DevConnect Program

Application Notes for Calabrio Quality Management 11.0 with Avaya Aura® Communication Manager 10.2, Avaya Aura® Application Enablement Services 10.2, and Avaya Session Border Controller 10.2 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Calabrio Quality Management 11.0 with Avaya Aura® Communication Manager 10.2, Avaya Aura® Application Enablement Services 10.2, and Avaya Session Border Controller 10.2. Calabrio Quality Management is a call center solution that uses call recordings to monitor agent performance.

Calabrio Quality Management connects to Avaya Session Border Controller via a SIP trunk using SIP-based media recording (SIPREC) to capture call audio for stereo call recordings. Calabrio Quality Management starts with a recording of the root call, which is a recording of the entire call, including transfers and consultations that can involve multiple people, and then performs a reconciliation process to segment the root call into call legs and associate them with agent stations. Reconciliation requires Call Detail Records (CDR) from Avaya Aura® Communication Manager and agent extensions retrieved from Avaya Aura® Application Enablement Services using System Management Service (SMS) Web Services.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the Avaya DevConnect Program.

Table of Contents

1. Introduction

These Application Notes describe the configuration steps required to integrate Calabrio Quality Management 11.0 with Avaya Aura® Communication Manager 10.2, Avaya Aura® Application Enablement Services 10.2, and Avaya Session Border Controller 10.2. Calabrio Quality Management is a call center solution that uses call recordings to monitor agent performance.

Calabrio Quality Management connects to Avaya Session Border Controller via a SIP trunk using SIP-based media recording (SIPREC) to capture call audio for stereo call recordings. Calabrio Quality Management starts with a recording of the root call, which is a recording of the entire call, including transfers and consultations that can involve multiple people, and then performs a reconciliation process to segment the root call into call legs and associate them with agent stations. Reconciliation requires Call Detail Records (CDR) from Avaya Aura® Communication Manager and agent extensions retrieved from Avaya Aura® Application Enablement Services using System Management Service (SMS) Web Services. A CDR link using Reliable Session Protocol (RSP) is established between Avaya Aura® Communication Manager and Calabrio Quality Management.

In the compliance test, Calabrio Quality Management solution is comprised of the Calabrio Cloud and a Calabrio Data Server deployed in the enterprise network. Calabrio Cloud hosts the Calabrio Quality Management application and storage for the call recordings. Calabrio Data Server connects to Avaya Session Border Controller via a SIP trunk using SIPREC, collects CDR from Avaya Aura® Communication Manager, and retrieves agent extensions from Avaya Aura® Application Enablement Service using SMS.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. Feature testing focused on retrieving station extensions from Application Enablement Services via SMS, collecting CDR from Communication Manager, and recording PSTN calls routed through Avaya SBC to agent stations in stereo.

Serviceability testing focused on verifying that Calabrio QM Data Server returned to service after busying out and releasing the CDR link to Communication Manager and restarting Avaya SBC, Communication Manager, and Calabrio QM Data Server.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member’s solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interfaces between Avaya systems and Calabrio QM Data Server used TLS/SRTP for the SIP trunk to Avaya SBC and HTTPS for SMS to Avaya Application Enablement Services.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Establish SIP trunk between Calabrio QM Data Server and Avaya SBC for SIPREC using TLS transport and verifying the exchange of SIP OPTIONS messages.

- Use of SIPREC to capture media from Avaya SBC for call recordings.

- Use of G.711 and G.729 codec support and SRTP with 128-bit encryption for secure media.

- CDR collection from Communication Manager using Avaya Reliable Session Protocol.

- Retrieve station extensions from Application Enablement Services using SMS and display station extensions under Device Associations in the Calabrio Cloud Portal.

- Calabrio QM reconciliation process to segment root calls into call legs associated with agent extensions.

- Proper recording, logging, and playback of calls for scenarios involving inbound and outbound trunk calls, internal calls, hold/resume, G.711 and G.729 codecs, forwarding, service observing, long duration, multiple calls, multiple agents, transfer, and conference.

The serviceability testing focused on verifying the ability of Calabrio QM Data Server to recover from adverse conditions, such as restarting CDR link, Communication Manager, Application Enablement Services, Avaya SBC, and Calabrio QM Data Server.

2.2. Test Results

All test cases passed with the following observation:

- Station extensions are statically mapped to agent users on Calabrio QM; hence, hot desking or free seating is not supported. Agent login-IDs on Communication Manager are not tracked by this solution.

2.3. Support

Technical support for Calabrio Quality Management can be obtained through the following:

- **Phone:** +1 (855) 784-2807
- **Web:** https://www.calabrio.com/support/

3. Reference Configuration

Figure 1 illustrates the test configuration. In the compliance test, Calabrio Quality Management is comprised of the Calabrio Cloud, which hosts the Calabrio QM application and call recording storage, and the Calabrio QM Data Server deployed in the enterprise network. The Calabrio QM Data Server interacts with the following Avaya servers:

- Avaya SBC via a SIP trunk using TLS/SRTP for SIPREC to capture RTP traffic for stereo call recordings
- Communication Manager for CDR using Reliable Session Protocol to collect call records
- Application Enablement Services using SMS to retrieve station extensions

Calabrio Quality Management uses CDR and agent extensions for the reconciliation process, where a root recording is segmented into separate call legs using CDR and associated with a station extension/agent.

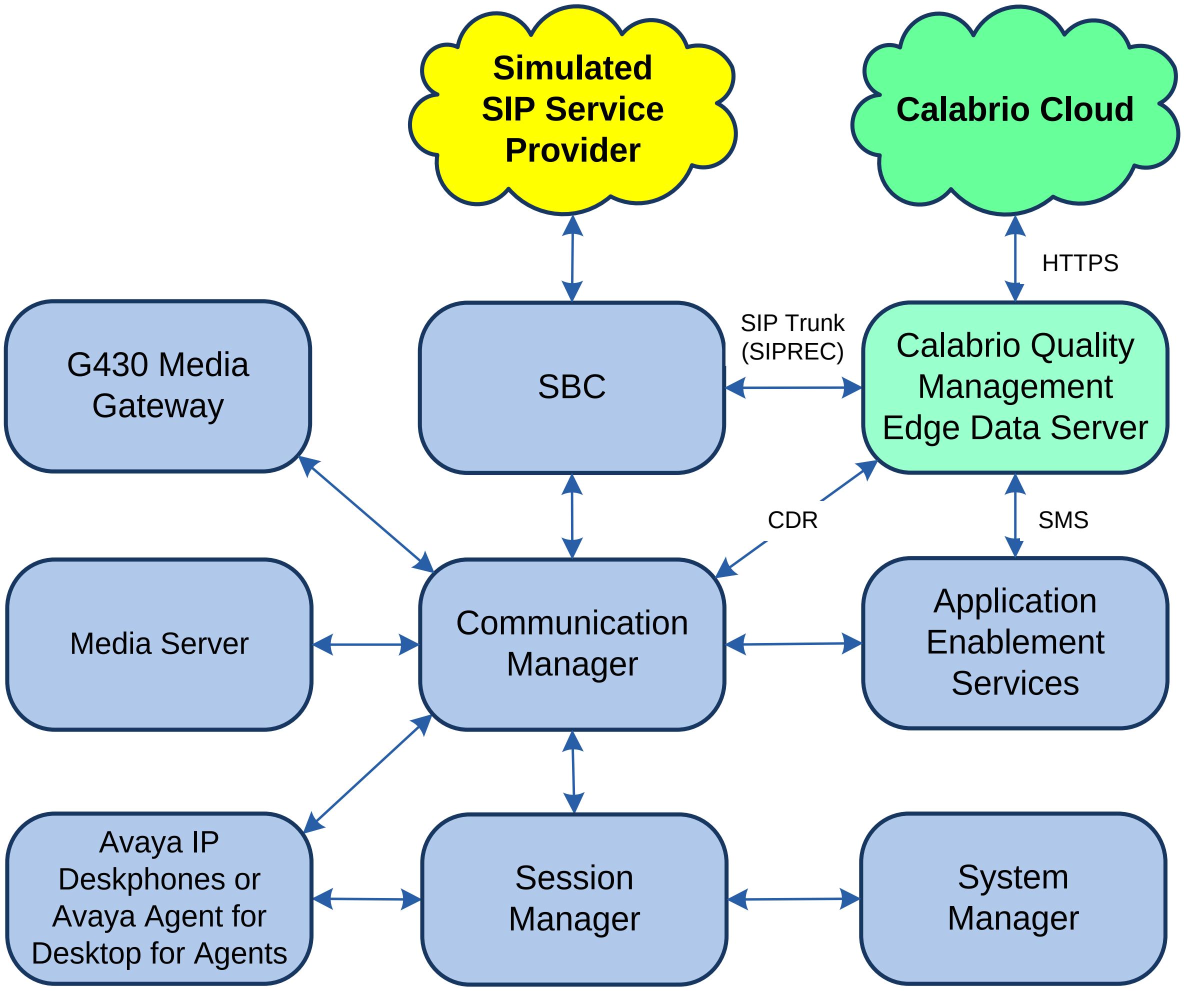

Simulated SIP Service Provider
Calabrio Cloud
HTTPS
G430 Media Gateway
SBC
SIP Trunk (SIPREC)
Calabrio Quality Management Edge Data Server
CDR
SMS
Media Server
Communication Manager
Application Enablement Services
Avaya IP Deskphones or Avaya Agent for Desktop for Agents
Session Manager
System Manager

Figure 1: Avaya Call Center with Calabrio Quality Management

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	10.2.0.1.1-SP1P1
Avaya G430 Media Gateway	FW 42.22.0
Avaya Aura® Media Server	10.1.0.176
Avaya Aura® Application Enablement Services	10.2.0.0.0-198-0
Avaya Aura® System Manager	10.2.0.1 Build No. – 10.2.0.0.439670 Software Update Revision No: 10.2.0.1.0516918
Avaya Aura® Session Manager	10.2.0.1.1020108
Avaya Session Border Controller	10.2.0.0-86-24077
Avaya Agent for Desktop	2.0.6.26.3003 (SIP)
Avaya 96x1 Series IP Deskphones	6.8.5.5.1 (H.323)
Avaya J100 Series IP Phones	4.1.4.0.5 (SIP)
Calabrio Quality Management	11.0.2.1210

5. Configure Avaya Aura® Communication Manager

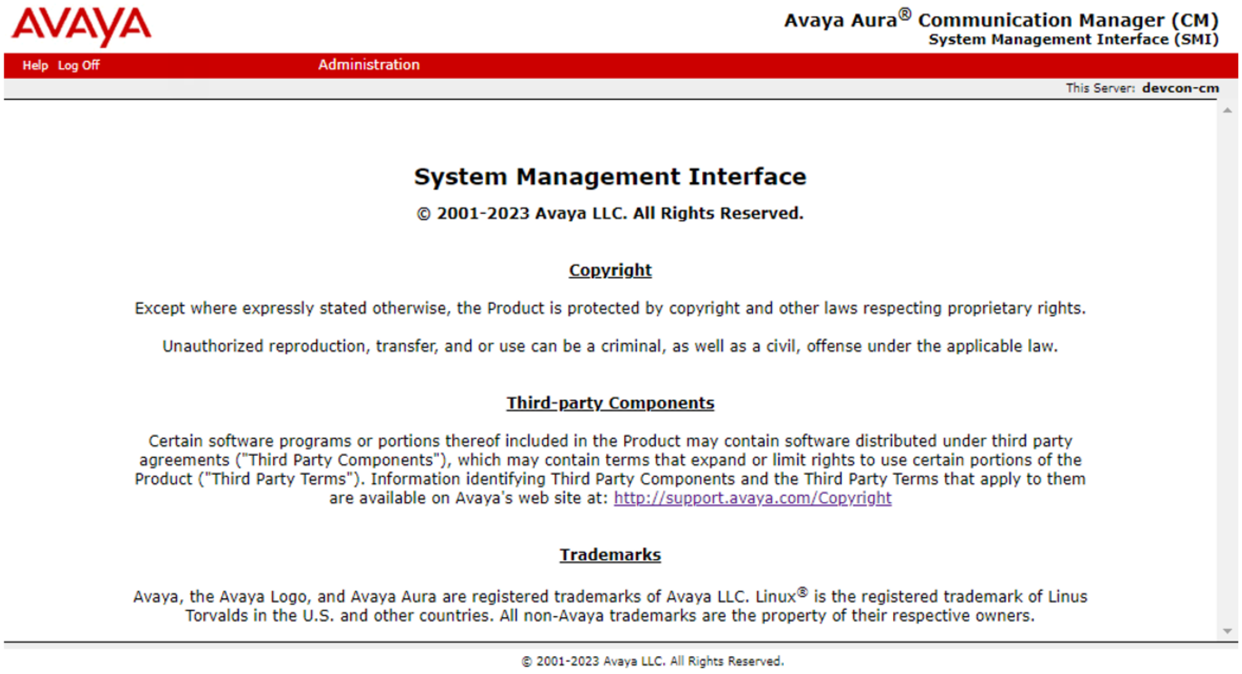
This section covers the configuration of Communication Manager is configured via the System Access Terminal (SAT), including the following areas:

- Launch System Management Interface
- Configure SAT Login
- Configure CDR
- Configure UCID Support

5.1. Launch System Management Interface

Access the Communication Manager System Manager Interface by using the URL **Error! Hyperlink reference not valid.** in a web browser, where *<ip-address>* is the Communication Manager IP address. Log in using the appropriate credentials.

In the subsequent webpage, select **Administration → Server (Maintenance)** from the top menu as shown below. The **Server Administration** webpage is displayed as shown in the following section.


AVAYA
Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)
Help
Log Off
Administration
This Server: devcon-cm

System Management Interface

© 2001-2023 Avaya LLC. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at: http://support.avaya.com/Copyright

Trademarks

Avaya, the Avaya Logo, and Avaya Aura are registered trademarks of Avaya LLC. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries. All non-Avaya trademarks are the property of their respective owners.

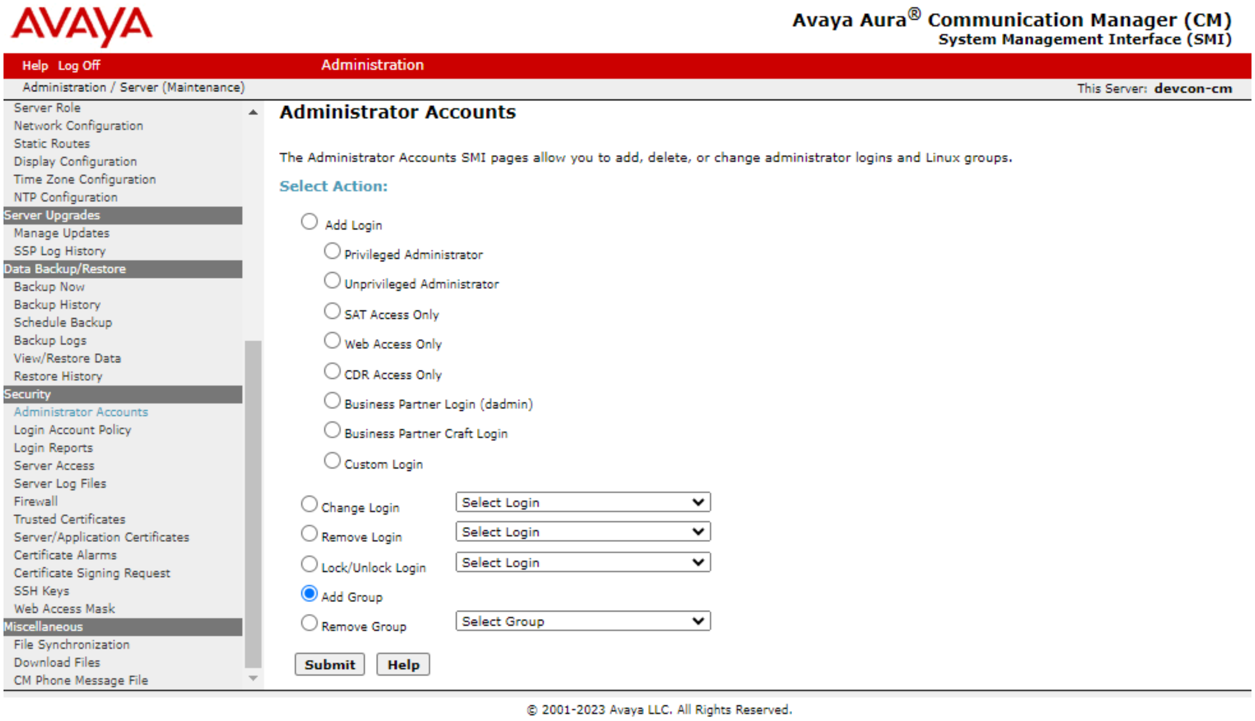
© 2001-2023 Avaya LLC. All Rights Reserved.

5.2. Configure SAT Login

This section covers the configuration of a SAT user account for Calabrio QM and its associated permissions. The SAT interface is used by Calabrio QM to retrieve capacity and station extensions from Communication Manager using SMS on Application Enablement Services.

5.2.1. Configure Login Group

Create an Access-Profile Group. Navigate to **Security → Administrator Accounts**. In the **Administrator Accounts** webpage, select **Add Group**, and then click **Submit**.



Administrator Accounts

The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups.

