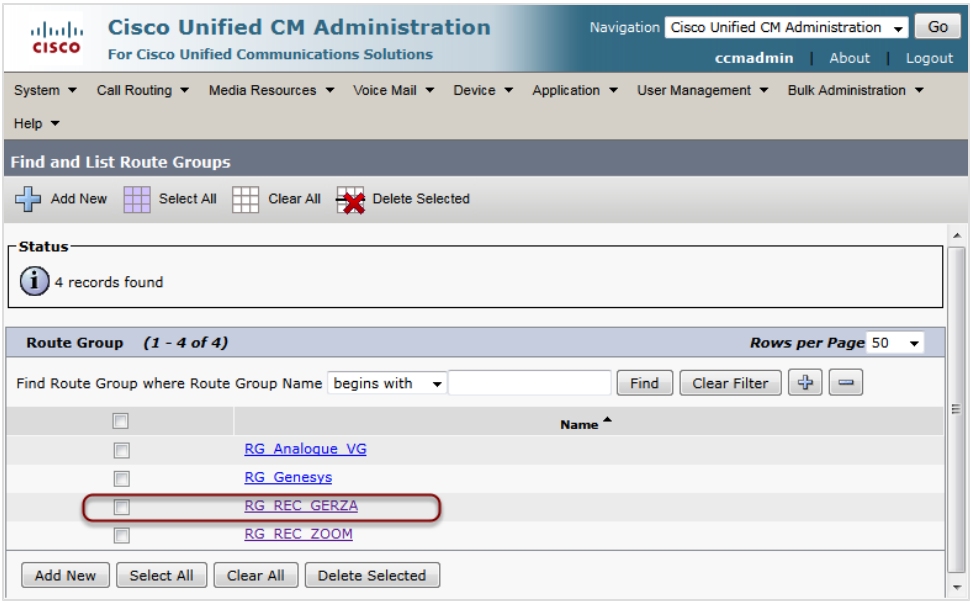


Figure 30: Select the Route Group

Select the **Route Group**.

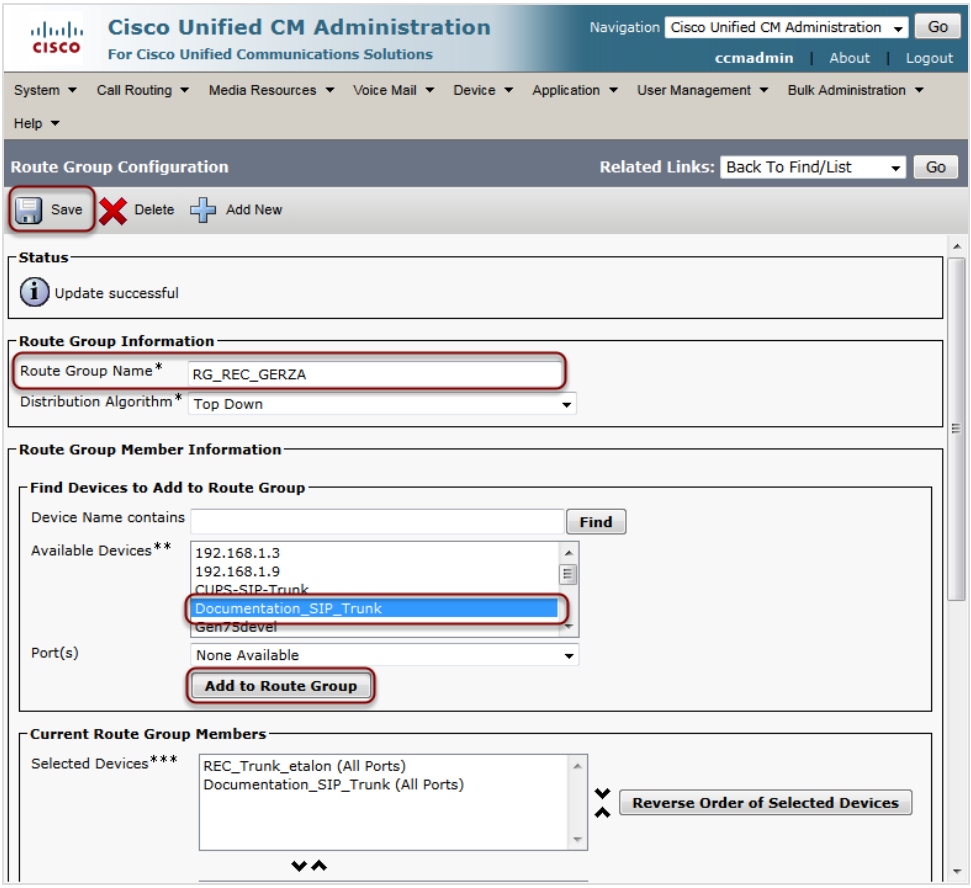


Figure 31: Route Group Confirmation

1. The **Route Group Name** displays.
2. Assign the SIP trunks to the **Selected Devices**.
3. Click **Add to Route Group**. The SIP trunk will appear in the **Current Route Group Members** list.
4. Click **Save**.

Creating a Route List and Assigning the SIP Trunk

For High Availability. Skip this task High Availability is not required.

The Route List will contain only one Route Group which includes both primary and secondary Recorders (SIP trunk).

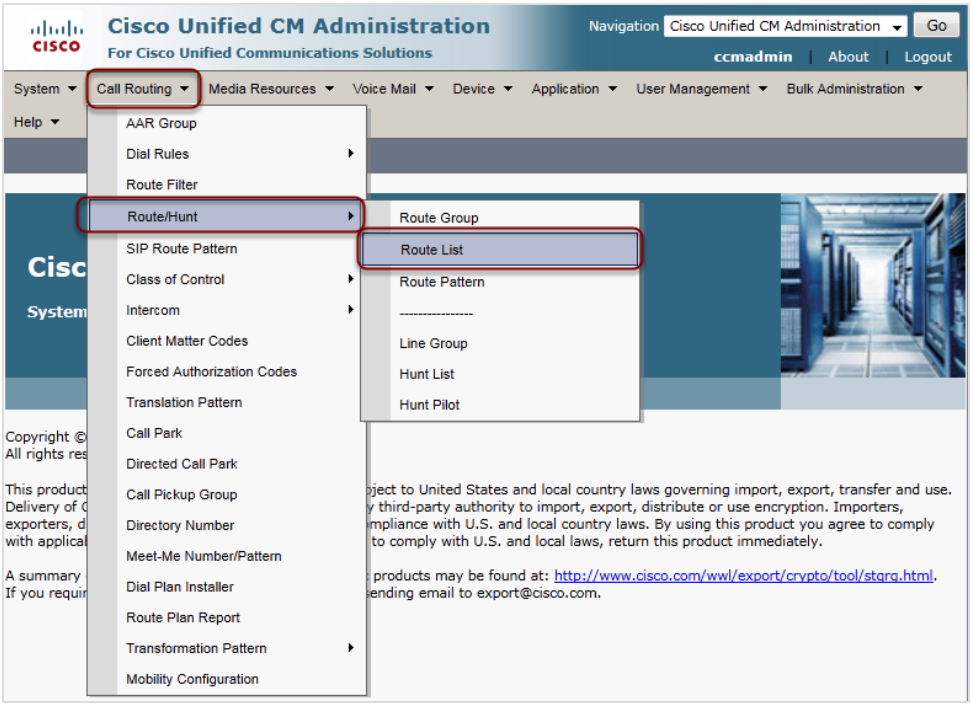


Figure 32: Select Route List

Select **Call Routing > Route/Hunt >Route List**.

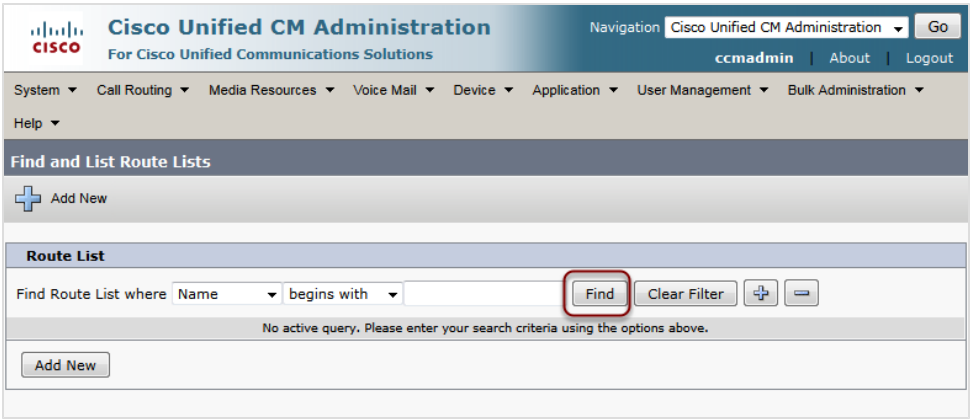


Figure 33: Find and List Route List

Click **Find**.