Select Action:

○ Add Login
- ○ Privileged Administrator
- ○ Unprivileged Administrator
- ○ SAT Access Only
- ○ Web Access Only
- ○ CDR Access Only
- ○ Business Partner Login (dadmin)
- ○ Business Partner Craft Login
- ○ Custom Login

○ Change Login — Select Login

○ Remove Login — Select Login

○ Lock/Unlock Login — Select Login

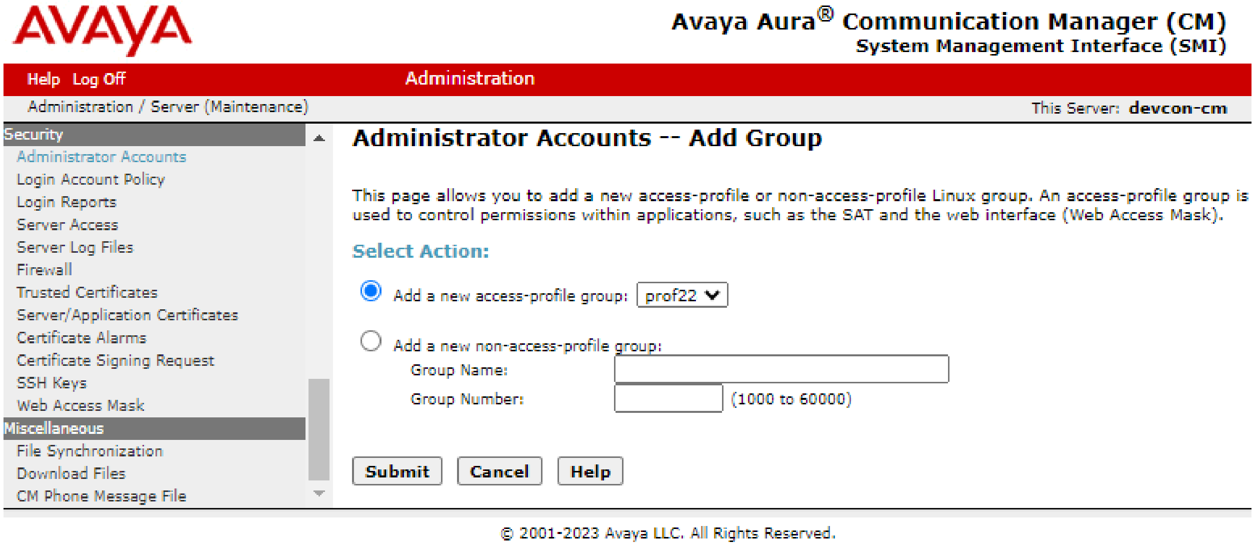
● Add Group

○ Remove Group — Select Group

Submit | Help

© 2001-2023 Avaya LLC. All Rights Reserved.

In the **Administrator Accounts – Add Group** webpage, select *prof22* from the drop-down list of the **Add a new access-profile** group field. Click **Submit**.



Administrator Accounts -- Add Group

This page allows you to add a new access-profile or non-access-profile Linux group. An access-profile group is used to control permissions within applications, such as the SAT and the web interface (Web Access Mask).

Select Action:

● Add a new access-profile group: prof22

○ Add a new non-access-profile group:

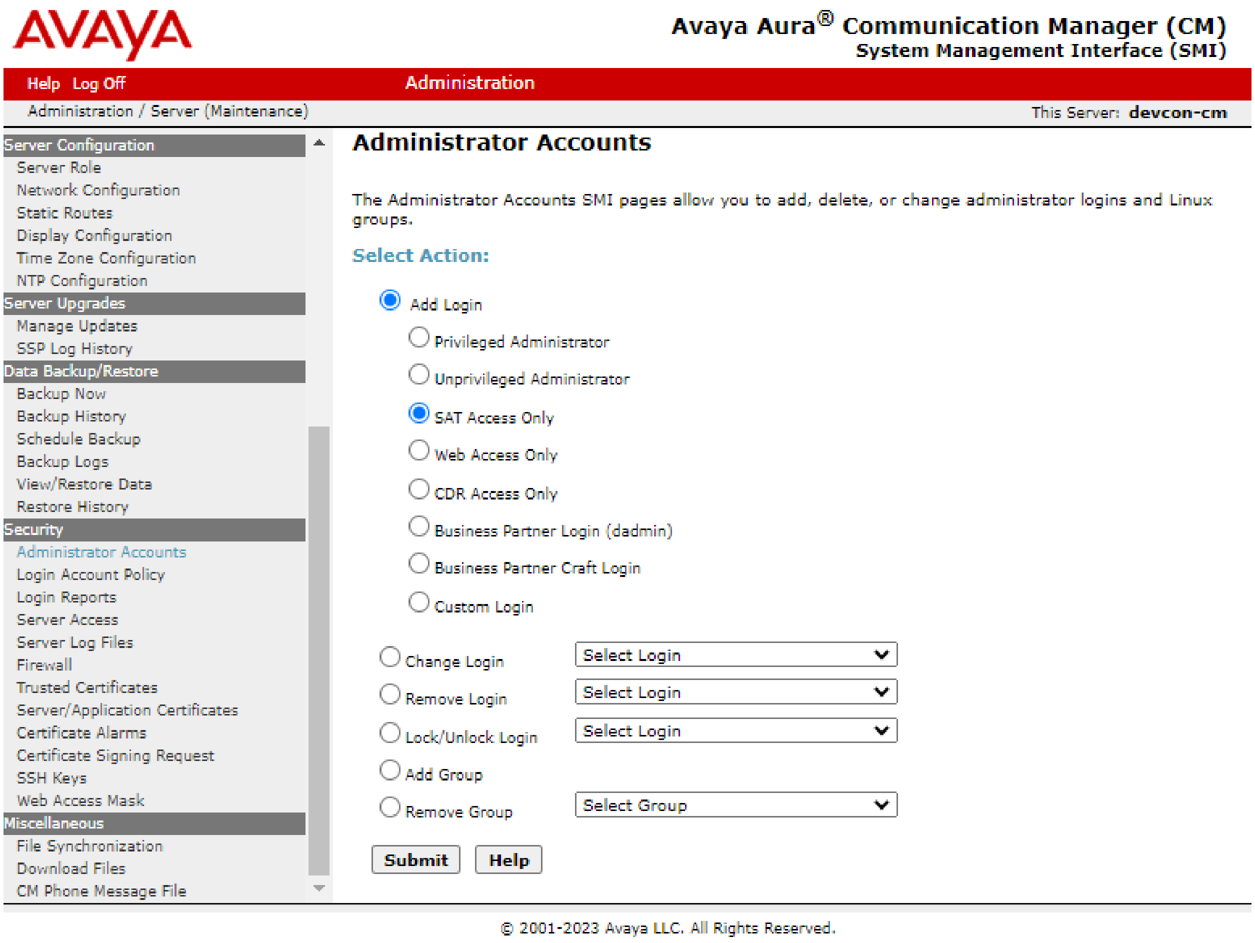
Group Name:

Group Number: (1000 to 60000)

© 2001-2023 Avaya LLC. All Rights Reserved.

5.2.2. Configure Login User

Create a login account for Calabrio QM to access the Communication Manager SAT. Navigate to **Security → Administrator Accounts** and select *SAT Access Only*. Click **Submit**.



Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)

Administrator Accounts

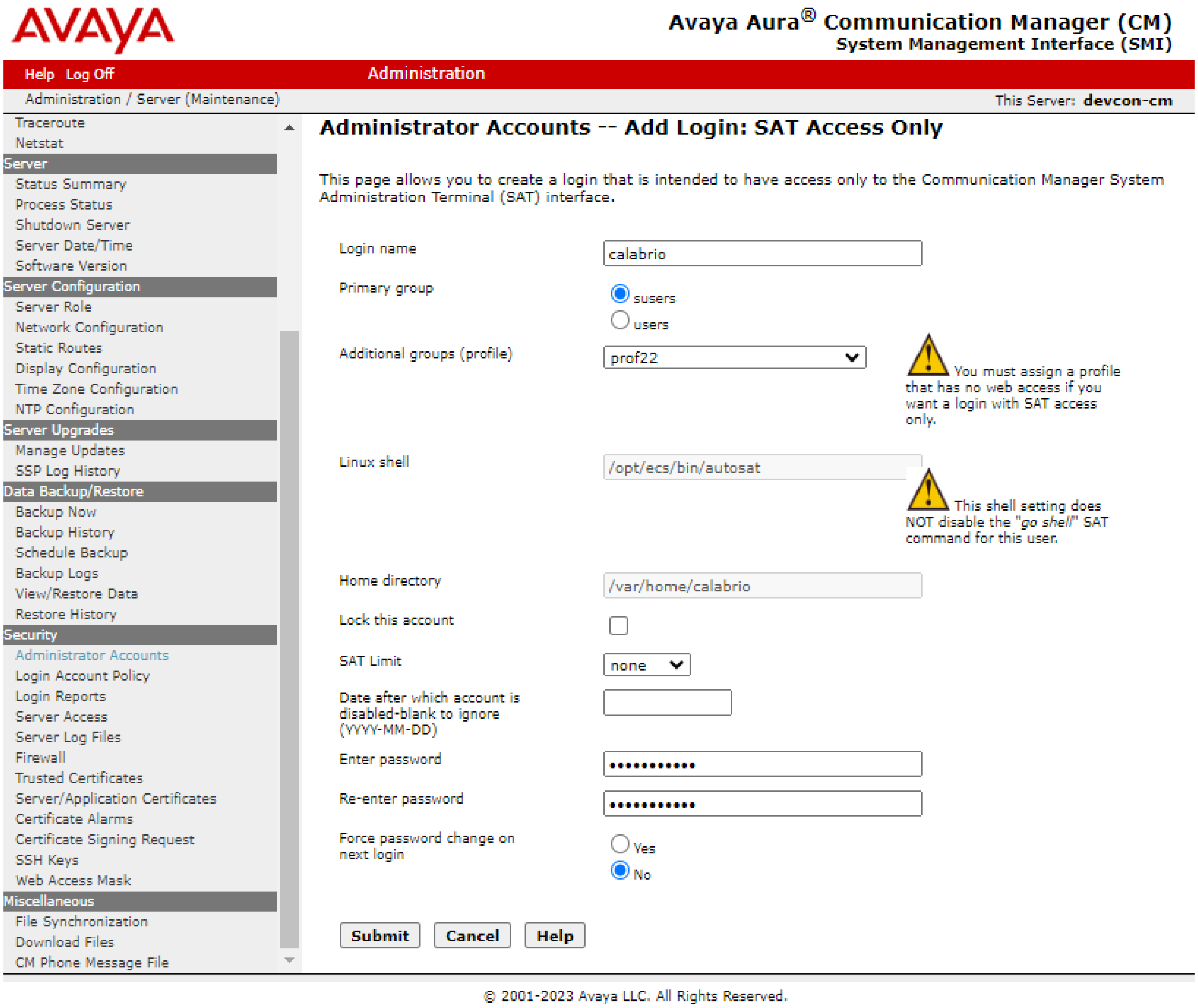
The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups.

Select Action:

- ● Add Login
  - ○ Privileged Administrator
  - ○ Unprivileged Administrator
  - ● SAT Access Only
  - ○ Web Access Only
  - ○ CDR Access Only
  - ○ Business Partner Login (dadmin)
  - ○ Business Partner Craft Login
  - ○ Custom Login
- ○ Change Login — Select Login
- ○ Remove Login — Select Login
- ○ Lock/Unlock Login — Select Login
- ○ Add Group
- ○ Remove Group — Select Group

© 2001-2023 Avaya LLC. All Rights Reserved.

In the **Administrator Accounts – Add Login: SAT Access** Only webpage, provide the **Login name** (e.g., *calabrio*), password, profile group (i.e., *prof22*), and accept all other default values. Click **Submit**.



Administrator Accounts -- Add Login: SAT Access Only

This page allows you to create a login that is intended to have access only to the Communication Manager System Administration Terminal (SAT) interface.

Login name	calabrio
Primary group	● susers ○ users
Additional groups (profile)	prof22
Linux shell	/opt/ecs/bin/autosat
Home directory	/var/home/calabrio
Lock this account	□
SAT Limit	none
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	
Enter password	•••••••••••
Re-enter password	•••••••••••
Force password change on next login	○ Yes ● No

You must assign a profile that has no web access if you want a login with SAT access only.

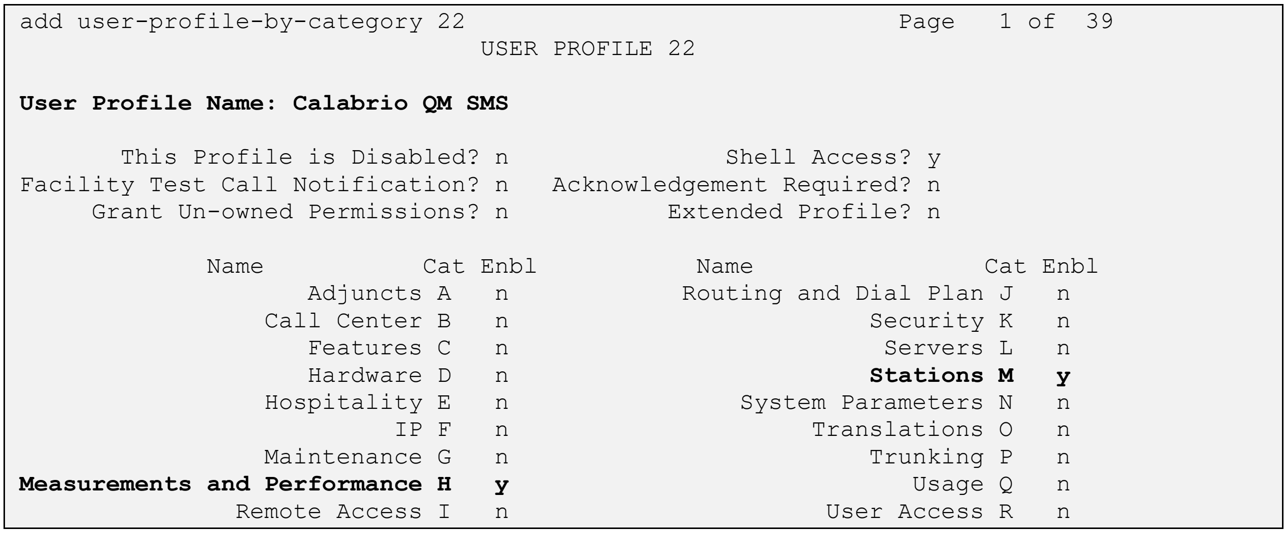
This shell setting does NOT disable the "*go shell*" SAT command for this user.

© 2001-2023 Avaya LLC. All Rights Reserved.

5.2.3. Configure SAT User Profile

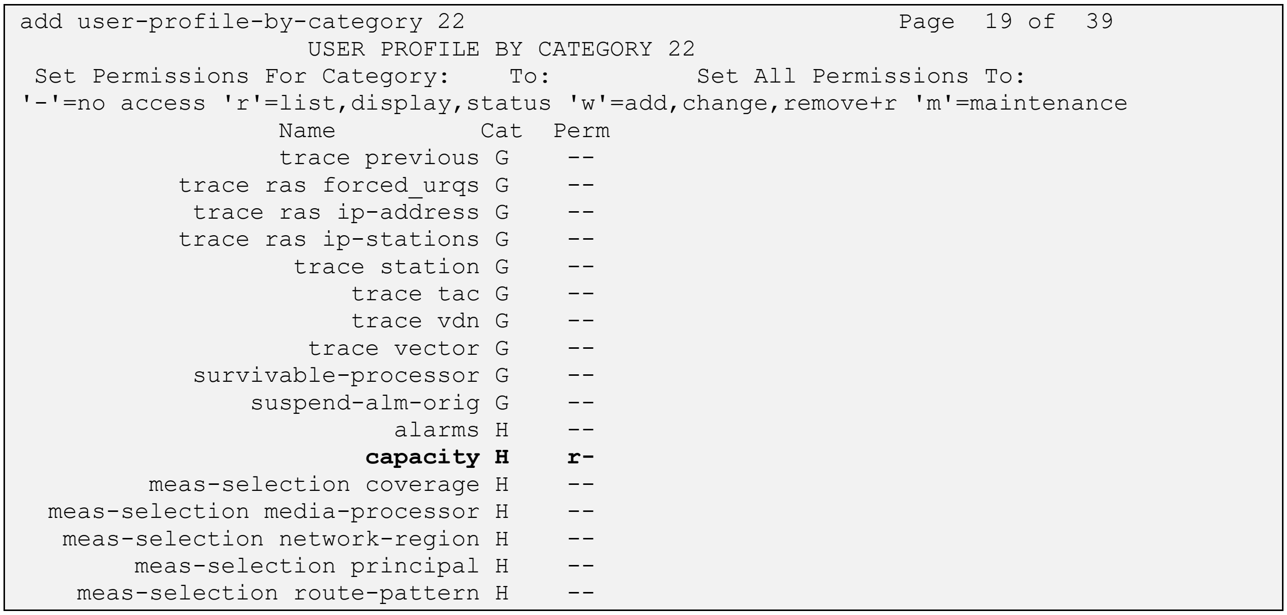
Configure a SAT User Profile via System Access Terminal (SAT). A SAT User Profile specifies which SAT screens may be accessed by the user assigned the profile and the type of access to each screen. Since Calabrio QM doesn’t modify any system configuration and only requires access to capacity and station extensions, create a SAT User Profile with limited permissions.

Use the **add user-profile-by-category 22** command, where **22** was the user profile assigned to the SAT login in **Section 5.2.2**. Enter a descriptive name for **User Profile Name** (e.g., *Calabrio QM SMS*) and enable the categories shown below. For the compliance test, user profile 22 was created.



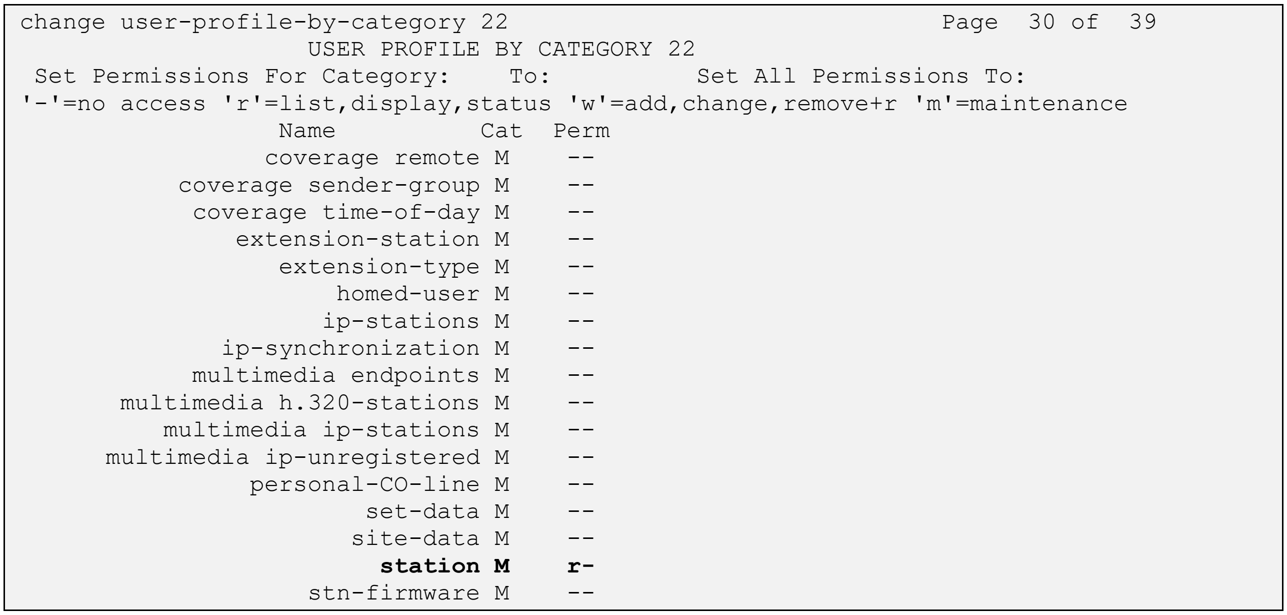
```
add user-profile-by-category 22                              Page   1 of  39
                                USER PROFILE 22

User Profile Name: Calabrio QM SMS

       This Profile is Disabled? n               Shell Access? y
Facility Test Call Notification? n   Acknowledgement Required? n
     Grant Un-owned Permissions? n           Extended Profile? n

             Name           Cat Enbl           Name                Cat Enbl
                    Adjuncts A   n            Routing and Dial Plan J   n
                 Call Center B   n                         Security K   n
                    Features C   n                          Servers L   n
                    Hardware D   n                         Stations M   y
                 Hospitality E   n                System Parameters N   n
                          IP F   n                     Translations O   n
                 Maintenance G   n                         Trunking P   n
Measurements and Performance H   y                            Usage Q   n
               Remote Access I   n                      User Access R   n
```

On Page 19, set **capacity** to *r-* to provide read-only access to capacity information. Calabrio QM uses the **display capacity** command to retrieve the station capacity in the **Capacity** form.



```
add user-profile-by-category 22                              Page  19 of  39
                    USER PROFILE BY CATEGORY 22
 Set Permissions For Category:    To:          Set All Permissions To:
'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance
                  Name          Cat  Perm
                  trace previous G    --
           trace ras forced_urqs G    --
            trace ras ip-address G    --
           trace ras ip-stations G    --
                   trace station G    --
                       trace tac G    --
                       trace vdn G    --
                    trace vector G    --
            survivable-processor G    --
                suspend-alm-orig G    --
                          alarms H    --
                        capacity H    r-
         meas-selection coverage H    --
  meas-selection media-processor H    --
   meas-selection network-region H    --
        meas-selection principal H    --
    meas-selection route-pattern H    --
```

On Page 30, set **station** to *r-* to provide read-only access to station information. Calabrio QM uses the **list stations** and **display station** commands to retrieve station extensions and other information.



```
change user-profile-by-category 22                              Page  30 of  39
                    USER PROFILE BY CATEGORY 22
 Set Permissions For Category:    To:          Set All Permissions To:
'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance
                  Name          Cat  Perm
                 coverage remote M    --
           coverage sender-group M    --
            coverage time-of-day M    --
               extension-station M    --
                  extension-type M    --
                      homed-user M    --
                     ip-stations M    --
              ip-synchronization M    --
            multimedia endpoints M    --
       multimedia h.320-stations M    --
          multimedia ip-stations M    --
      multimedia ip-unregistered M    --
                personal-CO-line M    --
                        set-data M    --
                       site-data M    --
                         station M    r-
                    stn-firmware M    --
```

5.3. Configure CDR

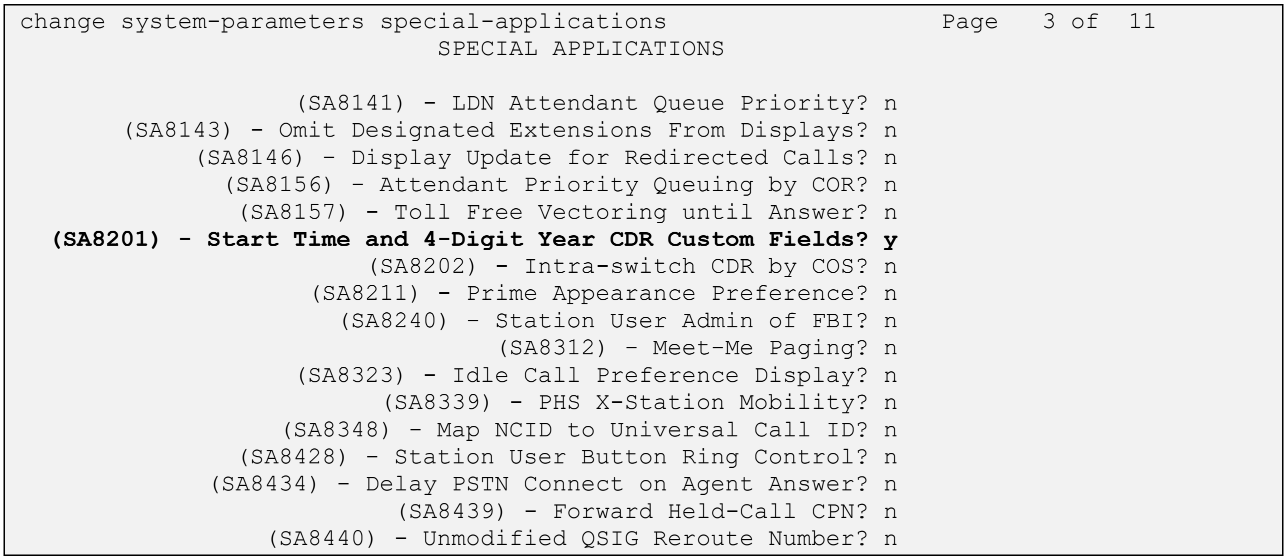
This section covers the Communication Manager CDR configuration, including:

- Enable Special Applications
- Administer IP Node Names
- Administer CDR Link
- Enabled CDR for Intra-Switch Calls
- Enable CDR for Trunk Calls

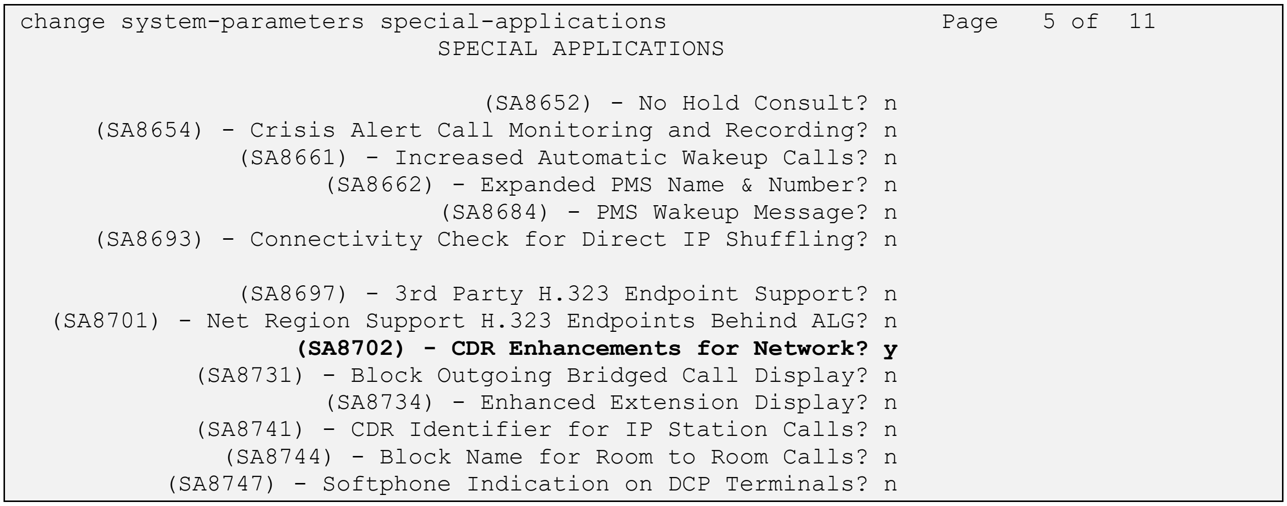
5.3.1. Enable Special Applications

Enable the following special applications for CDR.

- (SA8201) – Start Time and 4-Digit Year CDR Custom Fields
- (SA8702) – CDR Enhancements for Network



```
change system-parameters special-applications                   Page   3 of  11
                             SPECIAL APPLICATIONS

                   (SA8141) - LDN Attendant Queue Priority? n
       (SA8143) - Omit Designated Extensions From Displays? n
            (SA8146) - Display Update for Redirected Calls? n
              (SA8156) - Attendant Priority Queuing by COR? n
               (SA8157) - Toll Free Vectoring until Answer? n
  (SA8201) - Start Time and 4-Digit Year CDR Custom Fields? y
                        (SA8202) - Intra-switch CDR by COS? n
                    (SA8211) - Prime Appearance Preference? n
                      (SA8240) - Station User Admin of FBI? n
                                 (SA8312) - Meet-Me Paging? n
                   (SA8323) - Idle Call Preference Display? n
                         (SA8339) - PHS X-Station Mobility? n
                  (SA8348) - Map NCID to Universal Call ID? n
               (SA8428) - Station User Button Ring Control? n
             (SA8434) - Delay PSTN Connect on Agent Answer? n
                          (SA8439) - Forward Held-Call CPN? n
                 (SA8440) - Unmodified QSIG Reroute Number? n
```



```
change system-parameters special-applications                   Page   5 of  11
                             SPECIAL APPLICATIONS

                                (SA8652) - No Hold Consult? n
     (SA8654) - Crisis Alert Call Monitoring and Recording? n
               (SA8661) - Increased Automatic Wakeup Calls? n
                     (SA8662) - Expanded PMS Name & Number? n
                             (SA8684) - PMS Wakeup Message? n
     (SA8693) - Connectivity Check for Direct IP Shuffling? n

               (SA8697) - 3rd Party H.323 Endpoint Support? n
  (SA8701) - Net Region Support H.323 Endpoints Behind ALG? n
                   (SA8702) - CDR Enhancements for Network? y
            (SA8731) - Block Outgoing Bridged Call Display? n
                     (SA8734) - Enhanced Extension Display? n
            (SA8741) - CDR Identifier for IP Station Calls? n
              (SA8744) - Block Name for Room to Room Calls? n
          (SA8747) - Softphone Indication on DCP Terminals? n
```

5.3.2. Administer IP Node Names

Use the **change node-names ip** command to associate the IP address of Calabrio QM Data Server to a node name. In the compliance test, the node name *CDR-Calabrio* was assigned to IP address *10.64.102.144*. Also, highlighted in the example below is the node name *procr*, which represents the Processor Ethernet IP address used as the source of CDR data. These node names are required for the CDR link configuration in **Section 5.3.3**.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
CDR-Calabrio        10.64.102.144
default             0.0.0.0
devcon-aes          10.64.102.119
devcon-ams          10.64.102.118
devcon-sm           10.64.102.117
meetings            10.64.102.140
procr               10.64.102.115
procr6              ::

( 8  of 8    administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

5.3.3. Administer CDR Link

Use the **change ip-services** command to configure the CDR link between Communication Manager and Calabrio QM Data Server.

- **Service Type:** Set to *CDR1* for the primary CDR link.
- **Local Node:** Set to the Processor Ethernet interface, which terminates the CDR link on Communication Manager, configured in **Section 5.3.2**.
- **Local Port:** Set to *0*.
- **Remote Node**: Set to the node name defined for Calabrio QM Data Server, which is *CDR-Calabrio* for this compliance test.
- **Remote Port:** Set to a value between 5000 and 64500 inclusive, which must match the port configured on Calabrio QM in **Section 8.2**. In this example, remote port *9002* was used.
- **TLS Encryption:** Disable this option.

```
change ip-services                                              Page   1 of   4

                                   IP SERVICES
 Service     Enabled     Local        Local        Remote      Remote    TLS
  Type                   Node         Port         Node        Port   Encryption
CDR1                 procr            0       CDR-Calabrio    9002        n
```

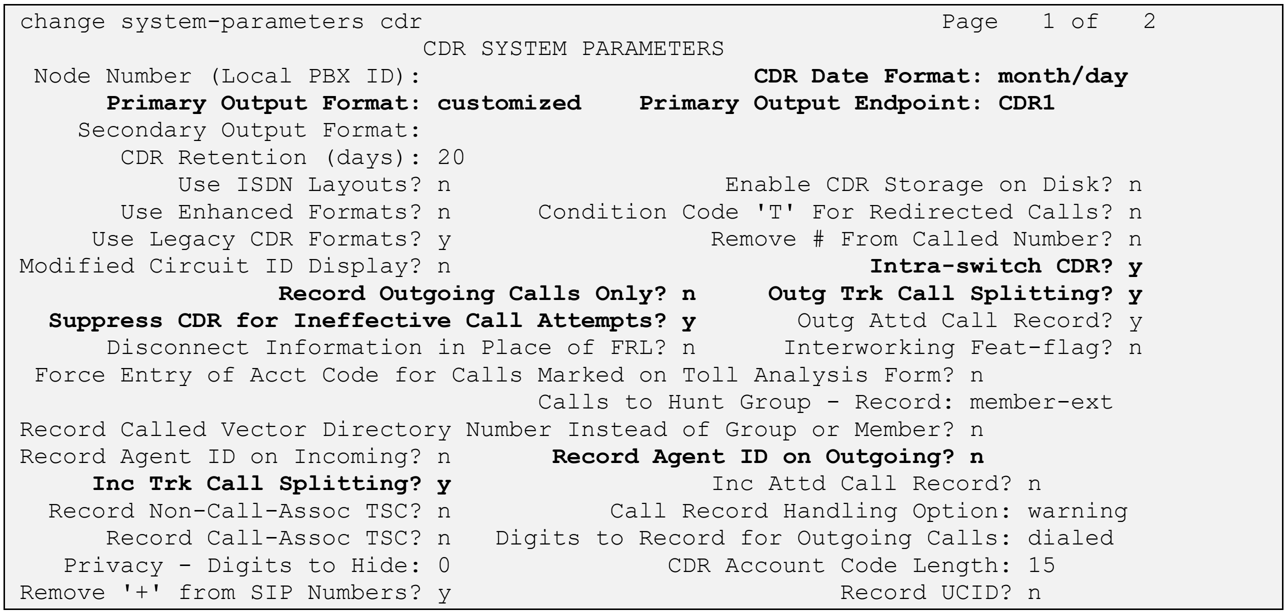
On **Page 3**, set the **Reliable Protocol** field to ***y*** to enable the use of the Avaya Reliable Session Protocol (RSP) for reliable CDR transmission.

```
change ip-services                                              Page   3 of   4

                              SESSION LAYER TIMERS
  Service     Reliable  Packet Resp   Session Connect  SPDU  Connectivity
   Type       Protocol     Timer       Message Cntr    Cntr     Timer

 CDR1            y        30                3          3         60
```

Use the **change system-parameters cdr** command to administer the following CDR system parameters. See reference **[2]** for a full explanation of each field.

- **CDR Date Format:** Set to *month/day*.
- **Primary Output Format**: Set to *customized*.
- **Primary Output Endpoint**: Set to *CDR1*.
- **Intra-switch CDR:** Enable this option to allow call records for internal calls. Refer to **Section 5.3.4**.
- **Record Outgoing Calls Only:** Disable this option to allow CDR for both incoming and outgoing trunk calls.
- **Outg Trk Call Splitting:** Enable this option to allow CDR to create separate records for each portion of an outgoing call that is transferred or conferenced.
- **Suppress CDR for Ineffective Call Attempts:** Enable this option to ignore ineffective call attempts.
- **Record Agent ID on Outgoing:** Disable this option to record the station extension in the **Calling Number** field of the CDR. For this solution, Calabrio QM reconciles root calls based on station extensions, not agent login-IDs.
- **Inc Trk Call Splitting:** Enable this option to allow CDR to create separate records for each portion of an incoming call that is transferred or conferenced.

Default values may be used for all other fields.



```
change system-parameters cdr                                    Page   1 of   2
                            CDR SYSTEM PARAMETERS
 Node Number (Local PBX ID):                       CDR Date Format: month/day
      Primary Output Format: customized    Primary Output Endpoint: CDR1
    Secondary Output Format:
       CDR Retention (days): 20
           Use ISDN Layouts? n                   Enable CDR Storage on Disk? n
       Use Enhanced Formats? n      Condition Code 'T' For Redirected Calls? n
     Use Legacy CDR Formats? y                  Remove # From Called Number? n
Modified Circuit ID Display? n                             Intra-switch CDR? y
                  Record Outgoing Calls Only? n     Outg Trk Call Splitting? y
  Suppress CDR for Ineffective Call Attempts? y       Outg Attd Call Record? y
      Disconnect Information in Place of FRL? n      Interworking Feat-flag? n
 Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                    Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? n       Record Agent ID on Outgoing? n
     Inc Trk Call Splitting? y                  Inc Attd Call Record? n
  Record Non-Call-Assoc TSC? n           Call Record Handling Option: warning
      Record Call-Assoc TSC? n   Digits to Record for Outgoing Calls: dialed
   Privacy - Digits to Hide: 0               CDR Account Code Length: 15
Remove '+' from SIP Numbers? y                           Record UCID? n
```

Page 2 specifies the customized record format that defines the call records sent to Calabrio QM Data Server. Calabrio QM requires the following data items in bold. The CDR record format defined below were used for the compliance test.