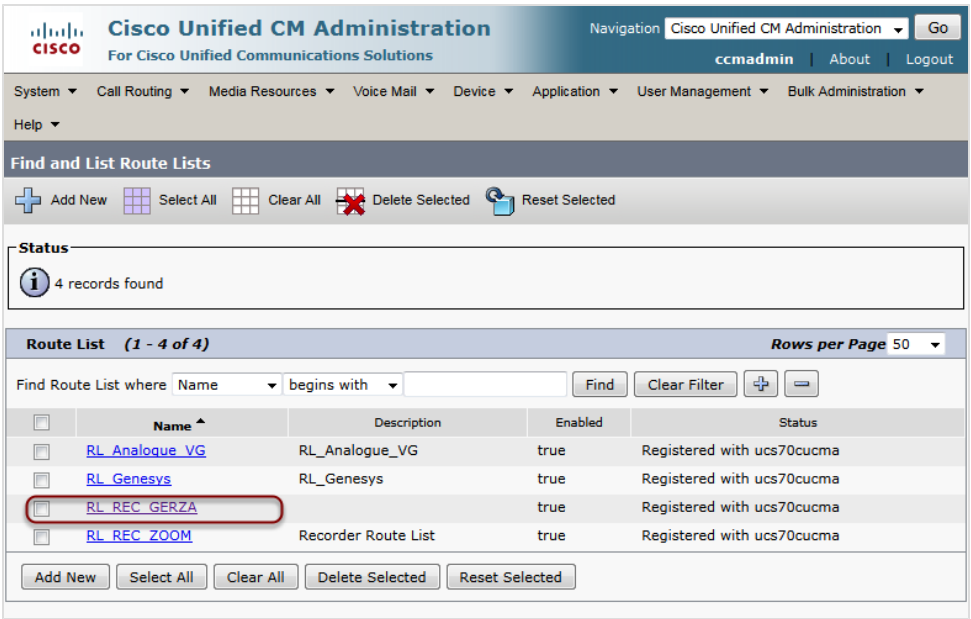


Figure 34: Route List

Select the route.

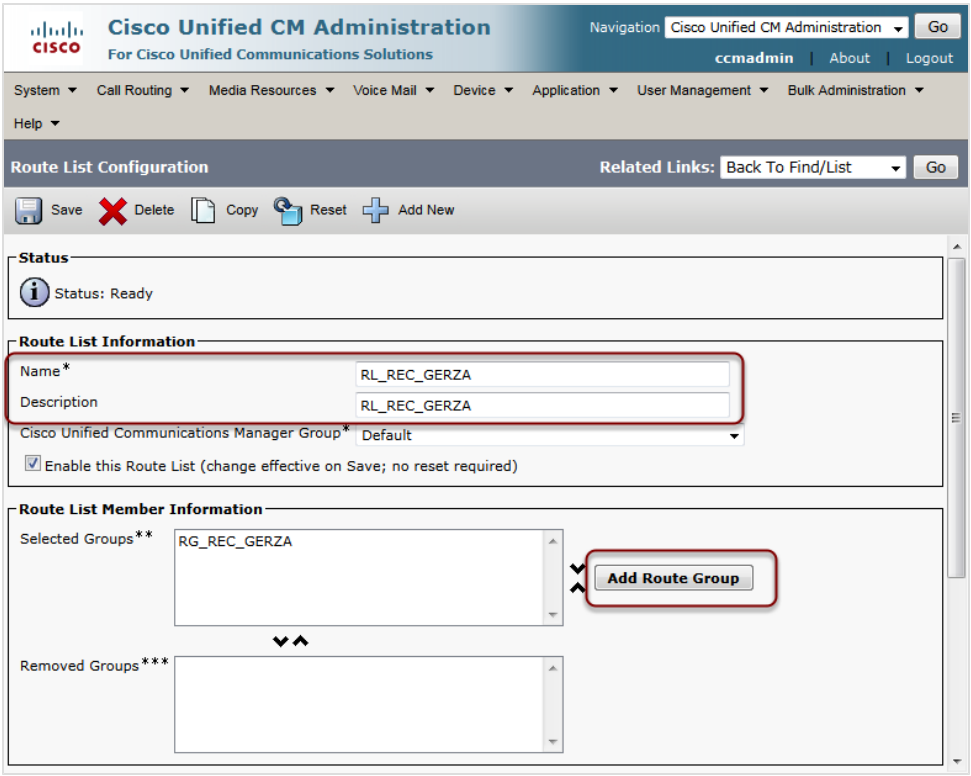


Figure 35: Route List Configuration

Click **Add Route Group**.

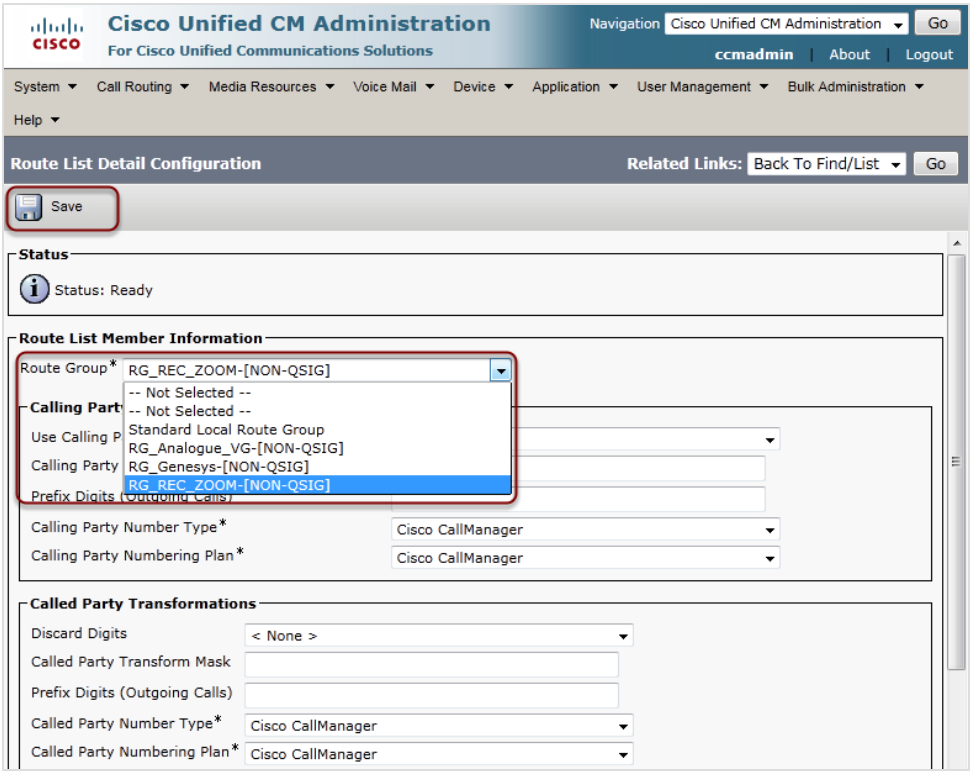


Figure 36: Route List Detail Configuration

1. Select the **Route Group**.
2. Click **Save**.

Creating a Route Pattern for the Recorder and Assigning the Route List

The Route Pattern points to the Route List where redundancy is deployed, or it can point directly to the SIP Trunk.

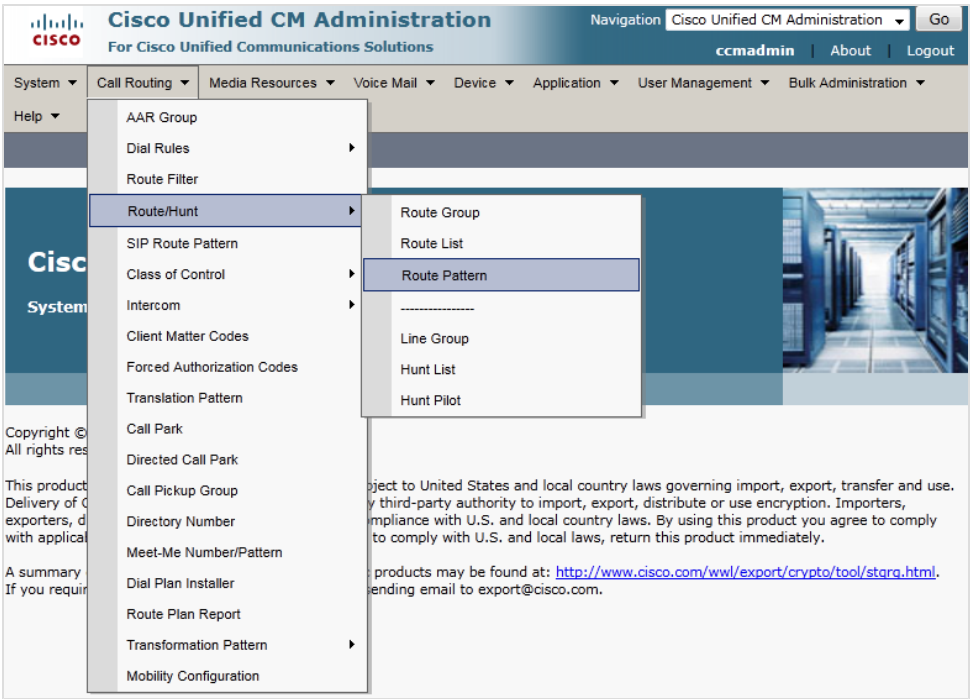


Figure 37: Select Route Pattern

Select **Call Routing > Route/Hunt > Route Pattern**.

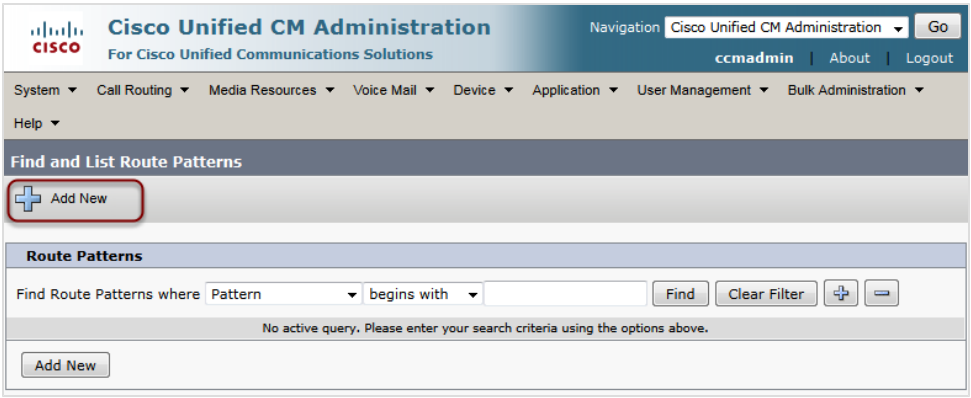


Figure 38: Find and List Route Pattern

Click **Add New**.