Notes: The **Duration** data item should not be included. If the **in-crt-id** and/or **out-crt-id** data items are included, they should be configured with a length of 3. If the **vdn** data field is used, it should be configured with a length of 13.

```
change system-parameters cdr                                    Page   2 of   2
                            CDR SYSTEM PARAMETERS

     Data Item - Length         Data Item - Length         Data Item - Length
 1: date             - 6   17: attd-console     - 2   33:                   -
 2: time             - 4   18: auth-code        - 13  34:                   -
 3: sec-dur          - 5   19: ucid             - 20  35:                   -
 4: cond-code        - 1   20: calling-num      - 15  36:                   -
 5: code-dial        - 4   21: calltype         - 1   37:                   -
 6: code-used        - 4   22: ma-uui           - 1   38:                   -
 7: dialed-num       - 23  23: vdn              - 13  39:                   -
 8: end-time         - 6   24: start-time       - 6   40:                   -
 9: space            - 1   25: return           - 1   41:                   -
10: ppm              - 5   26: line-feed        - 1   42:                   -
11: in-crt-id        - 3   27:                  -     43:                   -
12: out-crt-id       - 3   28:                  -     44:                   -
13: space            - 1   29:                  -     45:                   -
14: feat-flag        - 1   30:                  -     46:                   -
15: frl              - 1   31:                  -     47:                   -
16: clg-pty-cat      - 2   32:                  -     48:                   -

                              Record length = 143
```

5.3.4. Enable CDR for Intra-Switch Calls

If **Intra-switch CDR** is enabled in the CDR system parameters, use **change intra-switch-cdr** command to define the extensions that will be subject to CDR for local calls. Both H.323 and SIP extensions were added to this table for the compliance test.

```
change intra-switch-cdr                                         Page   1 of   3
                           INTRA-SWITCH CDR

                                Assigned Members:   4    of 5000   administered
   Extension          Extension          Extension          Extension
   77301
   77400
   78002
   78004


Use 'list intra-switch-cdr' to see all members, 'add intra-switch-cdr' to add
new members and 'change intra-switch-cdr <ext>' to change/remove other members
```

5.4. Enable CDR for Trunk Calls

For each trunk group for which CDR records are desired, verify that CDR reporting is enabled. Use the **change trunk-group *n*** command, where ***n*** is the trunk group number, to verify that the **CDR Reports** field is set to *y*.

The example below shows the SIP trunk between Communication Manager and Session Manager used for local SIP calls.

```
change trunk-group 10                                           Page   1 of   5
                                TRUNK GROUP

Group Number: 10                   Group Type: sip          CDR Reports: y
  Group Name: To devcon-sm                COR: 1        TN: 1        TAC: 1010
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 10
                                                     Number of Members: 10
```

The example below shows the SIP trunk between Communication Manager and Session Manager used for PSTN calls routed through Avaya SBC.

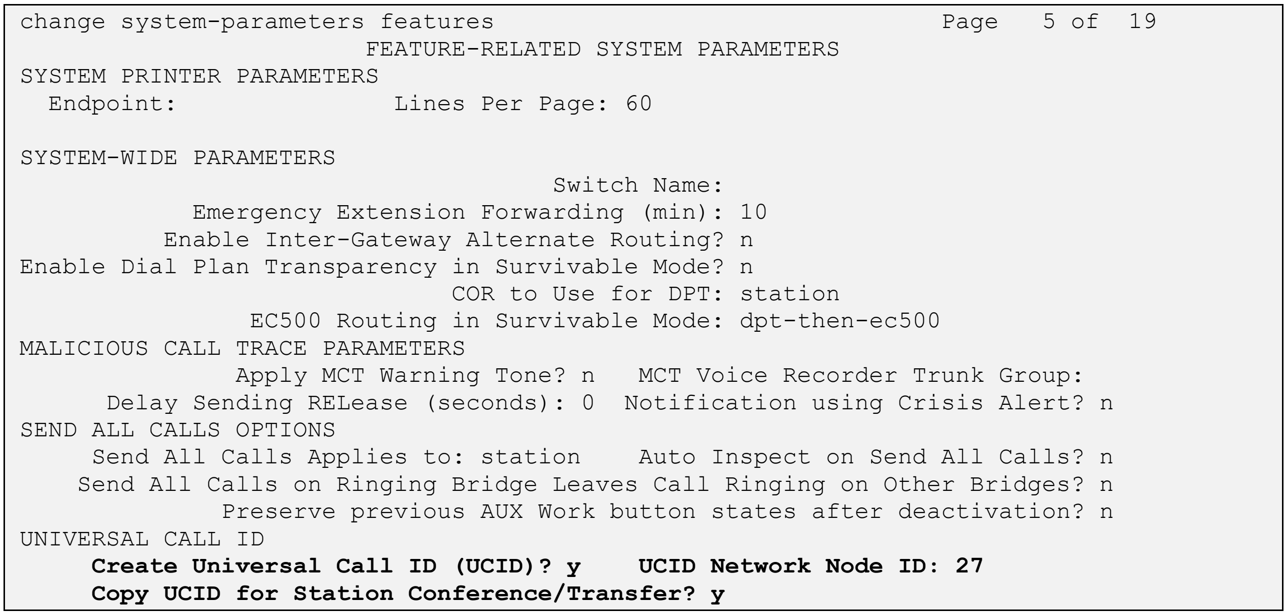
```
change trunk-group 11                                           Page   1 of   5
                                TRUNK GROUP

Group Number: 11                   Group Type: sip          CDR Reports: y
  Group Name: To SIP Service Provider     COR: 1        TN: 1        TAC: 1011
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 11
                                                     Number of Members: 10
```

5.5. Configure UCID Support

This section covers the configuration for Communication Manager to generate a UCID for outgoing calls and to send UCID over SIP trunks.

5.5.1. Administer System Parameters Features

Use the **change system-parameters features** command to enable **Create Universal Call ID (UCID)**, which is located on **Page 5**. For **UCID Network Node ID**, enter an available node ID, and enable **Copy UCID for Station Conference/Transfer**. The UCID is used to track calls across Communication Manager and Calabrio QM. The UCID Network Node ID is used for outbound calls from an agent to the PSTN.



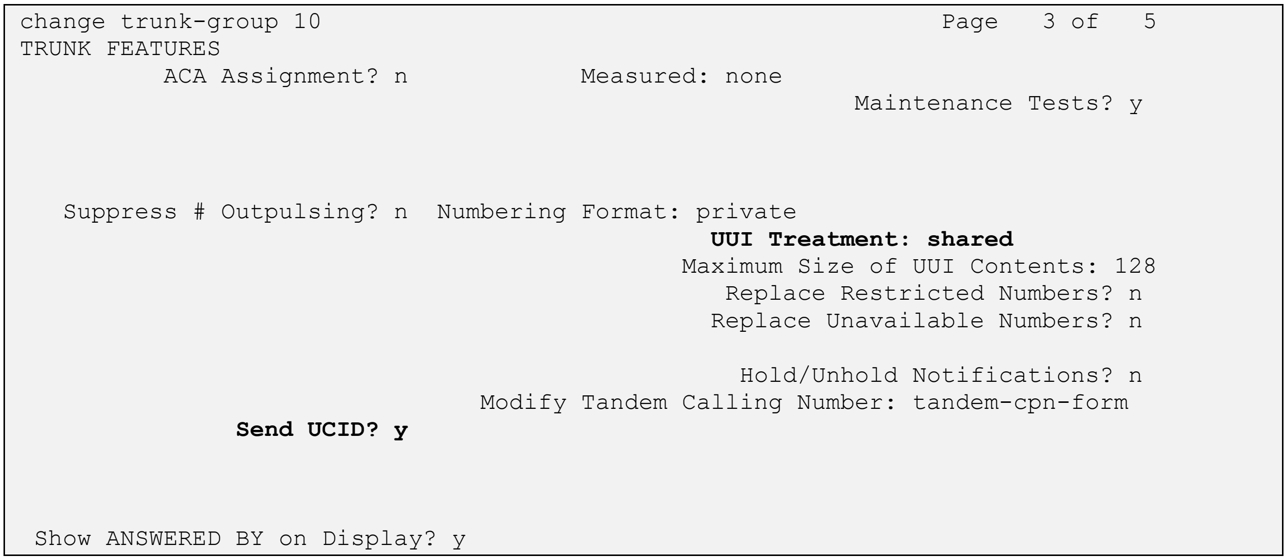
```
change system-parameters features                               Page   5 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
SYSTEM PRINTER PARAMETERS
  Endpoint:               Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                                     Switch Name:
            Emergency Extension Forwarding (min): 10
          Enable Inter-Gateway Alternate Routing? n
Enable Dial Plan Transparency in Survivable Mode? n
                              COR to Use for DPT: station
                EC500 Routing in Survivable Mode: dpt-then-ec500
MALICIOUS CALL TRACE PARAMETERS
               Apply MCT Warning Tone? n   MCT Voice Recorder Trunk Group:
      Delay Sending RELease (seconds): 0  Notification using Crisis Alert? n
SEND ALL CALLS OPTIONS
     Send All Calls Applies to: station    Auto Inspect on Send All Calls? n
    Send All Calls on Ringing Bridge Leaves Call Ringing on Other Bridges? n
              Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
     Create Universal Call ID (UCID)? y    UCID Network Node ID: 27
     Copy UCID for Station Conference/Transfer? y
```

5.5.2. Administer SIP Trunk Group

The SIP trunks between Communication Manager and Session Manager used for local calls and PSTN calls should be configured to send UCID. Use the **change trunk-group** command to modify the SIP trunk groups for local and PSTN calls. Navigate to **Page 3** and configure the following fields.

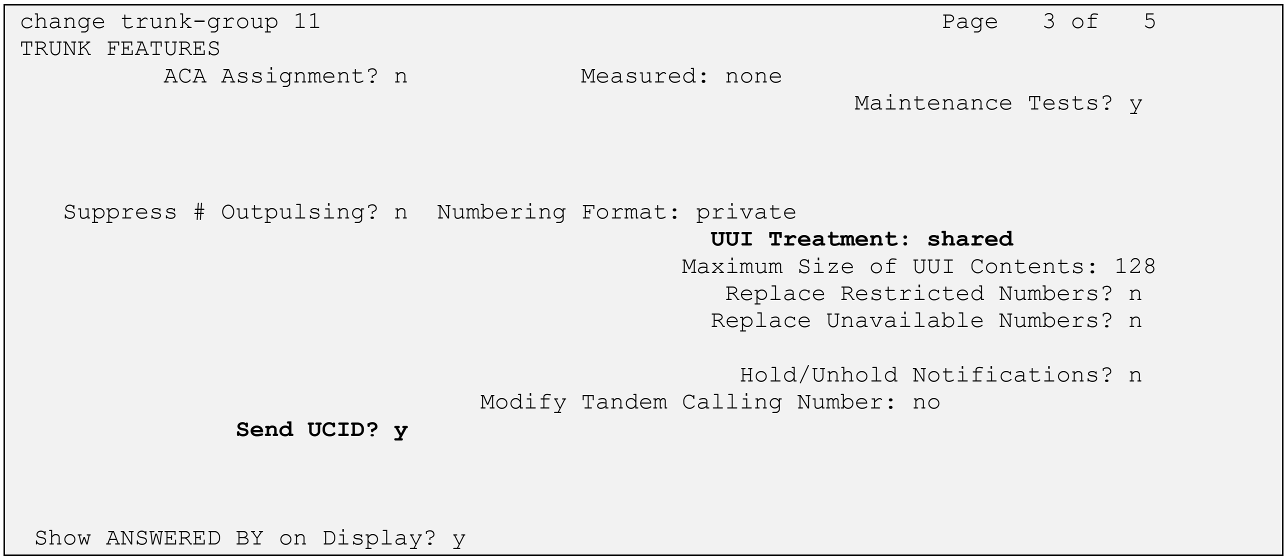
- **UUI Treatment:** Set to *shared*.
- **Send UCID:** Enable this option.

SIP trunk group 10 was used for local calls.



```
change trunk-group 10                                           Page   3 of   5
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



   Suppress # Outpulsing? n  Numbering Format: private
                                                UUI Treatment: shared
                                              Maximum Size of UUI Contents: 128
                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n

                                                  Hold/Unhold Notifications? n
                                Modify Tandem Calling Number: tandem-cpn-form
               Send UCID? y



 Show ANSWERED BY on Display? y
```

SIP trunk group 11 was used for PSTN calls routed through Avaya SBC.



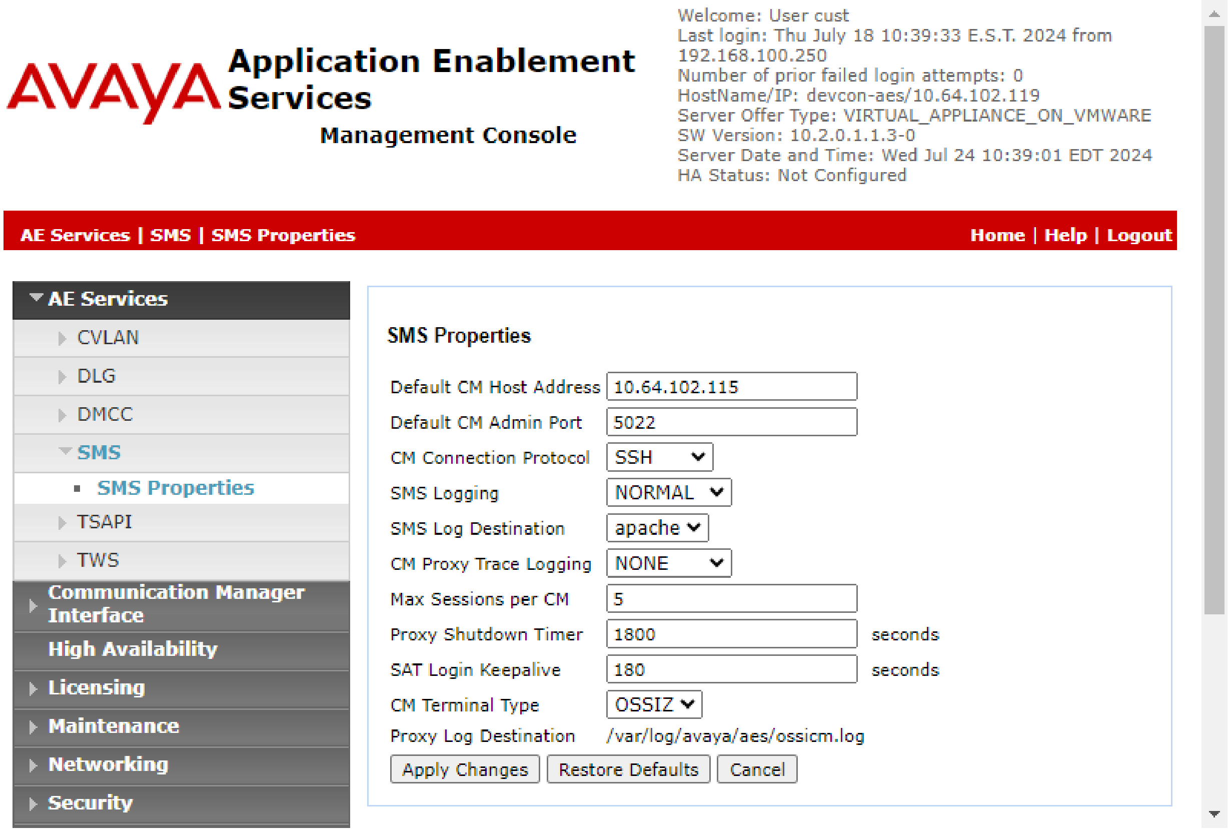
```
change trunk-group 11                                           Page   3 of   5
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



   Suppress # Outpulsing? n  Numbering Format: private
                                                UUI Treatment: shared
                                              Maximum Size of UUI Contents: 128
                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n

                                                  Hold/Unhold Notifications? n
                                Modify Tandem Calling Number: no
               Send UCID? y



 Show ANSWERED BY on Display? y
```

6. Configure Avaya Aura® Application Enablement Services

This section covers the configuration of SMS Properties, which is used by the SMS web service to access managed objects on Communication Manager. Calabrio QM only requests read-only access to managed objects via the SMS web service and will provide the Communication Manager login credentials to Application Enablement Services configured in **Section 5.2**.

Access the OAM web-based interface by using the URL "https://<*ip-address*>" in a web browser window, where <*ip-address*> is the IP address of Application Enablement Services. Log in using the appropriate credentials (not shown).

Navigate to **AE Services → SMS → SMS Properties**. In **SMS Properties**, set the **Default CM Host Address** to the Communication Manager IP address (e.g., *10.64.102.115*) and accept the default values for the other fields.



Welcome: User cust
Last login: Thu July 18 10:39:33 E.S.T. 2024 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.2.0.1.1.3-0
Server Date and Time: Wed Jul 24 10:39:01 EDT 2024
HA Status: Not Configured

SMS Properties

Default CM Host Address	10.64.102.115	
Default CM Admin Port	5022	
CM Connection Protocol	SSH	
SMS Logging	NORMAL	
SMS Log Destination	apache	
CM Proxy Trace Logging	NONE	
Max Sessions per CM	5	
Proxy Shutdown Timer	1800	seconds
SAT Login Keepalive	180	seconds
CM Terminal Type	OSSIZ	
Proxy Log Destination	/var/log/avaya/aes/ossicm.log	

Apply Changes | Restore Defaults | Cancel

7. Configure Avaya Session Border Controller

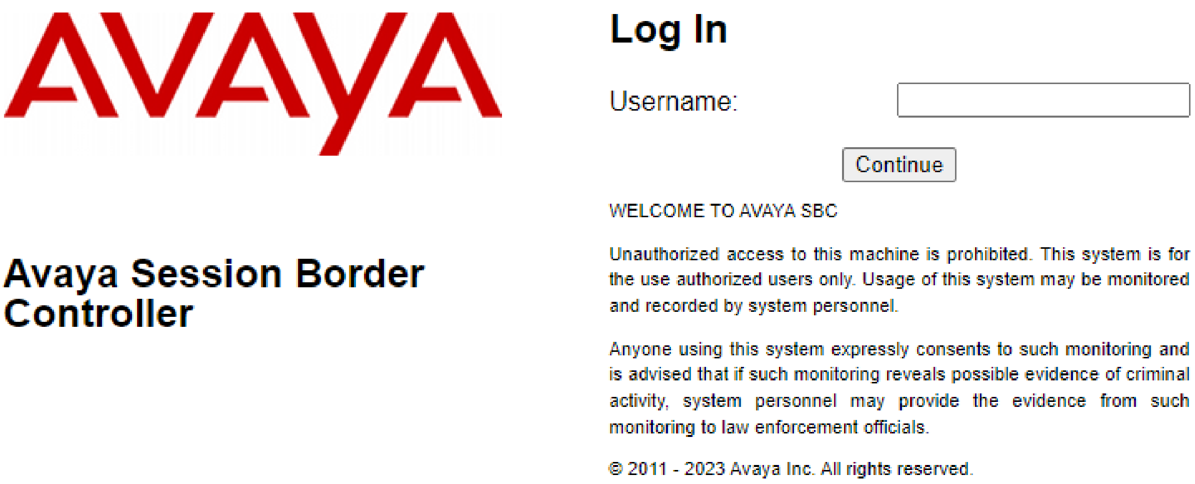
This section covers the SBC configuration required to establish a SIP trunk to Record for call recording using SIPREC. This section covers the following SBC configuration:

- Launch SBC Web Interface
- Administer TLS Management
- Administer SIP Servers
- Administer Routing Profiles
- Administer Media Rules
- Administer Signaling Rules
- Administer End Point Policy Groups
- Administer Recording Profile
- Administer Session Policies
- Administer Session Flows
- Administer Server Flows

Note: It is assumed that basic SBC configuration has already been performed, including SIP trunk and routing to Session Manager and PSTN for customer calls. However, any changes required for this solution to the existing configuration will be covered.

7.1. Launch SBC Web Interface

Access the SBC web interface by using the URL **https://<*ip-address*>/sbc** in an Internet browser, where **<*ip-address*>** is the IP address of the SBC management interface. The screen below is displayed. Log in using the appropriate credentials.



Avaya Session Border Controller

Log In

Username:

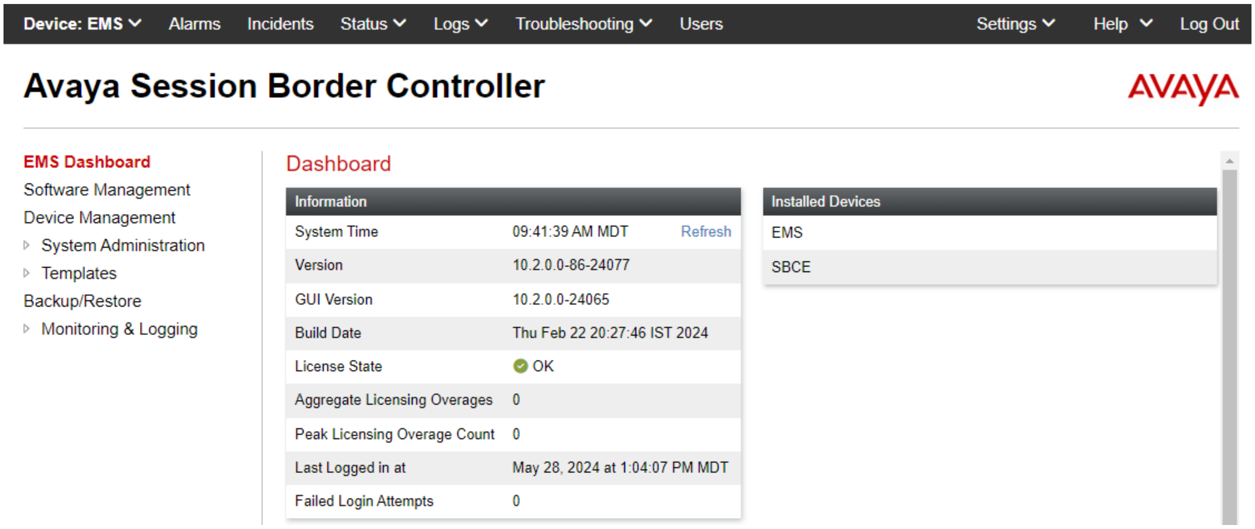
WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2023 Avaya Inc. All rights reserved.

After logging in, the **Dashboard** will appear as shown below. All configuration screens of the SBC are accessed by navigating the menu tree in the left pane. Select **Device → SBCE** from the top menu.



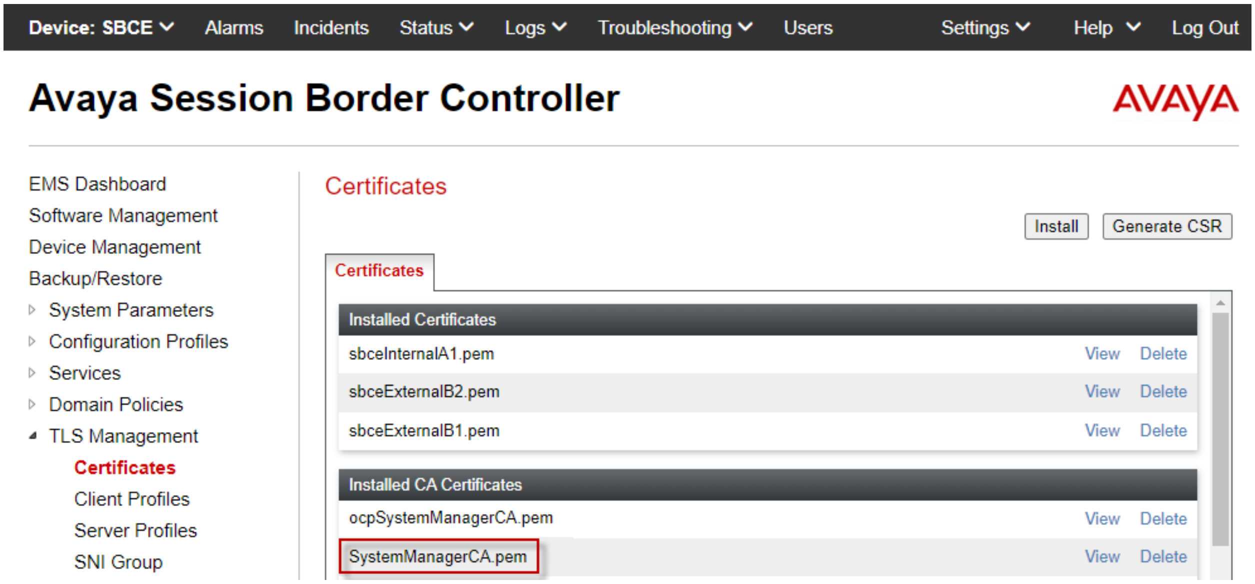
Information	
System Time	09:41:39 AM MDT
Version	10.2.0.0-86-24077
GUI Version	10.2.0.0-24065
Build Date	Thu Feb 22 20:27:46 IST 2024
License State	✓ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	May 28, 2024 at 1:04:07 PM MDT
Failed Login Attempts	0

Installed Devices
EMS
SBCE

7.2. Administer TLS Management

The SIP trunk between Avaya SBC and Calabrio QM Data Server will use TLS transport. For the compliance test, System Manager was used as the certificate authority. Therefore, the System Manager CA certificate was installed on Avaya SBC as shown below under TLS **Management → Certificates**. This section is provided for informational purposes only as TLS management may differ at customer sites.

Note: For the compliance test, a certificate for Calabrio QM Data Server was created by generating a certificate signing request using the Microsoft Management Console (MMC) Certificate Snap-in on the data server and signing the certificate by the System Manager CA. No additional Calabrio QM certificate was required to be installed on Avaya SBC.



Avaya Session Border Controller

Certificates

Installed Certificates

sbceInternalA1.pem View Delete

sbceExternalB2.pem View Delete

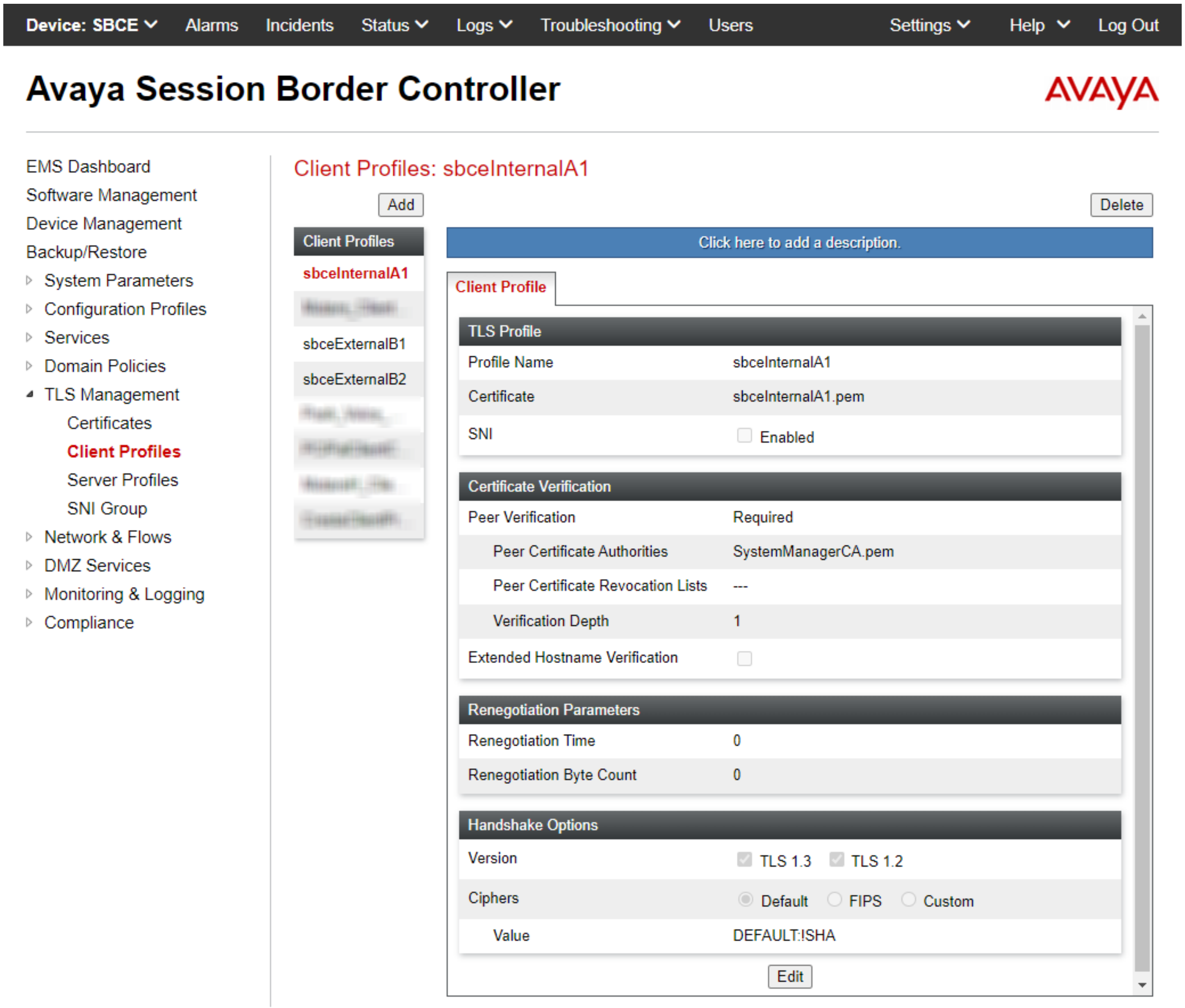
sbceExternalB1.pem View Delete

Installed CA Certificates

ocpSystemManagerCA.pem View Delete

SystemManagerCA.pem View Delete

Navigate to **TLS Management → Client Profiles** and create a **Client Profile** for Calabrio QM Data Server as shown below. Set **Certificate** to the identity certificate assigned to the private SBC interface, which connects to Calabrio QM Data Server. For **Peer Certificate Authorities**, select the System Manager CA certificate. Set the **Verification Depth** to *1*. Default values for the remaining fields may be used. Calabrio QM Data Server used TLS 1.2, which is enabled by default.



Client Profiles: sbceInternalA1

Client Profiles
- sbceInternalA1
- [redacted]
- sbceExternalB1
- sbceExternalB2
- [redacted]
- [redacted]
- [redacted]
- [redacted]

TLS Profile	
Profile Name	sbceInternalA1
Certificate	sbceInternalA1.pem
SNI	☐ Enabled

Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	SystemManagerCA.pem
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	☐

Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0

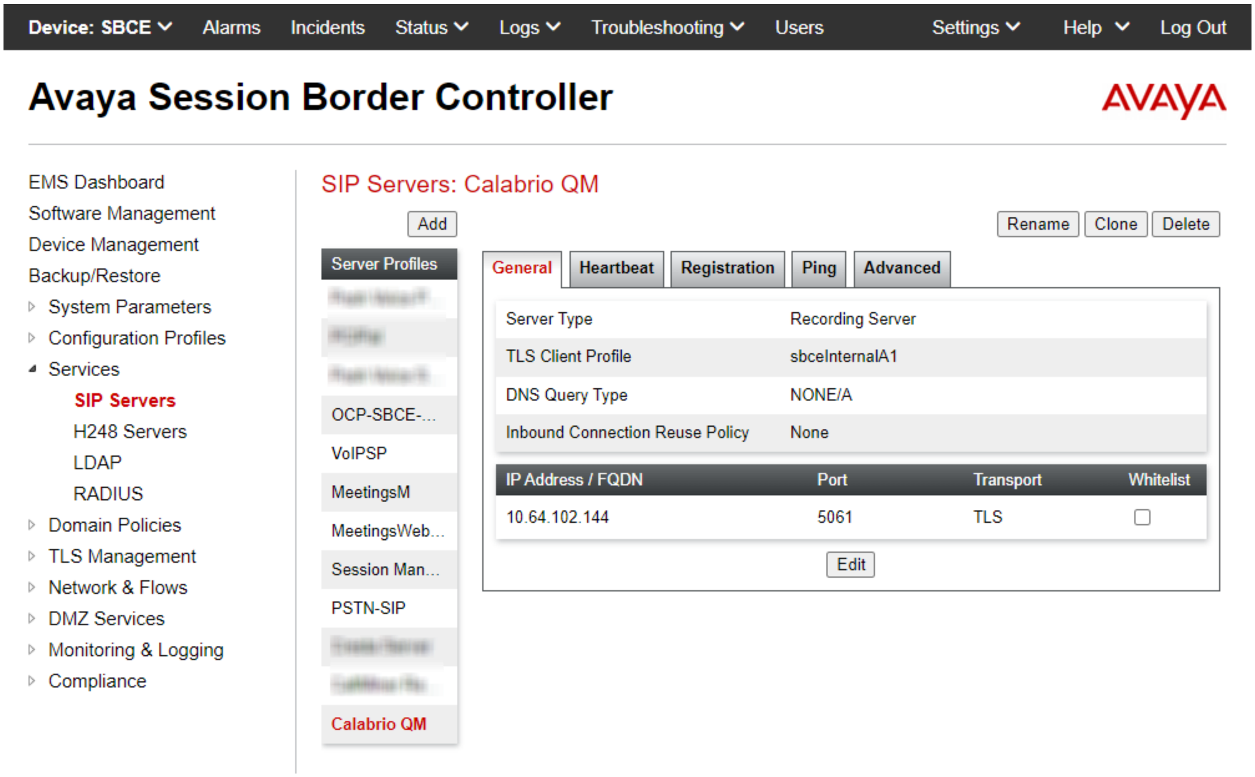
Handshake Options	
Version	☑ TLS 1.3 ☑ TLS 1.2
Ciphers	● Default ○ FIPS ○ Custom
Value	DEFAULT:!SHA

7.3. Administer SIP Servers

Navigate to **Services → SIP Servers** from the left pane to create a SIP server for Calabrio QM. Calabrio QM is configured as a recording server to allow session recording using SIPREC. Click **Add** to create a SIP Server for Record.

The **General** tab of the Calabrio QM SIP server was configured with the following field values.

▪ **Server Type:**	Set to *Recording Server* since Calabrio QM will record SIP sessions.
▪ **TLS Client Profile:**	Set to the **TLS Client Profile** configured in **Section 7.2**.
▪ **IP Address / FQDN:**	For the compliance test, the Calabrio QM Data Server IP address was used.
▪ **Port:**	Set to *5061*.
▪ **Transport:**	Set to *TLS*.

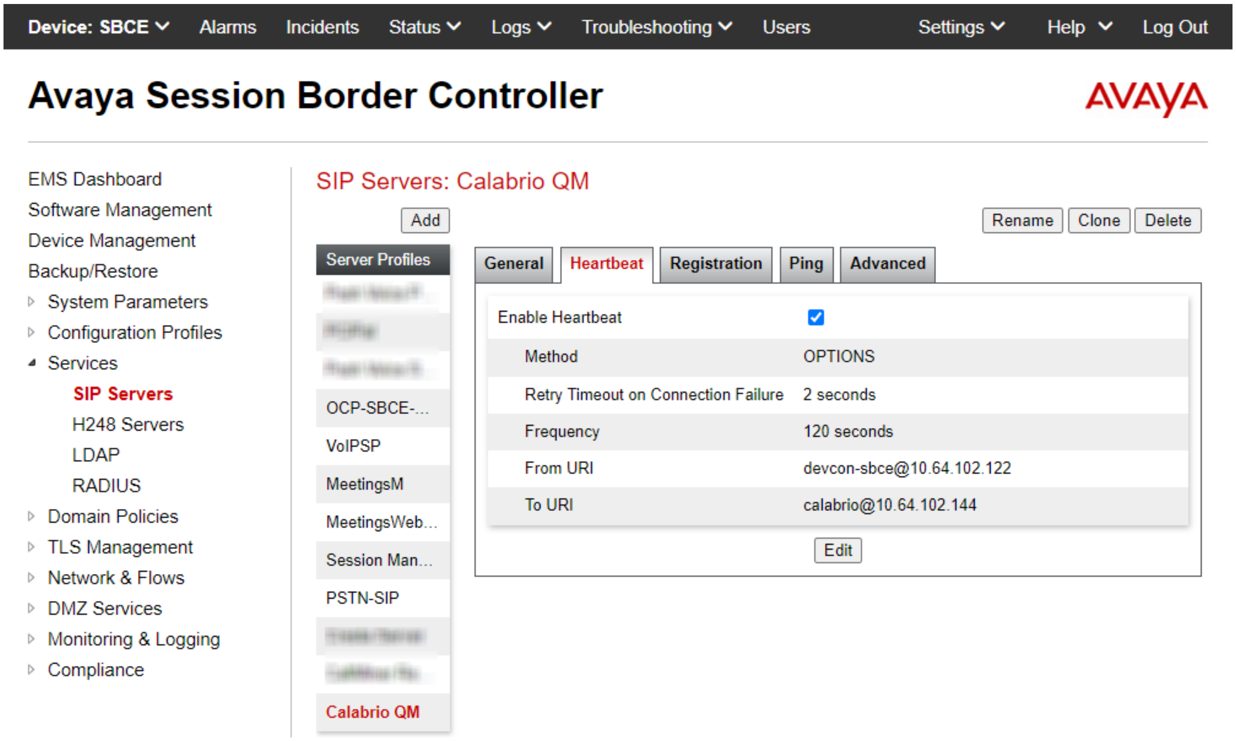


SIP Servers: Calabrio QM

Server Type	Recording Server
TLS Client Profile	sbceInternalA1
DNS Query Type	NONE/A
Inbound Connection Reuse Policy	None