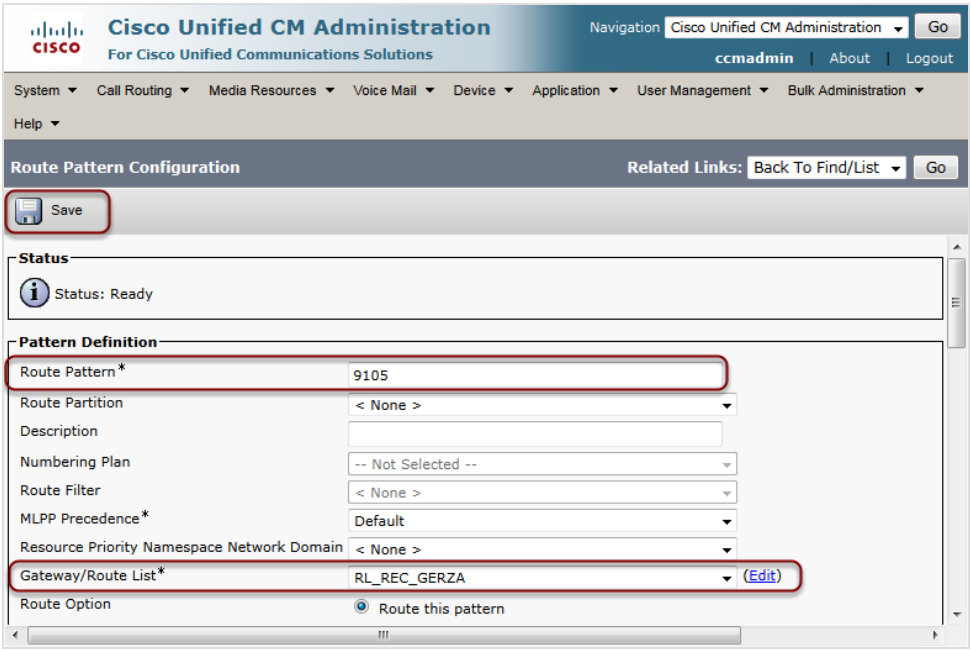


Figure 39: Route Pattern Configuration

1. Enter the **Route Pattern**.
2. Select the **Gateway/Route List**.
3. Click **Save**.

Enabling the Phone Built-In Bridge (BIB) to allow Recording

The Built-In Bridge can be activated on the Service Parameter level for all devices or can be activated phone by phone.

For an up-to-date list of all Cisco phones that support Active Recording see Unified CM Silent Monitoring Recording Supported Device Matrix.

Enabling Phone BIB for all devices

This method is useful for recording all phones.

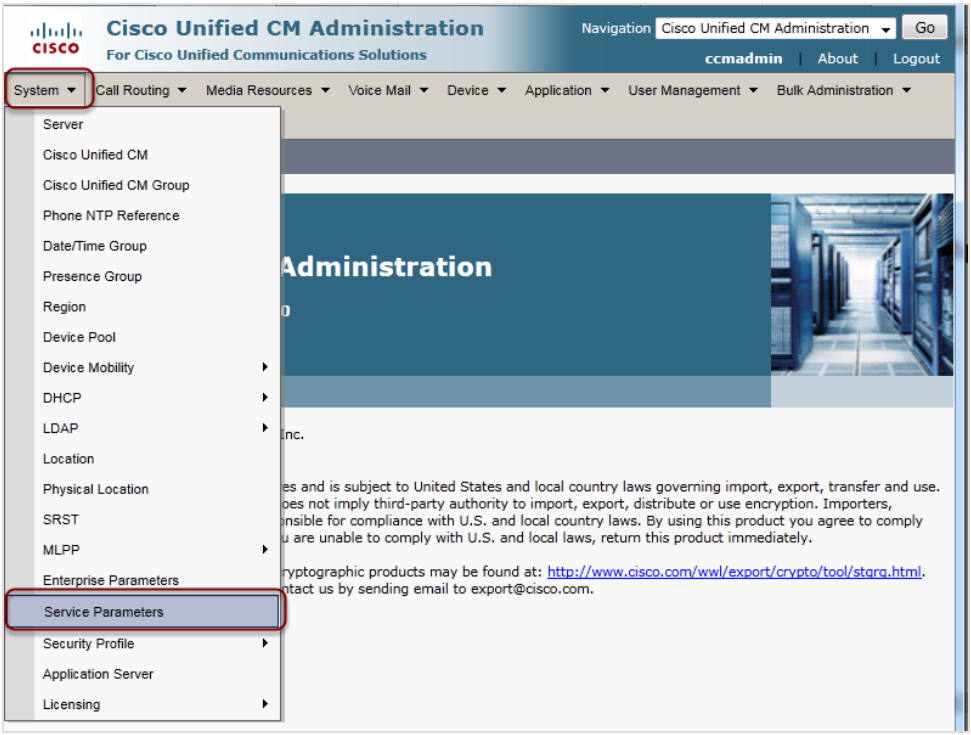


Figure 40: Select Service Parameters

Select **System > Service Parameters**.

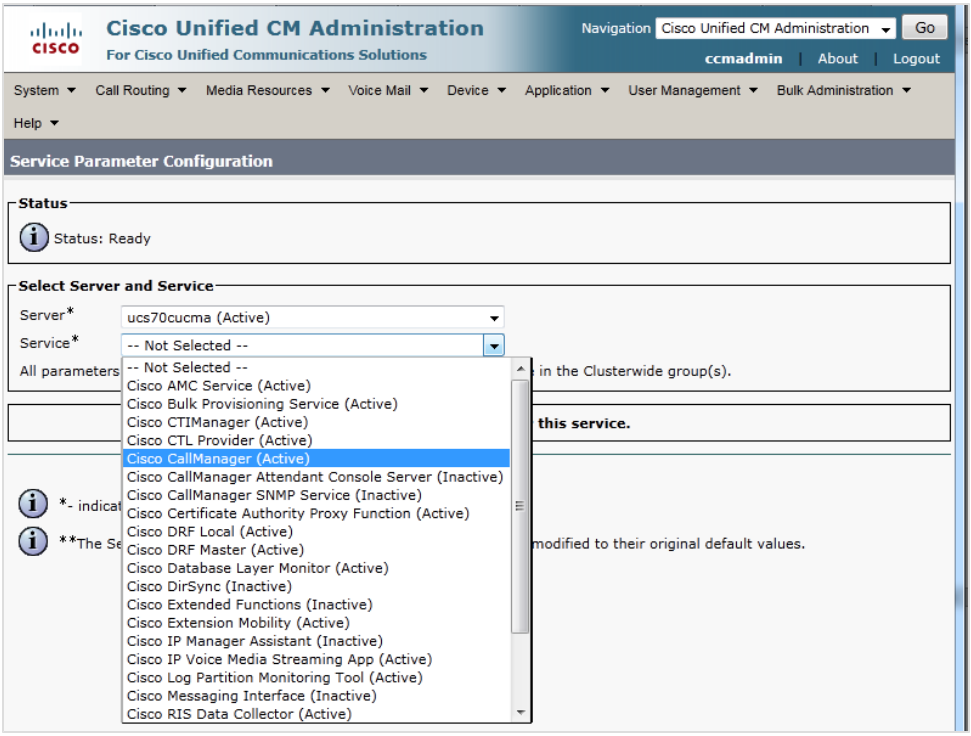


Figure 41: Select Server and Services

Select the service **Cisco CallManager (Active)**.

The Service Parameter Configuration screen opens. Scroll down to **Clusterwide Parameters (Device-Phone)**.

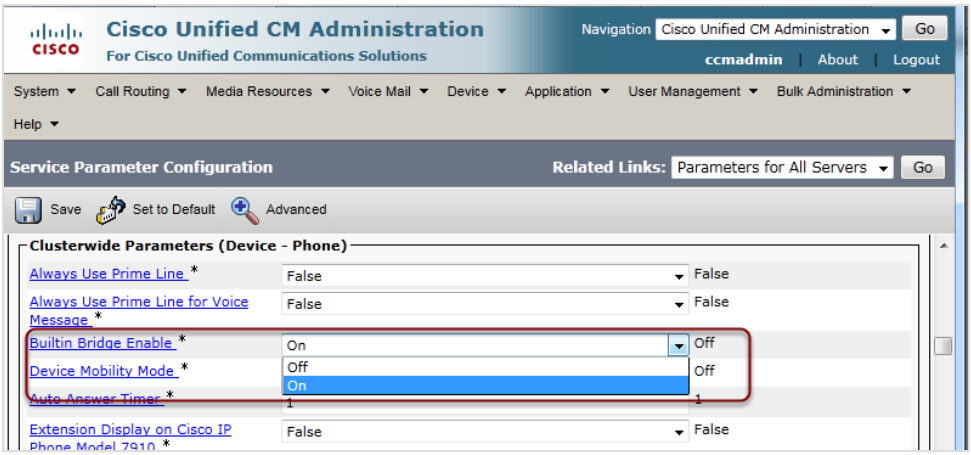


Figure 42: Clusterwide Parameters Phone

Ensure that **Builtin Bridge Enable** is **On**.