IP Address / FQDN	Port	Transport	Whitelist
10.64.102.144	5061	TLS	□

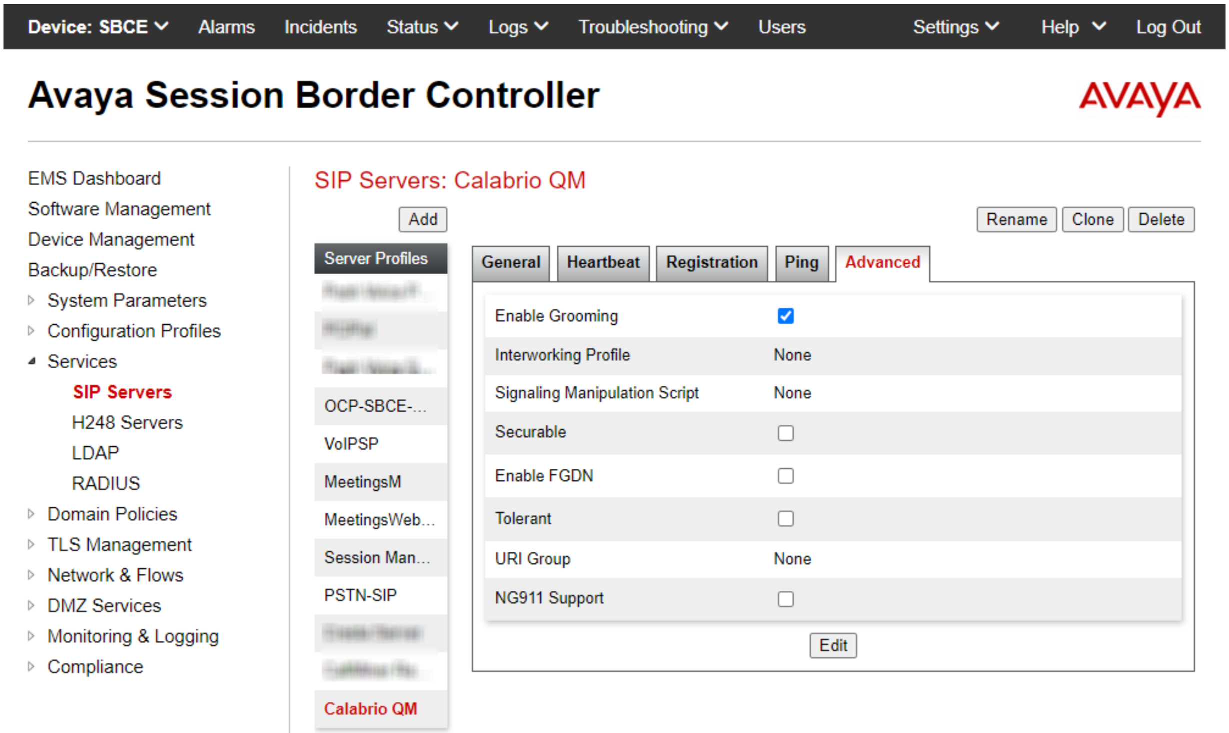
Select the **Heartbeat** tab and enable SBC to send SIP OPTIONS to Calabrio QM to track the status of the SIP trunk. Specify the frequency and appropriate URIs as shown below.



SIP Servers: Calabrio QM

Enable Heartbeat	☑
Method	OPTIONS
Retry Timeout on Connection Failure	2 seconds
Frequency	120 seconds
From URI	devcon-sbce@10.64.102.122
To URI	calabrio@10.64.102.144

The **Advanced** tab was configured with default settings as shown below.



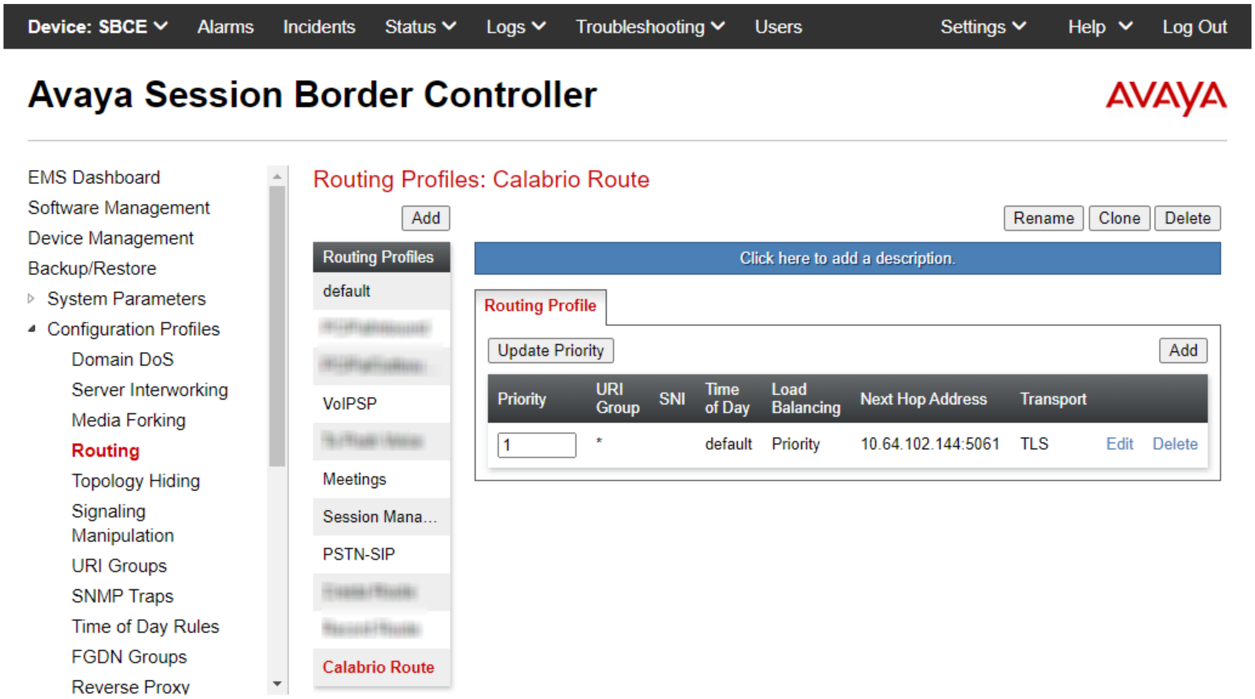
SIP Servers: Calabrio QM

Enable Grooming	☑
Interworking Profile	None
Signaling Manipulation Script	None
Securable	☐
Enable FGDN	☐
Tolerant	☐
URI Group	None
NG911 Support	☐

7.4. Administer Routing

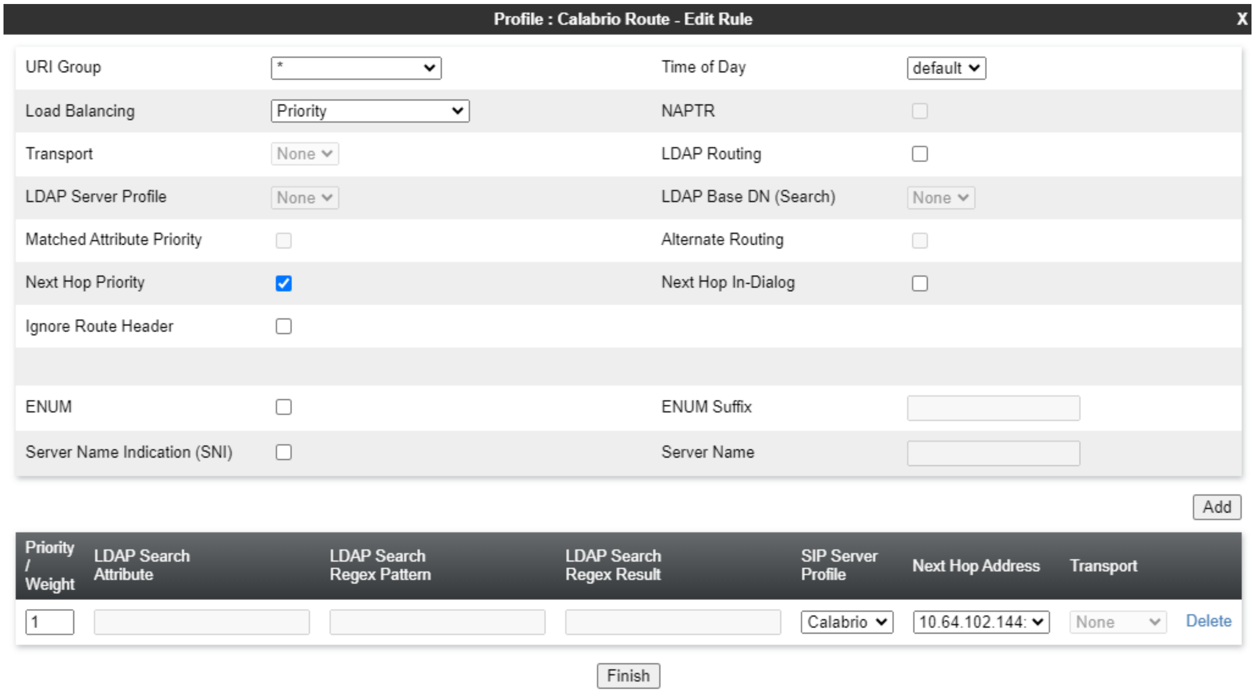
Navigate to **Configuration Profiles → Routing** to add a **Routing Profile** for routing SIP messages to Calabrio QM. Click **Add** to create a routing profile for Record.

The **Routing Profile** specifies the **Next Hop Address**, which was set to the Calabrio QM Data Server IP address, and the **Transport**, which was set to *TLS*, as shown below.



Priority	URI Group	SNI	Time of Day	Load Balancing	Next Hop Address	Transport		
1	*		default	Priority	10.64.102.144:5061	TLS	Edit	Delete

The details of the *Calabrio QM* routing profile are shown below with most fields left at default values. The **Priority/Weight** and **SIP Server Profile** were configured.



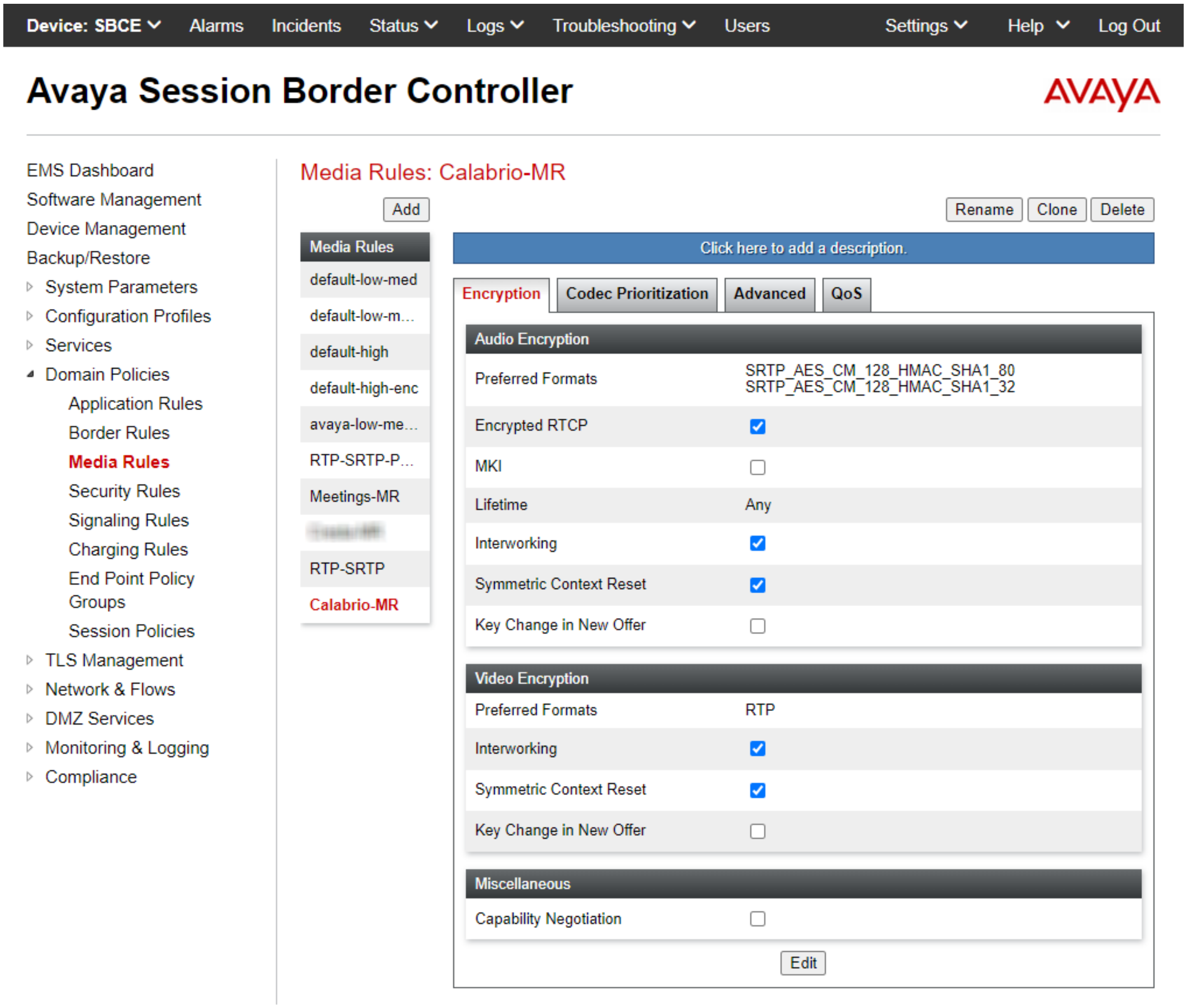
Profile : Calabrio Route - Edit Rule

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	□
Transport	None	LDAP Routing	□
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	□	Alternate Routing	□
Next Hop Priority	☑	Next Hop In-Dialog	□
Ignore Route Header	□		
ENUM	□	ENUM Suffix	
Server Name Indication (SNI)	□	Server Name	

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Calabrio	10.64.102.144:	None	Delete

7.5. Administer Media Rules

Navigate to **Domain Policies → Media Rules** to create a media rule for Calabrio QM Data Server. The **Encryption** tab was configured as shown below with SRTP ciphers allowed for the **Preferred Formats**. Encrypted RTCP may be enabled or disabled.



Media Rules: Calabrio-MR

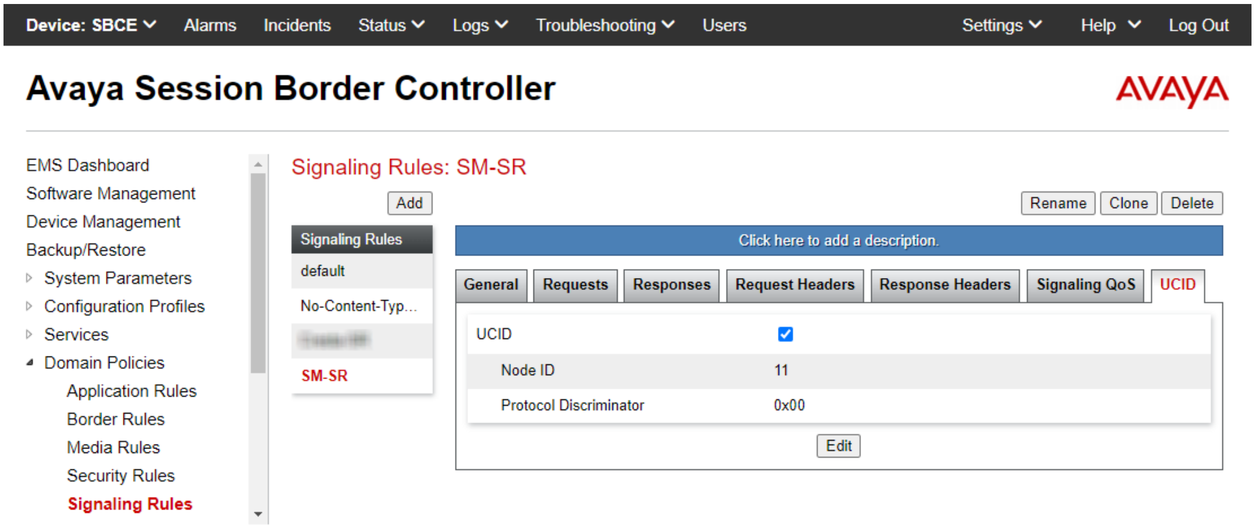
Audio Encryption	
Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 SRTP_AES_CM_128_HMAC_SHA1_32
Encrypted RTCP	☑
MKI	☐
Lifetime	Any
Interworking	☑
Symmetric Context Reset	☑
Key Change in New Offer	☐

Video Encryption	
Preferred Formats	RTP
Interworking	☑
Symmetric Context Reset	☑
Key Change in New Offer	☐

Miscellaneous	
Capability Negotiation	☐

7.6. Administer Signaling Rules

Navigate to **Domain Policies → Signaling Rules** to enable UCID on the signaling rule assigned to the Session Manager endpoint policy group. In the signaling rule, select the **UCID** tab and set the **Node ID** to a unique number (e.g., *11*). This specifies the UCID to send to Calabrio QM and Communication Manager for incoming calls from the PSTN (i.e., customer calls) to agents in the call center. This signaling rule will be assigned to the Session Manager **End Point Policy** in **Section 7.7.2**.



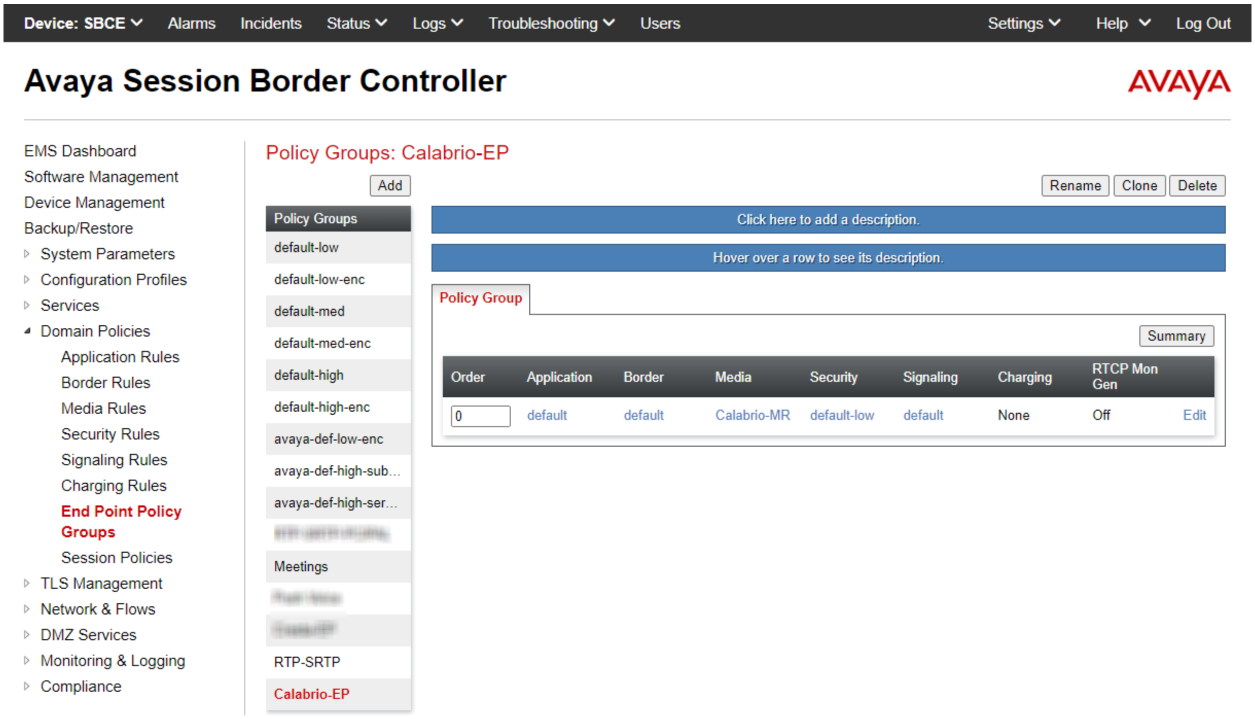
UCID	☑
Node ID	11
Protocol Discriminator	0x00

7.7. Administer End Point Policy Groups

An **Endpoint Policy Group** is a set of policies that will be applied to traffic between SBC and a connected server, such as Session Manager or Calabrio QM Data Server. End Point Policy Groups are assigned to **Server Flows** in **Section 7.11**.

7.7.1. Calabrio QM End Point Policy

Navigate to **Domain Policies → End Point Policy Groups** to create an end point policy group for Calabrio QM, which sets the media rule to one configured in **Section 7.5**



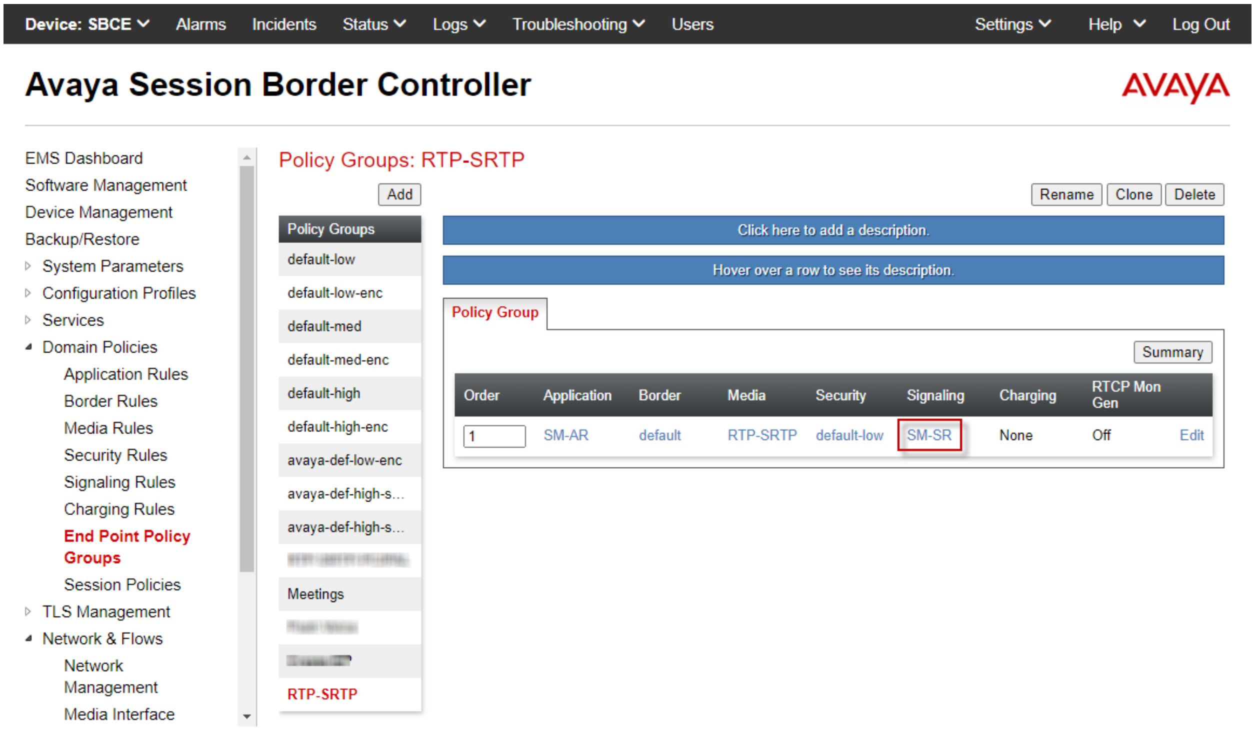
Policy Groups: Calabrio-EP

Policy Groups
- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- avaya-def-low-enc
- avaya-def-high-sub...
- avaya-def-high-ser...
- [redacted]
- Meetings
- [redacted]
- [redacted]
- RTP-SRTP
- Calabrio-EP

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
0	default	default	Calabrio-MR	default-low	default	None	Off	Edit

7.7.2. Session Manager End Point Policy

The Session Manager End Point Policy Group was configured as shown below. The signaling rule configured in **Section 7.6**, which specifies the UCID, was assigned to the end point policy group.



Policy Groups: RTP-SRTP

Policy Groups
default-low
default-low-enc
default-med
default-med-enc
default-high
default-high-enc
avaya-def-low-enc
avaya-def-high-s...
avaya-def-high-s...
[redacted]
Meetings
[redacted]
[redacted]
RTP-SRTP

Click here to add a description.

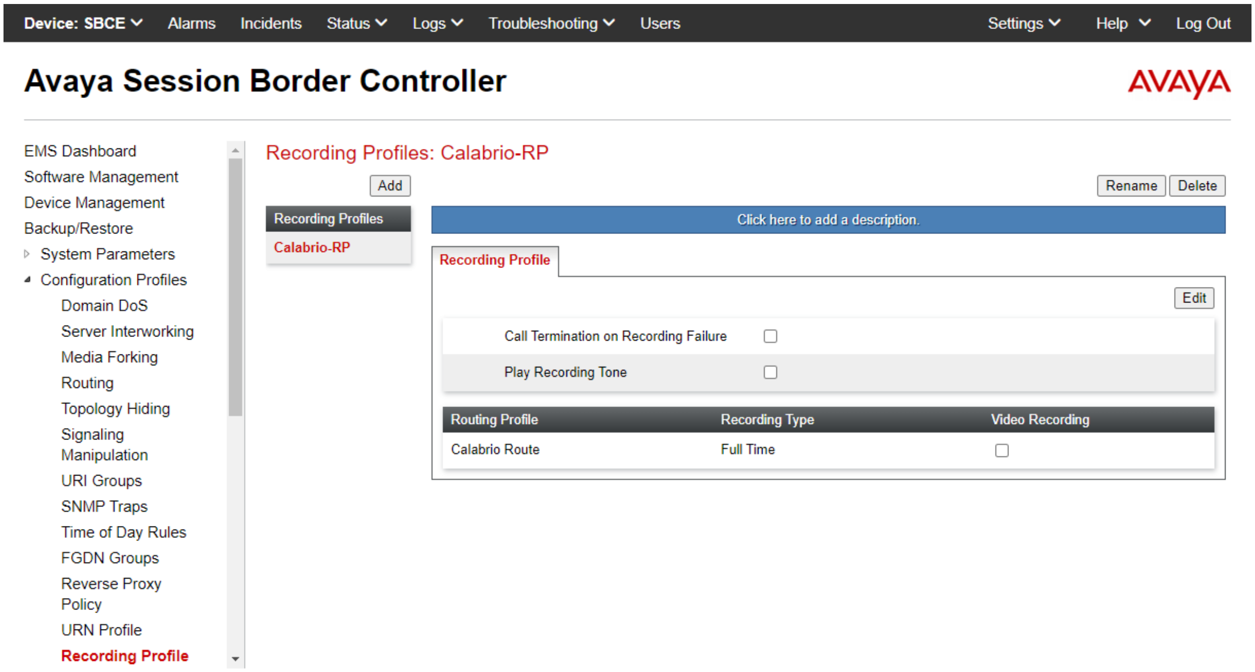
Hover over a row to see its description.

Policy Group

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
1	SM-AR	default	RTP-SRTP	default-low	SM-SR	None	Off	Edit

7.8. Administer Recording Profile

Navigate to **Configuration Profiles → Recording Profile**. Click **Add** to add a recoding profile for Calabrio QM. Set **Routing Profile** to the one configured in **Section 7.4** and **Recording Type** to *Full Time* as shown below.



Recording Profiles: Calabrio-RP

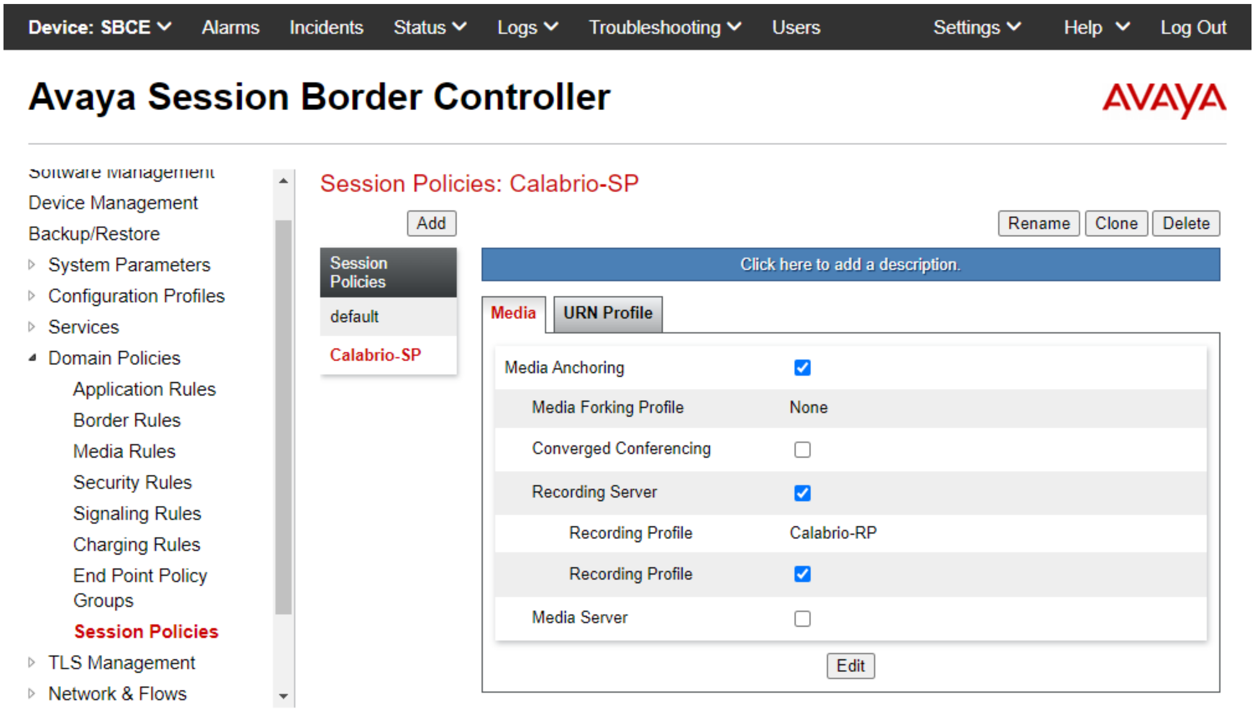
Call Termination on Recording Failure ☐

Play Recording Tone ☐

Routing Profile	Recording Type	Video Recording
Calabrio Route	Full Time	☐

7.9. Administer Session Policies

Navigate to **Domain Policies → Session Policies**. Click **Add** to create a session policy for Calabrio QM. Enable **Media Anchoring** and **Recording Server** and set **Recording Profile** to the one configured in **Section 7.8** as shown below.

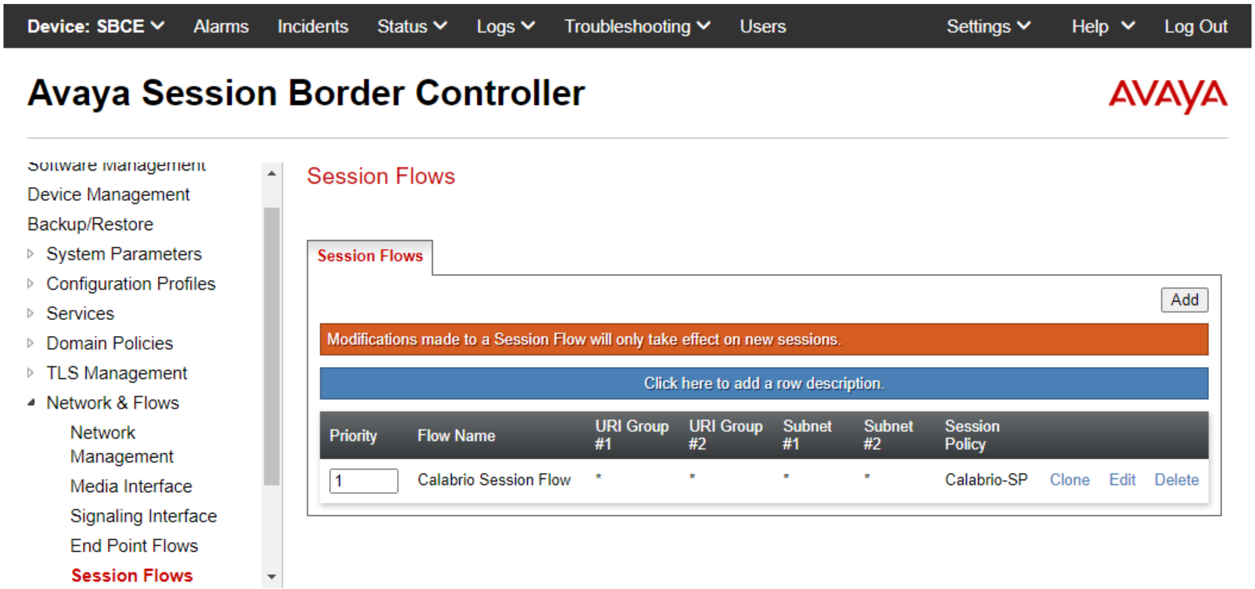


Session Policies: Calabrio-SP

Media Anchoring	☑
Media Forking Profile	None
Converged Conferencing	□
Recording Server	☑
Recording Profile	Calabrio-RP
Recording Profile	☑
Media Server	□

7.10. Administer Session Flows

Navigate to **Network & Flows → Session Flows**. Click **Add** to create a session flow for Calabrio QM. Set the **Flow Name** to a desired name and the **Session Policy** to the one configured in **Section 7.9** as shown below. Default values for all other fields were used. Since the wildcard (*) was used for the subnet fields, this session flow would apply to all SIP sessions.

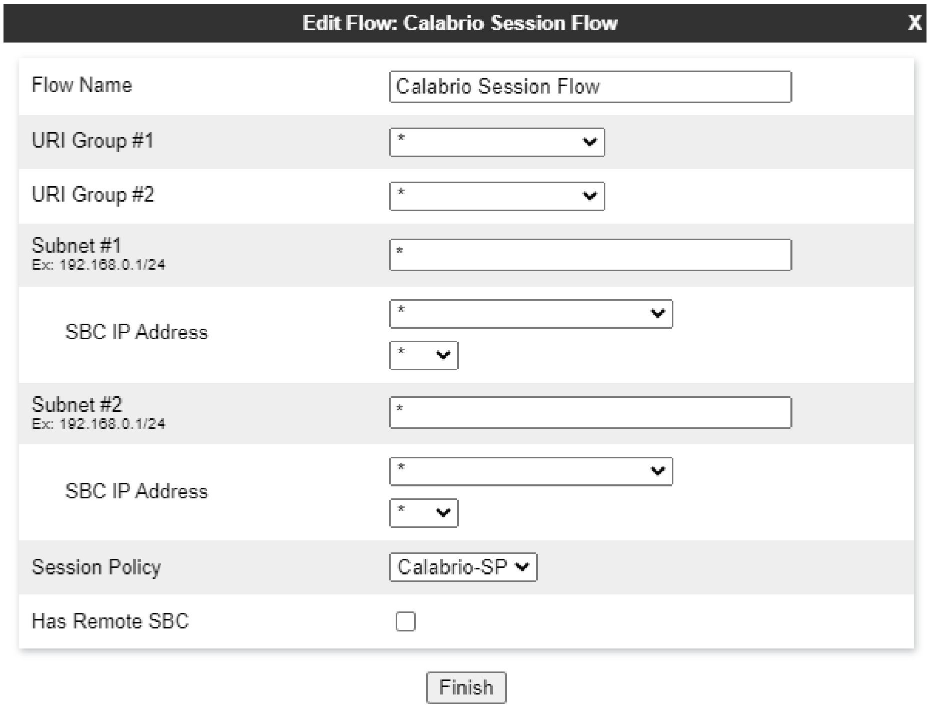


Modifications made to a Session Flow will only take effect on new sessions.

Click here to add a row description.

Priority	Flow Name	URI Group #1	URI Group #2	Subnet #1	Subnet #2	Session Policy			
1	Calabrio Session Flow	*	*	*	*	Calabrio-SP	Clone	Edit	Delete

The details of the Calabrio QM Session Flow are shown below.