Enabling the Phone BIB Phone by Phone

This second method is useful for adding amending phones or devices to be recorded. Or for where only a selected few phones are to be recorded. Enable recording for each line. A phone or device can have several numbers, each number must be configured separately.

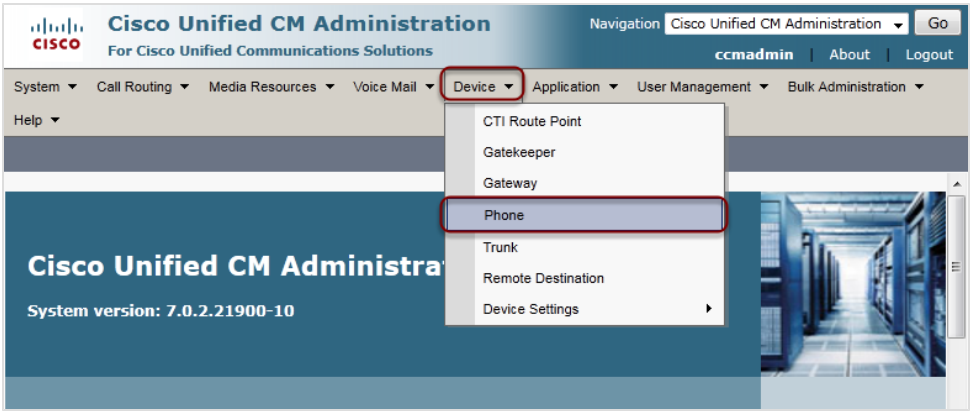


Figure 43: Select Phone

Select **Device > Phone**.

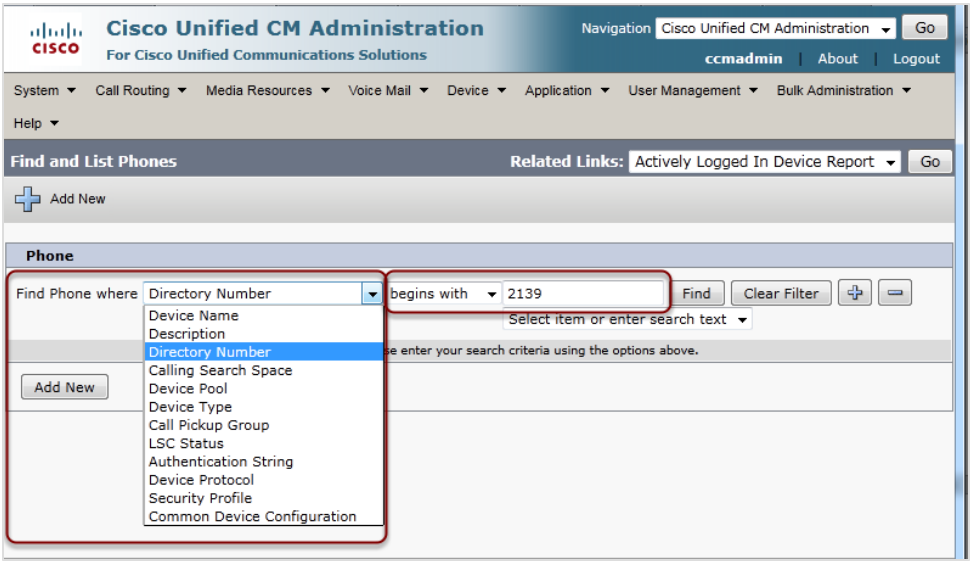


Figure 44: Find Phone by Selected Parameter

Select a parameter from the **Find Phone where** dropdown, for example, select **Directory Number** and type in the number or just the first digits to select an individual phone.

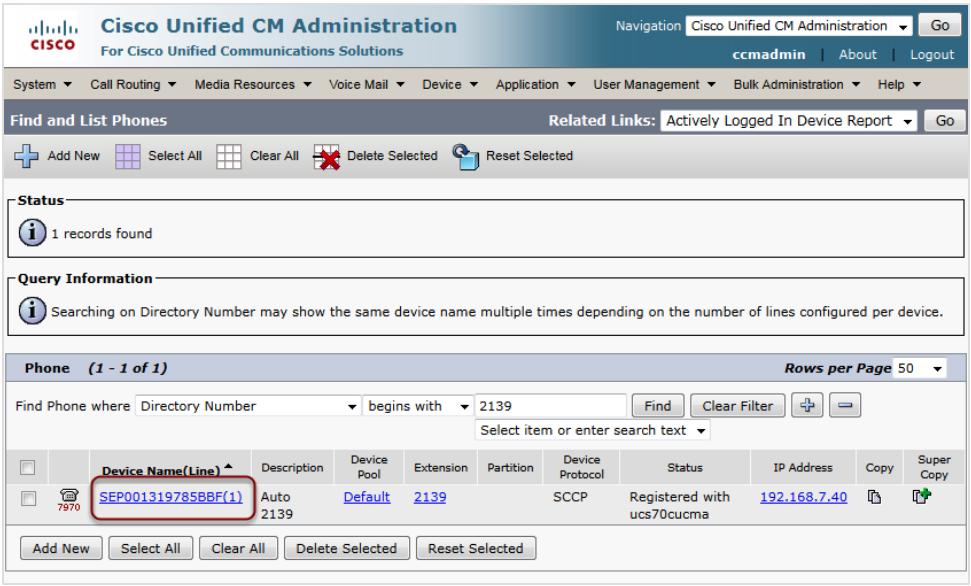


Figure 45: Find Phone by Number

Double click the **Device Name (Line)**. The **Phone Configuration** Dialog opens.

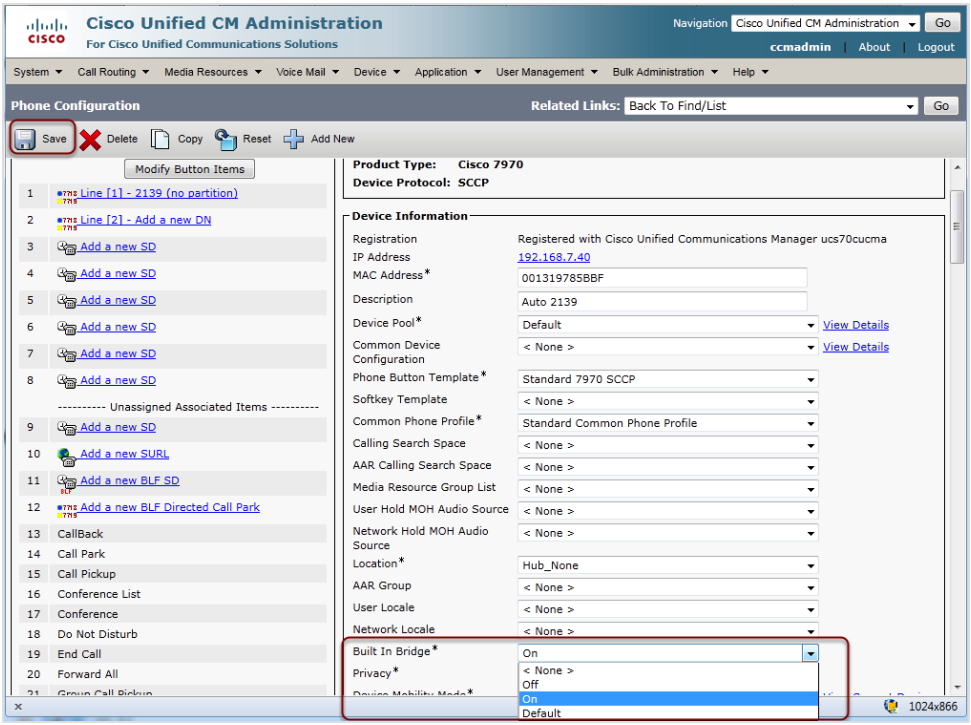


Figure 46: Enable BIB in Phone Configuration

1. Set the **Built In Bridge** to **On**.

2. Click **Save**.

Increasing the SIP Expires Timer

Select **System > Service Parameters** as in the previous step and scroll down to **Clusterwide Parameters (Devices - SIP)**.

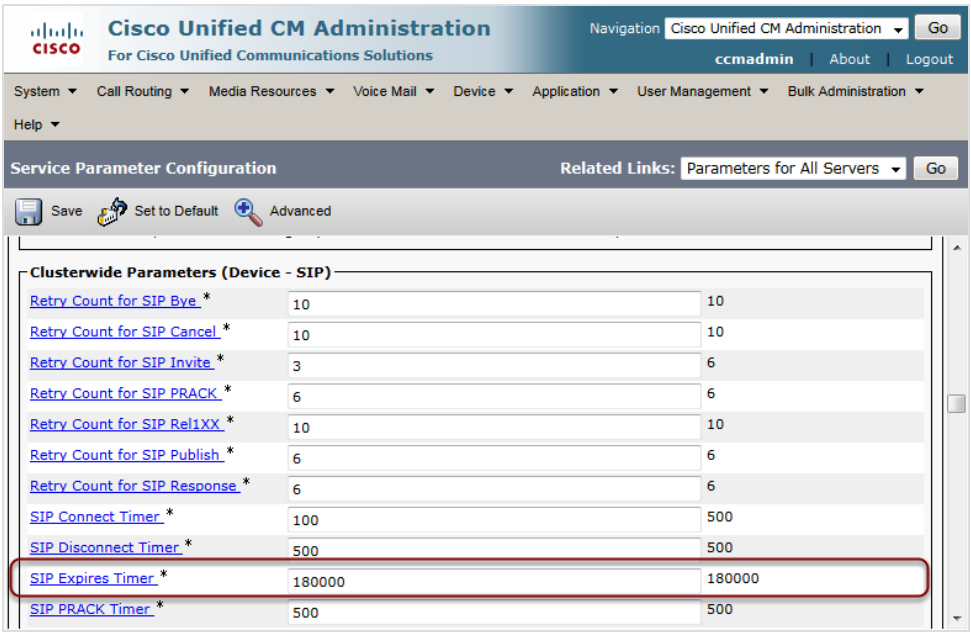


Figure 47: Increase SIP Expires Timer

Increase the **SIP Expires Timer** to 172800 (48 hrs) to prevent recordings of calls using SIP from being terminated before the call has ended.

Resetting the Trunk

To complete the changes, reset the trunk.

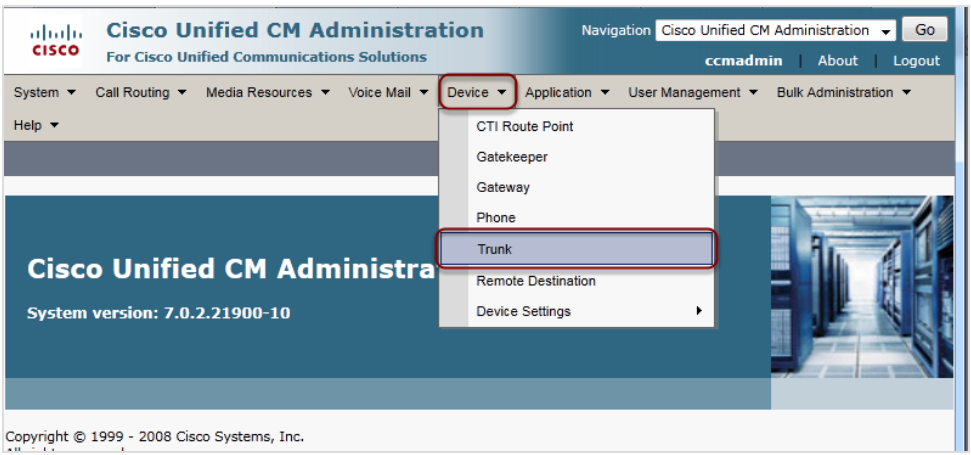


Figure 48: Select Trunk

Select **Device > Trunk**.

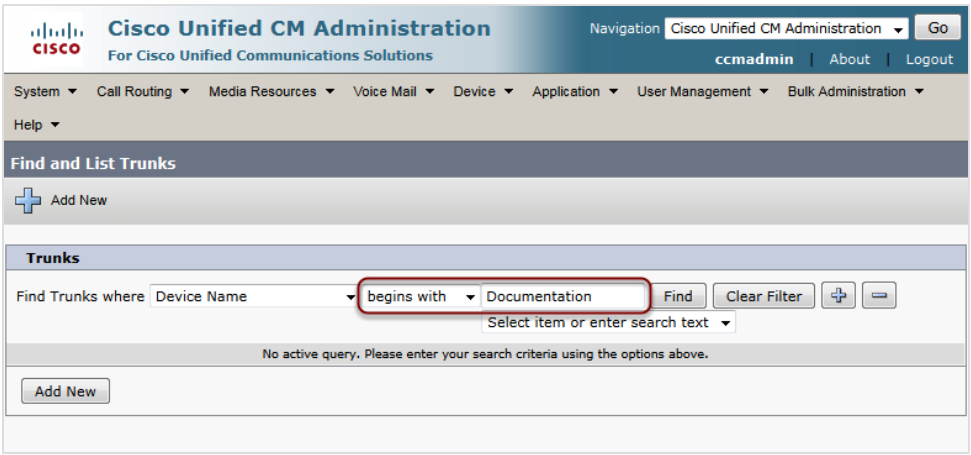


Figure 49: Find and List Trunks 2

Use **Find and List Trunk** to find the Trunks.

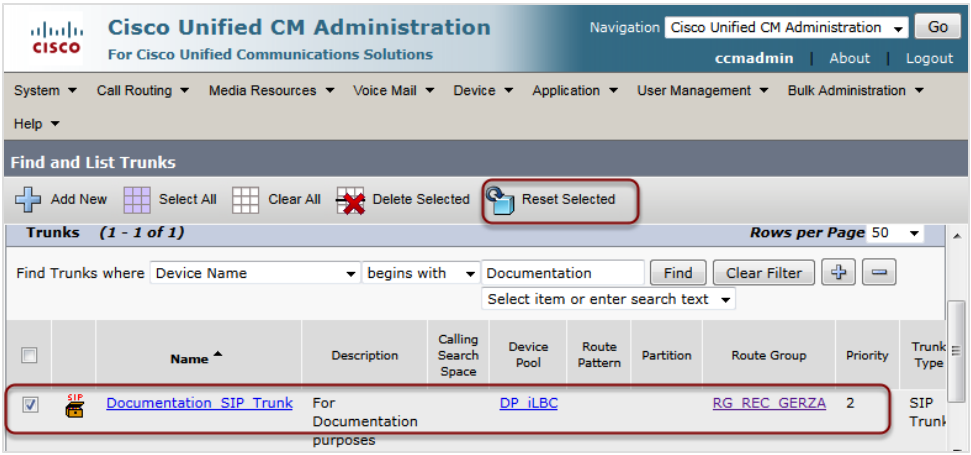


Figure 50: Reset Trunk

1. Select the Trunk.
2. Click **Reset Selected**.

Chapter

7 Setting up Genesys Configuration Server and T-servers for Call Recording

Genesys Configuration Server and T-servers must be configured to enable Call Recording to communicate with the system. Upload and enable the Genesys Integration Module application template and create a new user account for Call Recording in both the primary and backup servers.

Adding the Call Recording Application to the Configuration Manager

Open Genesys Configuration Manager. Navigate to **Start menu > All Programs > Genesys Solutions > Framework > Configuration Manager > Start Configuration Manager**.

1. Open **Configuration > Environment > Application Templates** in tree view.
2. Install the application template provided with the Call Recording integration module by clicking the context menu in **Application Templates** and selecting **Import Application Template**. Then locate the file `CallREC-GenesysIntegrationModule.adp` and open it. By default this is in `/opt/callrec/etc` on the Call Recording server.
3. Create a new application based on this template. From the Context or File menu, go to **Environment > Application** and select **New > Application**.
4. Select Call Recording Genesys Integration Module and click **OK** (twice).

Adding a New Person to the Configuration Manager

The Integration Module requires a configured Person for authorization when connecting to the T-Server and Configuration Server.The same account can be used for both T-Server and Configuration Server connections. If two separate accounts are required do so by repeating this step.

Go to **Resources > Person**.

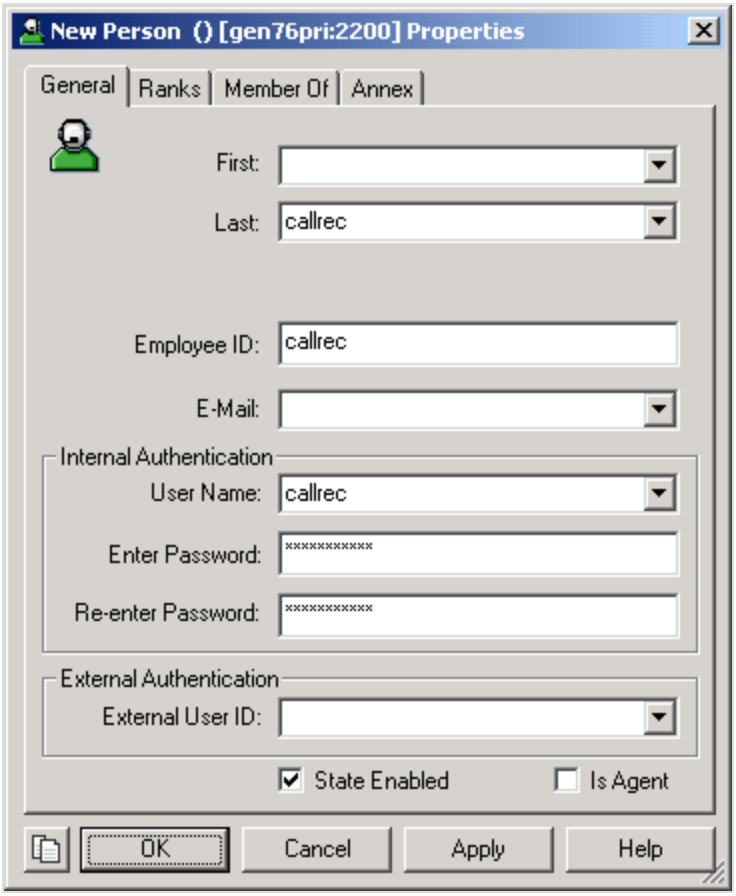


Figure 51: Adding a New Person in Genesys Configuration Manager

1. Add a **New Person**.
   Type at least, **Last** Name, **Employee ID**, **User Name**, and **Password**. Select the **State Enabled** checkbox and ensure that the **Is Agent** checkbox is not selected.
2. Add the **Access Group** membership in the **Member Of** tab.

Important:

The person that Call Recording uses for authentication must only have permission to “see” Agent DNs that will be recorded.

It may be useful to limit the number of observed DNs and thus decrease the number of processed events (only the DNs that are interesting will be observed), so the system load can be lowered. To achieve this goal, one possible approach is to make the person a member of the ‘Users’ group and block access to all sub trees in the SWITCH directory except for the SWITCH\DNs directory which is mandatory for successful events processing.

In certain installations it may be necessary to add the person to additional groups in order to see Agents DNs.

3. Click **OK** to save the new person.

Prerequisites for Network Infrastructure

Genesys 7.5, 7.6, 8.0, and 8.1 T-Server are supported.

The Genesys T-Server (SIP server) must have the configuration option rtp-info-password set.

For Genesys 7.6 T-Server, this option is located in the Configuration Manager: **Configuration > Environment > Applications >T-Server_Switch**, on the **Options** tab.

Important:

If the rtp-info-password option is not configured, or the passwords do not match, the Genesys Driver cannot receive any information about call RTP streams, which effectively disables the recording capabilities of QM.

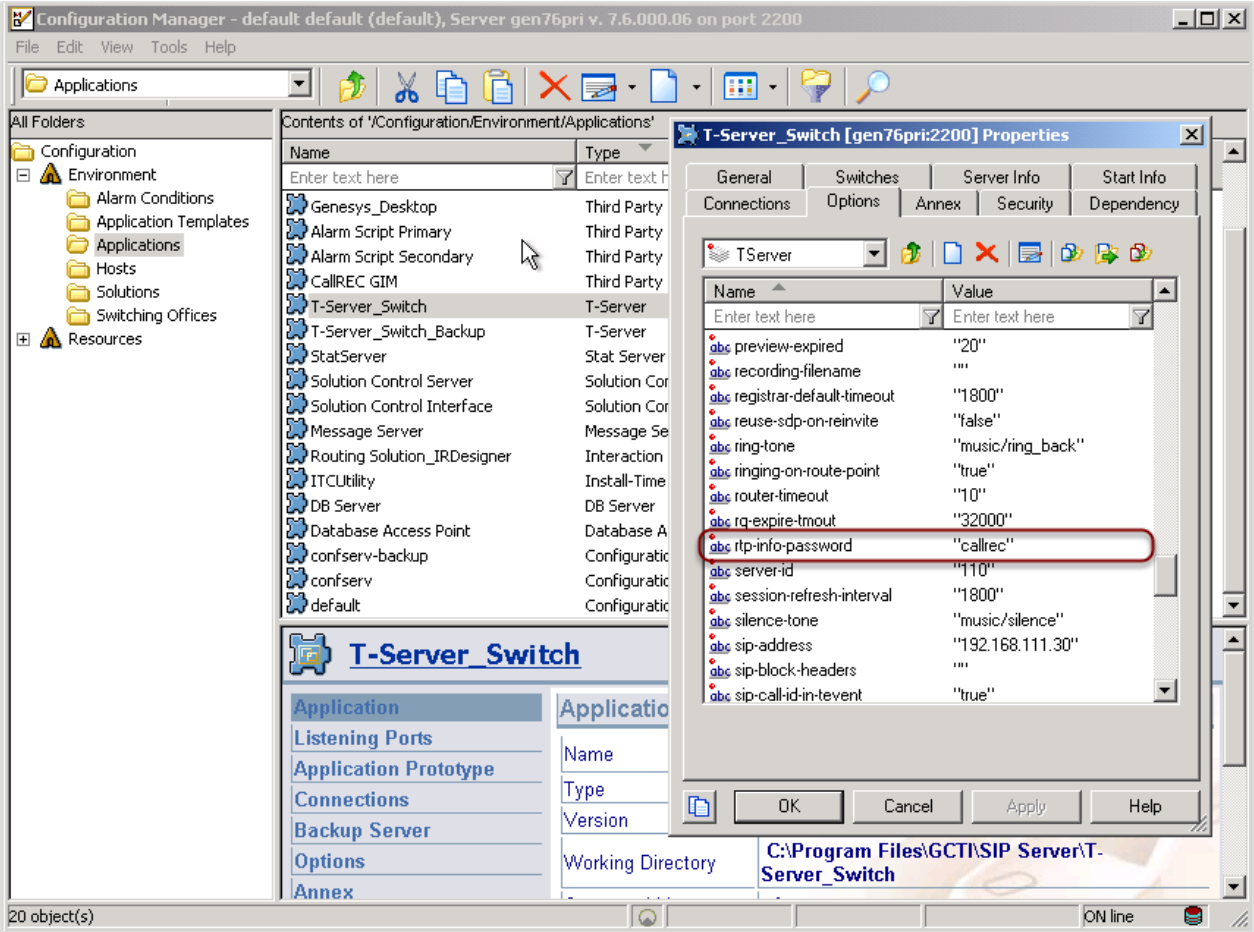


Figure 52: Configuring rtp-info-password in Genesys 7.6 T-Server

Chapter

8 Installing the OS and Installation Files

Only use this document if implementing GQM 8.1.51 or above. Previous versions of GQM require an earlier version of the operating system. Installation procedures differ significantly between versions.

The Operating System (OS) used for Genesys Quality Management 8.1.500 and above is RedHat Enterprise Linux 6.2, 32-bit version. After you have installed the OS according to your requirements, the RPMs and setup files required for GQM installation need to be copied to the server from the GQM ISO/DVD, and any RPM dependency issues resolved before GQM installation and setup can begin. For this reason, access is also required to the RHEL distribution file repository, ISO or DVD during the installation process.

See Installing GQM Packages for RHEL for a description of the typical package installation procedure on RHEL.

Do not use earlier versions of RedHat Enterprise Linux.

This chapter contains the following sections:

Next Steps

Pre-installation Check

Prior to installation of OS and Genesys GQM please check for the following conditions:

- There is at least 25GB of free space on the storage device.
- The system time and date are set to the UTC time zone and NTP (Network Time Server) synchronization is enabled. Only use a different configuration if required by the network administrator.

Integration of Call Recording with the Genesys CIM requires further configuration after installation is complete; please ensure that you have read Integrating Genesys CIM with Call Recording in the Appendix before proceeding with the installation.

Domain Naming Conventions

Ensure that any domain name conforms to the international RFC 1034 standard on domain names and the DNS system:

The labels must follow the rules for ARPANET host names. They must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphen. There are also some restrictions on the length. Labels must be 63 characters or less.

[RFC 1034 section 3.5: Preferred name syntax]

Installation Media

The installation media set consists of the following item:

- Genesys GQM ISO image file
- ISO checksum files for ISO integrity checks

Genesys GQM is delivered as a single ISO image file or DVD.

Important:
The ISO image file is too large for a CD therefore only DVDs can be used.

The ISO image file contains the complete installation of the Genesys GQM 8.1.5x recording system as well as optional plug-ins and components. The ISO can be mounted and then used in place of an installation disc.

Download the `.iso` file along with the `.md5` and `.sha1` checksum files. Once the files download completely check the ISO against either the `.md5` or `.sha1` hash files before using it for installation.

Verifying ISO file integrity

Verify the integrity of all downloaded ISO image files. Use the MD5 checksum provided together with the ISO download file. Download WinMD5Sum and install it according to the manufacturer's instructions from:

http://www.nullriver.com/products/WinMD5Sum

The MD5 verification procedure using WinMD5Sum for a GQM ISO file is as follows:

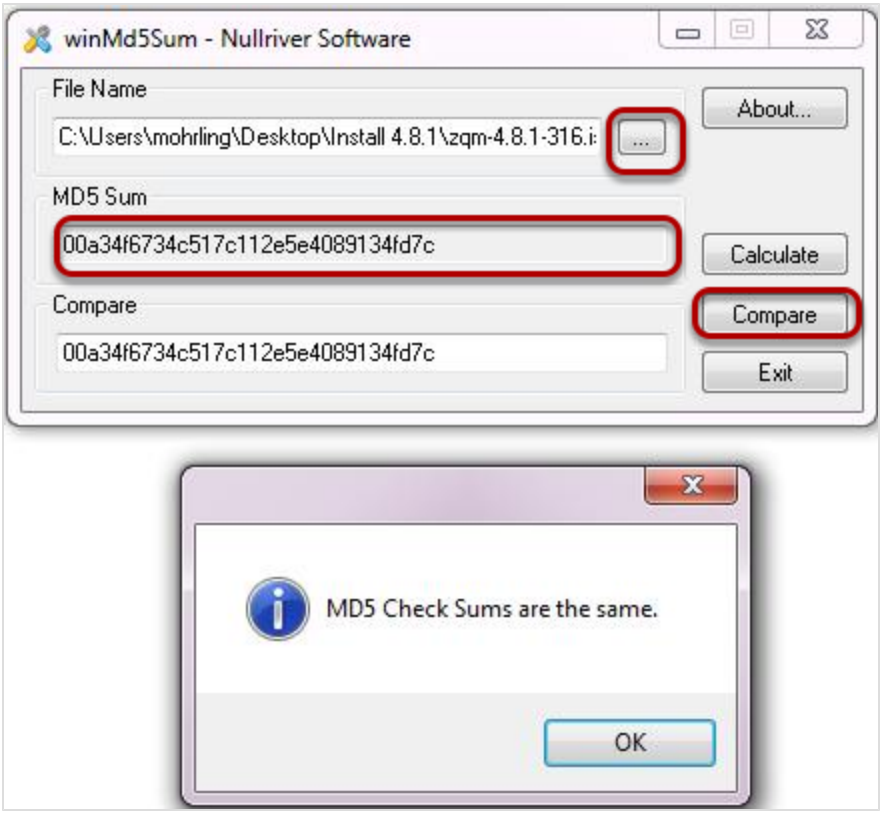


Figure 53: MD5 Checksums are the Same

1. Click **...** to browse for the downloaded ISO image file.
2. The **MD5 Sum** field checksum appears.

   Open the `gqm-x.x.x-xxx.iso.md5` file using a text editor, copy the number from the text file and paste into the **Compare** field. The checksum is 32 characters long.
3. Click **Compare**.

4. If the checksums are the same the confirmation dialog displays.

Automated OS Installation

When a custom installation of RHEL is required on multiple servers, such as in a lab or large-scale deployment scenario, automating OS installation using a kickstart file on a USB flash drive is recommended.

The kickstart file contains answers to all prompts that would appear during a typical installation. The GQM ISO or installation media includes a sample kickstart file for use in this way.

To prepare a USB flash drive for use in OS installation, perform the following steps:

Format the USB Flash Drive

Formatting the flash drive removes all existing data. Format the drive on both Linux and Windows systems:

Linux

- Connect or insert the USB flash drive.
- Find out what block device is associated with it:

```
#~ dmesg | tail
...
[44800.285937] sd 7:0:0:0: [sdb] Attached SCSI removable disk
#~ fdisk -l /dev/sdb
...
/dev/sdb1 2048 1050623 524288 b W95 FAT32
#~ mkfs.ext2 /dev/sdb1
#~ mount /dev/sdb1 /mnt/usb
```

Windows

- Connect or insert the USB flash drive.
- In Windows Explorer, right-click on the USB flash drive and select **Format...**.
- Select the FAT filesystem type.

Acquire the Kickstart Config File

The file is located on GQM media, with the name `ksminimal.cfg`, in the root folder.

Linux

- Insert or attach the GQM media.
- Enter the following commands:

```
#~ mount /dev/cdrom /media/cdrom
#~ cp /media/cdrom/ksminimal.cfg /mnt/usb
```

Windows

- Insert or attach the GQM media.
- Open the media using Windows Explorer.
- Copy the `ksminimal.cfg` file to the USB flash drive.

Disconnect the USB Flash Drive from the Computer.

Linux

- Enter the following command:

```
#~ umount /mnt/usb
```

Windows

- Using Windows Explorer, right-click on the USB flash drive icon in the status bar and select **Safely remove USB device**.

Use the USB Flash Drive during Boot

- Connect or insert the USB flash drive into the server.
- Boot the RHEL GQM installation media.
- On the boot screen, press the TAB key to modify boot options.
- Add the following command into the text box that appears:

```
ks=hd:sdb1:/ksminimal.cfg
```

[Note that the USB flash drive may be recognized as a different device such as sd??]

- The installation will now continue.
- After the final reboot, continue with the installation using GQM meta packages as described in the Implementation Guide.

Operating System Requirements

GQM installation requires a server on which the following operating system must be installed:

- RedHat Enterprise Linux version 6.2, 32-bit commercial license. Installation files (disc / ISO) and RHEL license need to be provided by the administrator.

Important:

Genesys GQM requires a specific release of the operating system. Using another version of the operating system is not recommended and may lead to installation failure since GQM expects exact matches for package names and configuration files.

Installing Red Hat Enterprise Linux

This document does not cover the installation of RedHat Enterprise Linux (RHEL) in detail, but please review the following notes on RHEL installation:

- GQM only supports the RHEL 6.2 32 bit version of the OS.
- The default server package install ('Basic') is adequate for single server GQM implementations. For multi-server scenarios, it will be necessary to optimize the server configuration based on the role of each server. OS package optimization is outside the scope of this document.
- After RHEL installation, ensure that standard OS functionality such as connectivity and networking works correctly before attempting to install and configure GQM.
- The next section will explain how to install GQM installation packages on your RHEL server.

Installing GQM Packages for RHEL

1. Mount the GQM installation media and copy over the required RPM setup files.

```
mkdir -p /media/cdrom/
mount /dev/cdrom /media/cdrom/
cp /media/cdrom/GQM_Suite/RPMS/qm-meta-os*.rpm /tmp/
cp /media/cdrom/rhel.repo /etc/yum.repos.d/
umount /media/cdrom/
```

2. Mount the RHEL 6.2 installation media and install the local RPM repository and dependencies.

```
mount /dev/cdrom /media/cdrom/
yum localinstall --nogpgcheck -y /tmp/qm-meta-os*.rpm
```

If there are any dependency problems when running the `yum localinstall` command, there will be messages stating which packages are involved; these will need to be removed. Note that the Open JDK package (for example, `java-1.6.0-openjdk`) often causes dependency issues and can safely be removed.

Remove the affected packages using the `yum remove` command first, for example, `yum remove java-1.6.0-openjdk`, then enter again the `yum localinstall` command again as before. Repeat this procedure until the command is successful.

3. You must now ensure that the following packages are uninstalled: `gcj`, and `java-1.4.2-compat`, then unmount the RHEL installation media.

```
yum remove gcj java-1.4.2-gcj-compat --disablerepo=qm
umount /media/cdrom/
```

4. Mount the GQM media again and install GQM from the RPM package.

```
mount /dev/cdrom /media/cdrom/
cd /media/cdrom
yum clean all
yum makecache --disablerepo=rhel
yum install -y qm-meta --disablerepo=rhel --nogpgcheck
cd -
umount /media/cdrom/
```

Important:

Be aware that the `/etc/yum.repos.d/rhel.repo` RHEL repository file is being modified during the installation process.

Next Steps

After successfully installing the Operating System, the server is ready for installation and configuration of GQM.

GQM installation must be performed by a certified ZOOM Certified Implementation Engineer. The complete procedure is covered in the *Implementation Guide* document.

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 1: 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 2: Genesys Default Ports for MSR/EPR/GIM

RMI communications between modules uses random ports from range: 1024 – 65535 (TCP).

Important:

Do not change **Port** settings directly in configurations files without consulting Genesys Support. Change these settings through the Admin User Interface. Ensure that there is a backup of all configuration files before changing port numbers.

Chapter

10 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.

Integrating Genesys CIM with GQM

Genesys Customer Interaction Management (CIM) platform supports several underlying PBXs. Call Recording supports the following PBXs for call recording and contact center integration:

- Genesys contact center with Genesys SIP Server
- Genesys contact center with Cisco Unified Communications Manager

Three Call Recording services are available for Genesys integration: GIM, EPR and MSR. All three provide the same data.

This chapter contains the following sections:

MSR Integration

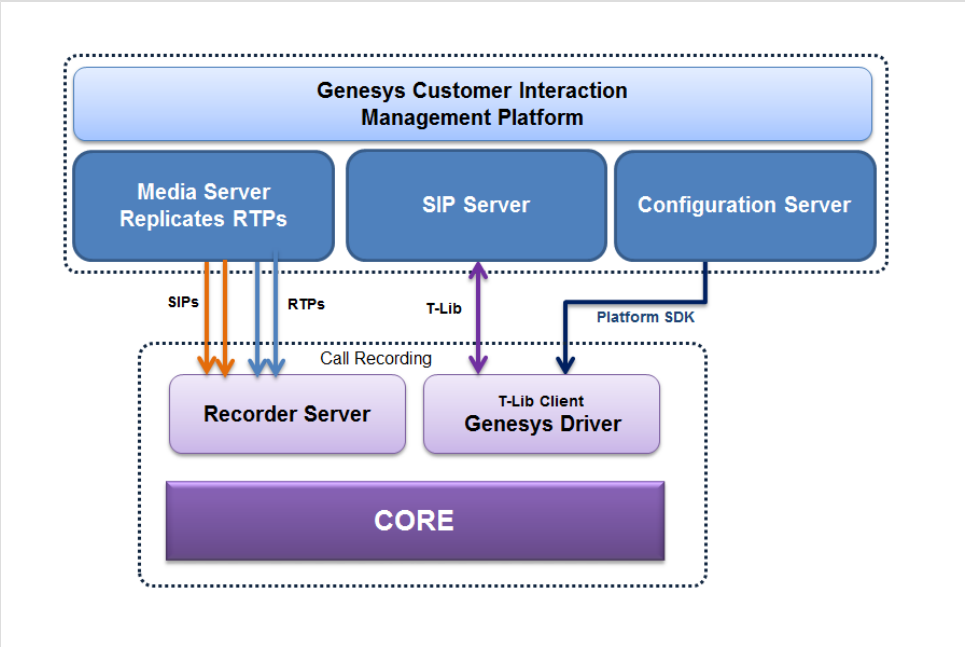


Figure 54: MSR Integration with Call Recording

The Genesys driver has a T-Lib Client that handles all communication via T-Lib. The Genesys driver also handles communication with the Configuration Server.

Call Recording caches information from the Configuration Manager including the list of agents, devices, and other such information. This can be configured to be done in regular intervals.

Genesys Enhanced Passive Recording (EPR)

EPR is a combination of active signaling capture and passive voice capture, often referred to as 'hybrid' recording. EPR uses the Voice Monitoring API, which is a part of the Genesys SDK Platform.

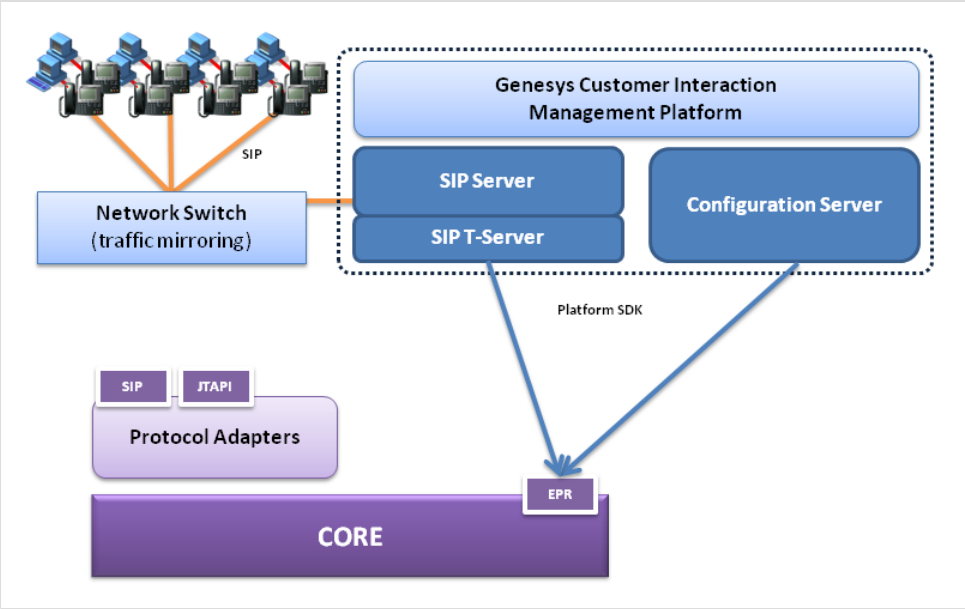


Figure 55: Genesys EPR Connectivity

The EPR provides a much more stable and reliable method of call recording on the Genesys platform than the older GIM. Since all the phone- and agent-based events are being received over the API, there is no risk that some important information will be lost because of a lost packet on the network. Although the voice streams are still delivered from the monitoring (SPAN) port on a network switch. This is not a significant issue and the signaling events are reliably handled by the "active driver."

EPR also integrates two different recording components; the protocol driver and the integration module. This means that with the EPR, there is just one component responsible for all of the information that comes from the Genesys platform. This makes the recording process easier. The attached metadata are more consistent and their delivery and completeness isassured. It also makes manageability and troubleshooting easier, because all of the events are delivered together by one component.

Genesys Integration Module

The Genesys Integration Module (GIM) is required when SIP or JTAPI based call recording is deployed. The GIM connects Call Recording and Genesys T-Server using the Voice Platform SDK and Configuration Platform SDK.

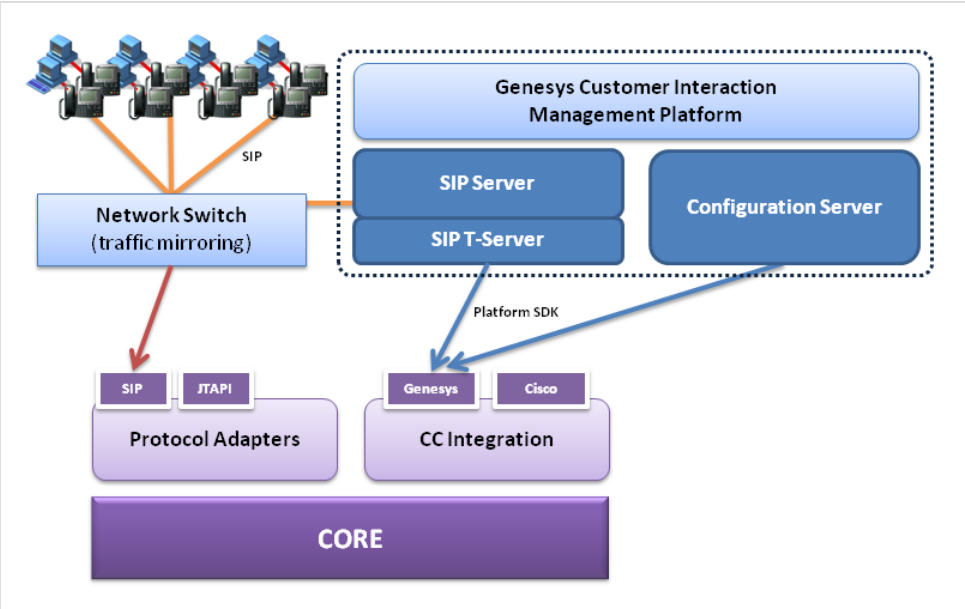


Figure 56: Genesys GIM Connectivity

Connection with Call Recording is implemented using the Call Recording API. Via its API, Call Recording notifies the integration library of every newly established call it detects or records. After the integration library learns of the available call information, it queries T-Server whether the call is controlled by Genesys contact center. If it is, it acquires the available properties of the call and hands selected data over to Call Recording, which saves it as external data.

If recording is based on the Cisco Unified Communications Manager softswitch Call Recording must be set to record through JTAPI adapter, since the lookup of information in both systems leverages call identification (GlobalCallID), which is available in Call Recording only through Cisco JTAPI.

For Genesys SIP Server deployments no specific settings are required.

Genesys CIM to Call Recording information exchange

The data saved in the Call Recording external data table comes from various sources. There are four basic classes of information available:

- Basic call-related data
- Call-related user data (attached data)
- Agent configuration data
- Notification of recording

The presence of specific data depends on the system configuration, routing design, network topology and on other conditions. Configuration of particular properties which have to be stored in the Call Recording external data table has to be done during integration library implementation.

Basic Call-related data

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

The data is stored using the following naming convention:

External data key:`GEN_TEV_<TEvent.key>`
Example:`GEN_TEV_AgentID = "AG_3017"`

The following values are available:

Key	Description
AgentID	The agent identifier specified by PBX or ACD.
ANI	Automatic Number Identification. Specifies from which number the current inbound call originates.
CallID	The call identifier provided by the switch (as opposed to connection identifier, or ConnID, which is assigned by T-Server).
CallUuid	The UUID of the call; a unique call identifier provided by the Genesys platform.
CallType	Type of the call; one of the following values: Inbound, Outbound, Internal, Consult, Unknown.
CollectedDigits	The digits that have been collected from the caller.
ConnID	Connection identifier of the current call handled by the DN.
CustomerID	The string containing the customer identifier through which processing of the call was initiated.
DNIS	The Directory Number Information Service. Specifies to which DN the current inbound call was made.
NetworkCallID	In the case of network routing, the call identifier assigned by the switch where the call initially arrived.
NetworkNodeID	In the case of network routing, the identifier of the switch where the call initially arrived.
NodeID	The unique identifier of a switch within a network.

Key	Description
OtherDN	The other main Directory Number (which your application did not register) involved in this request or event. For instance, the DN of the main party of the call.
ThisDN	The Directory Number (which your application registered) involved in this request or event.
ThisQueue	The queue related to ThisDN.

Table 3: Basic Call-Related Data

Important:

Please note that if the value is empty the respective key is NOT stored in the Call Recording database!

Call-related User Data

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

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

Any value extracted from User Data will be attached using the following naming convention:

Externaldata key: `GEN_USR_<UserData.key>`
Example: `GEN_USR_RStrategyName = "default"`

Important:
The list of the User Data to attach must be defined in the configuration (see in the chapter below). By default no User data get attached.

(Since User Data depends on the specific configuration there is no list available)

Agent Configuration Data

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

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

Externaldata key: `GEN_CFG_<CfgData.key>`
Example: `GEN_CFG_UserName = "jsmith"`

The following information is available from the Configuration Platform SDK:

Key	Description
EmployeeID	The code identifying the person within the tenant staff.
FirstName	The person's first name.
LastName	The person's last name.
UserName	The name the person uses to log into a CTI system.
AdminType	Specifies whether the person is configured as 'Admin'. Yes=1, No=0
AgentType	Specifies whether the person is configured as 'Agent'. Yes=1, No=0
PlaceDbid	A unique identifier of the Place assigned to this agent by default.
State	The current state of the person object.

Table 4: Agent Configuration Data

Important:
Please note that if the value is empty, the respective key is NOT stored in the Call Recording database!

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

Key	Description
AgentLoginInfo_<index>_ LoginDbid	agentLoginDBID — A unique identifier of the Agent Login identifier.
AgentLoginInfo_<index>_ WrapupTime	wrapupTime — Wrap-up time in seconds associated with this login identifier. Cannot be a negative value.
AgentSkillLevels_<index>_ SkillDbid	skillDBID — A unique identifier of the skill the level relates to.
AgentSkillLevels_<index>_ Level	level — Level of the skill. Cannot be a negative value.

Table 5: Agent and Skill Info

Important:

Please note that if the value is empty the respective key is NOT stored in the Call Recording database!

Notification of Recording

The Notification of Recording option allows the system to provide information regarding whether a particular call is being successfully recorded. It is necessary for banks or financial institutions that undertake financial transactions and need to make sure that a specific call is being recorded. Notification is provided by adding a preconfigured key in the attached data.

The principle of notification is that Call Recording ensures that the call has been detected and all actions leading to successful recording have been performed, after which it provides status information. This takes some time, usually fractions of a second, but it is not possible to generally guarantee that the state information will be available in one second. The timeout for waiting for the state is configurable; the default is 3 seconds.

When the state is known or the timeout expires, Call Recording provides state information within pre-configured attached data. Both key and value strings are configurable, for example:

```
RecordingStatus_GIM1 = Recording
RecordingStatus_GIM2 = Unknown
```

The example demonstrates that it is possible to configure different key names for different servers recording the same Genesysplatform, useful in the case of redundant deployment.

Important:

Please note that in some situations notification may not be 100% correct. For example in the case when the recorder is not getting any voice data during the call, it cannot be recognized and reported. Such situations must be solved by additional monitoring system that monitors SPAN ports and recording results.