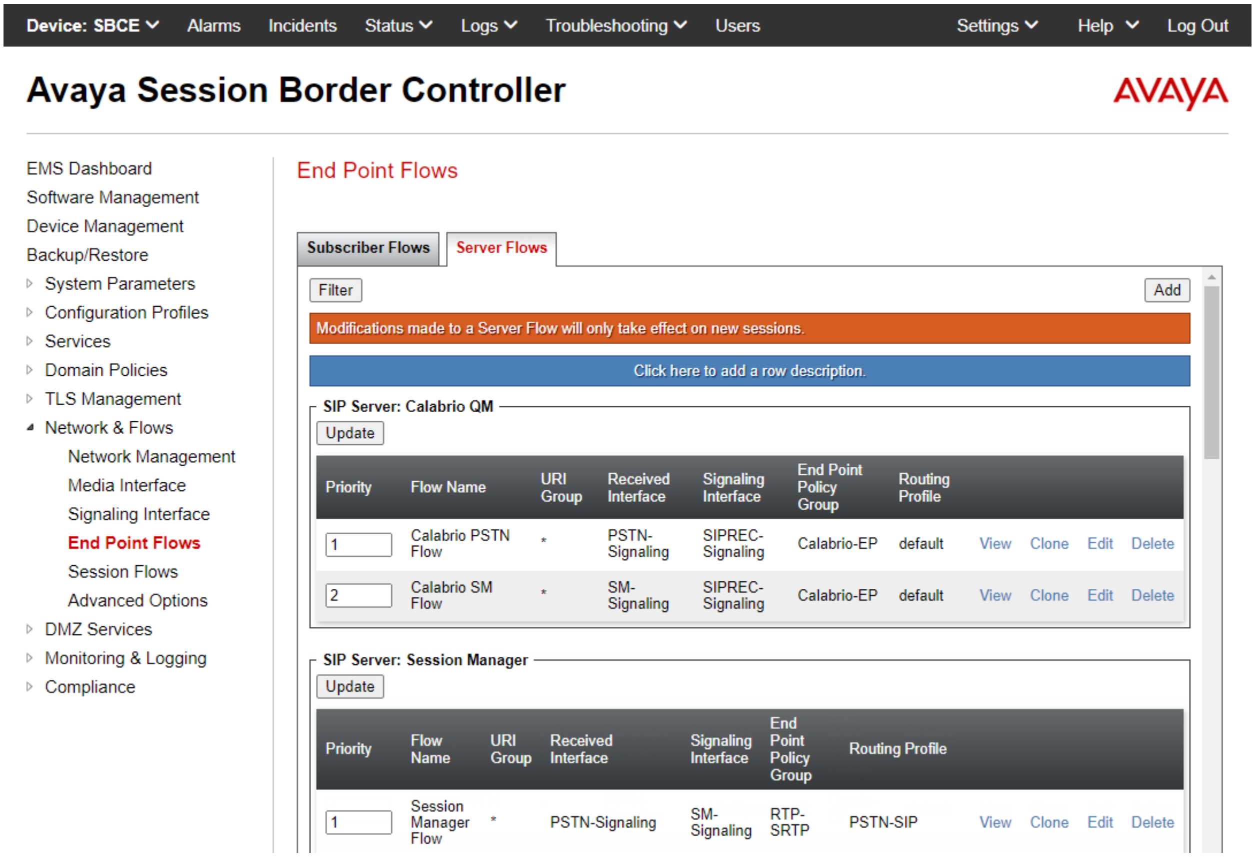


Flow Name	Calabrio Session Flow
URI Group #1	*
URI Group #2	*
Subnet #1 Ex: 192.168.0.1/24	*
SBC IP Address	* *
Subnet #2 Ex: 192.168.0.1/24	*
SBC IP Address	* *
Session Policy	Calabrio-SP
Has Remote SBC	□

7.11. Administer Server Flows

Navigate to **Network & Flows → End Point Flows** and select the **Server Flows** tab. The configured **Server Flows** used in the compliance test are shown below.

For Calabrio QM, two server flows were configured to allow SIP messages to be sent between Avaya SBC and Calabrio QM in both directions. For Session Manager, an existing server flow was modified with an end point policy group, configured in **Section 7.7.2**, that was assigned the signaling rule, configured in **Section 7.6**, that includes a unique UCID Node ID. The PSTN server flow is not shown below because no changes were required. The following sub-sections shows the configuration of the Calabrio QM and Session Manager server flows in more detail.



Modifications made to a Server Flow will only take effect on new sessions.

SIP Server: Calabrio QM

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Calabrio PSTN Flow	*	PSTN-Signaling	SIPREC-Signaling	Calabrio-EP	default	View	Clone	Edit	Delete
2	Calabrio SM Flow	*	SM-Signaling	SIPREC-Signaling	Calabrio-EP	default	View	Clone	Edit	Delete

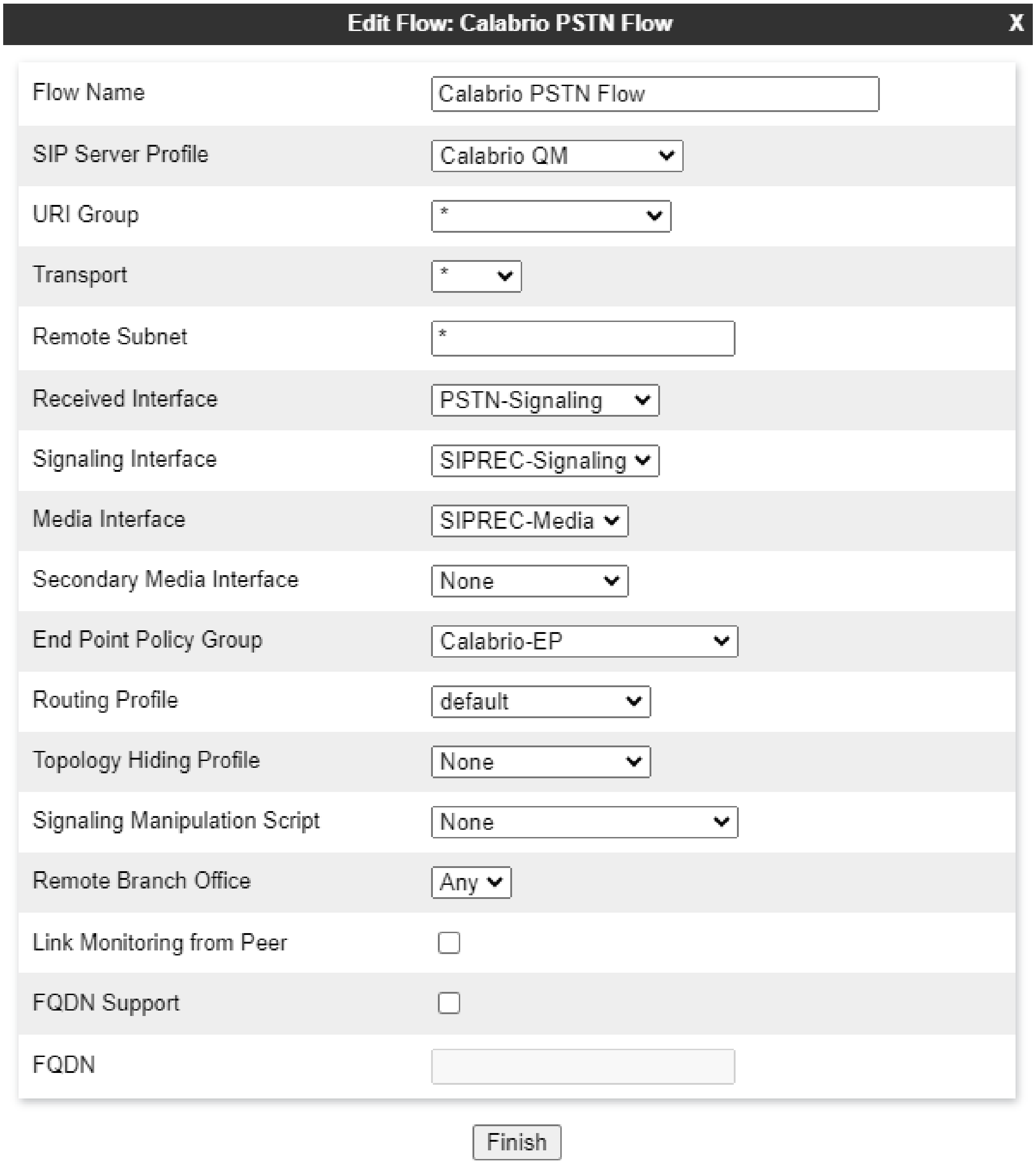
SIP Server: Session Manager

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Session Manager Flow	*	PSTN-Signaling	SM-Signaling	RTP-SRTP	PSTN-SIP	View	Clone	Edit	Delete

7.11.1. Calabrio QM Server Flows

In the compliance test, two server flows were created for Calabrio QM: *Calabrio PSTN Flow* and *Calabrio SM Flow*. *Calabrio PSTN Flow* is used for sending SIP messages from PSTN to Calabrio QM and *Calabrio SM Flow* is used for sending SIP messages from Session Manager to Calabrio QM. Note that the **End Point Policy Group** is set to the one configured in **Section 7.7.1**. A media and signaling interface were configured for Calabario QM with TLS enabled and the appropriate TLS Server Profile assigned to each interface (not shown).

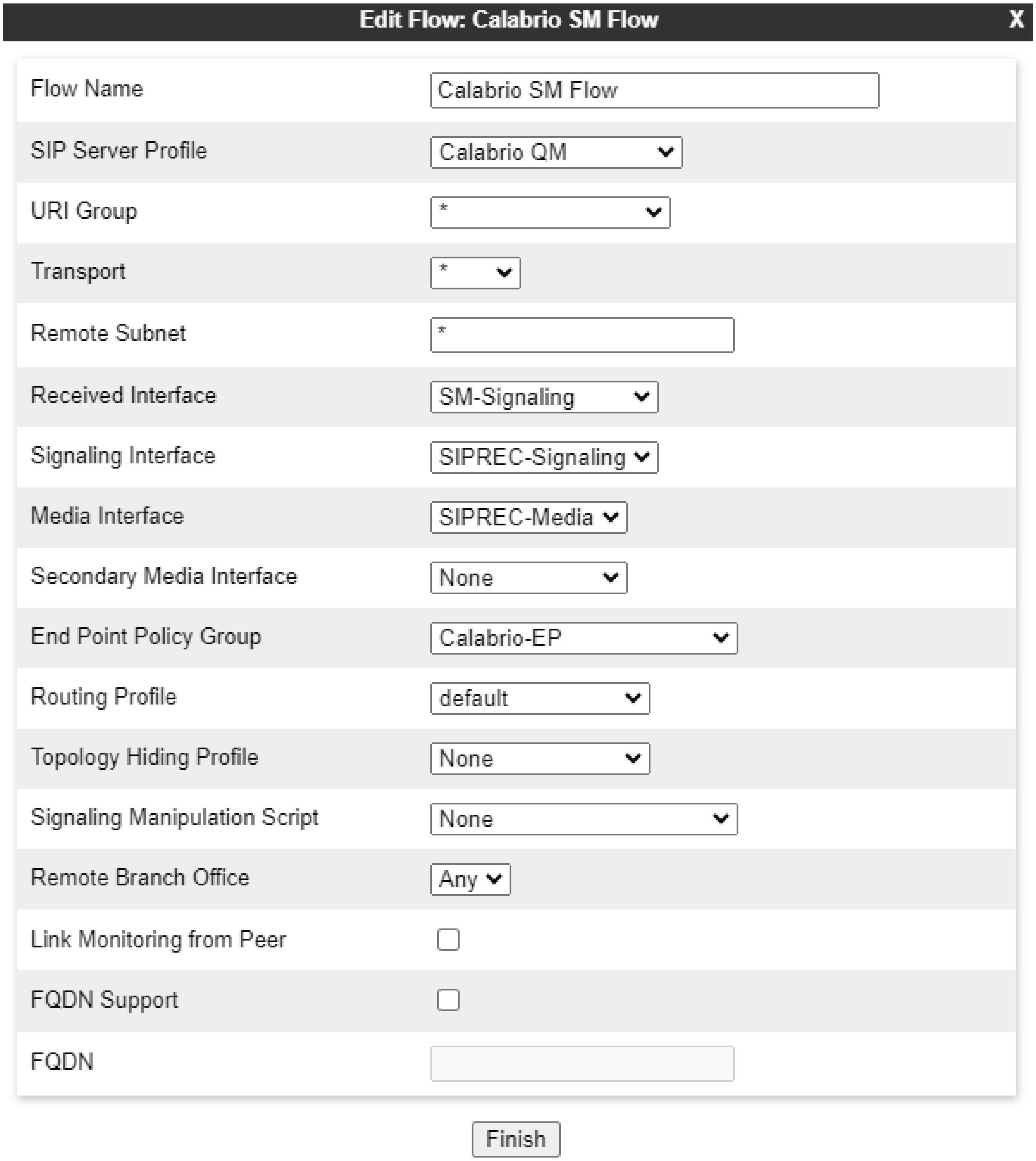
The *Calabrio PSTN Flow* is shown below.



Edit Flow: Calabrio PSTN Flow

Flow Name	Calabrio PSTN Flow
SIP Server Profile	Calabrio QM
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	PSTN-Signaling
Signaling Interface	SIPREC-Signaling
Media Interface	SIPREC-Media
Secondary Media Interface	None
End Point Policy Group	Calabrio-EP
Routing Profile	default
Topology Hiding Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	☐
FQDN Support	☐
FQDN	

The *Calabrio SM Flow* is shown below.

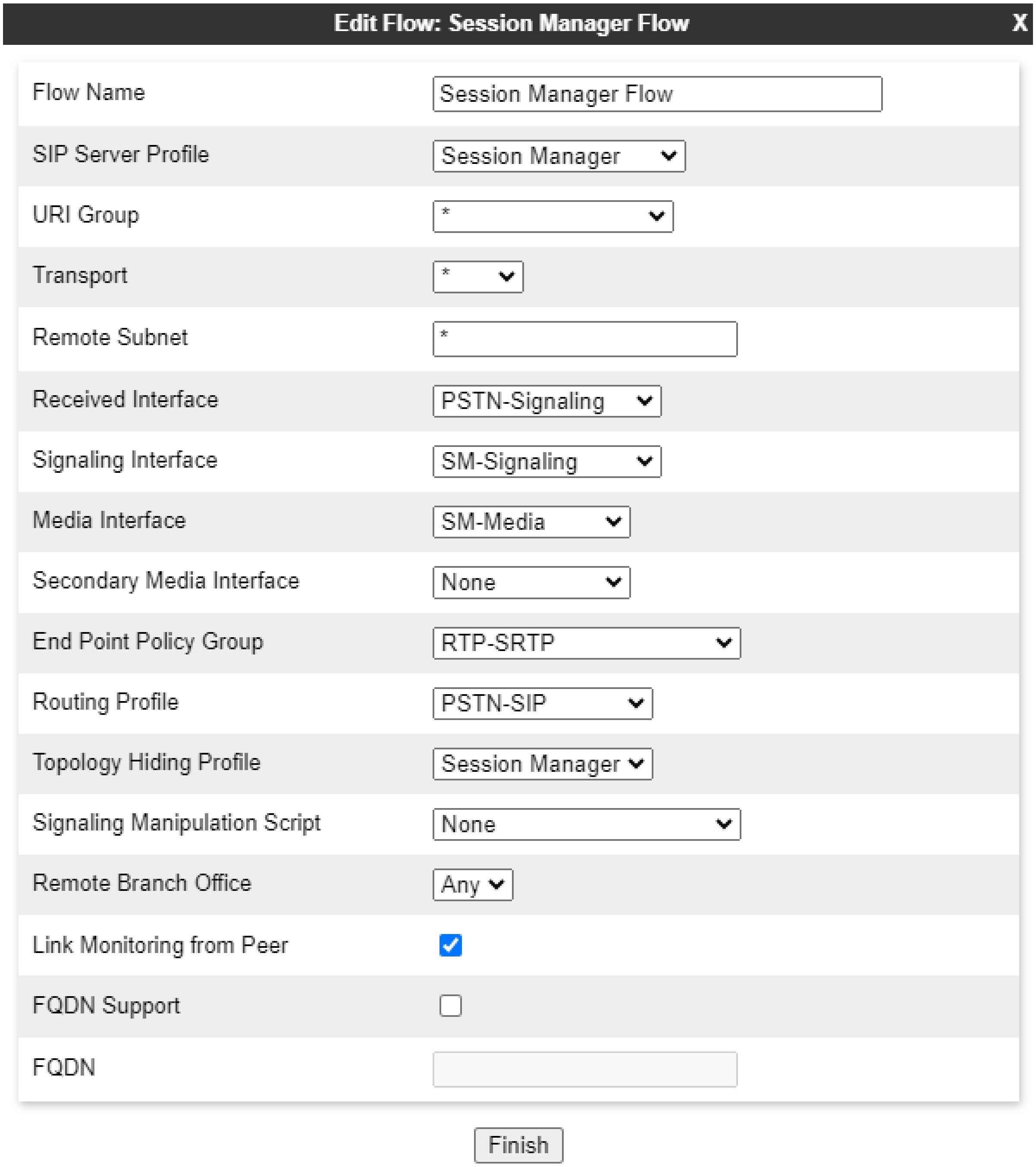


Edit Flow: Calabrio SM Flow

Flow Name	Calabrio SM Flow
SIP Server Profile	Calabrio QM
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	SM-Signaling
Signaling Interface	SIPREC-Signaling
Media Interface	SIPREC-Media
Secondary Media Interface	None
End Point Policy Group	Calabrio-EP
Routing Profile	default
Topology Hiding Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	□
FQDN Support	□
FQDN	

7.11.2. Server Flows for Session Manager

In the compliance test, one server flow was used for Session Manager: *Session Manager Flow*. *Session Manager Flow* is used for sending SIP messages between PSTN and Session Manager. Note that the **End Point Policy Group** is set to the one configured in **Section 7.7.2**.



Flow Name	Session Manager Flow
SIP Server Profile	Session Manager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	PSTN-Signaling
Signaling Interface	SM-Signaling
Media Interface	SM-Media
Secondary Media Interface	None
End Point Policy Group	RTP-SRTP
Routing Profile	PSTN-SIP
Topology Hiding Profile	Session Manager
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	☑
FQDN Support	☐
FQDN	

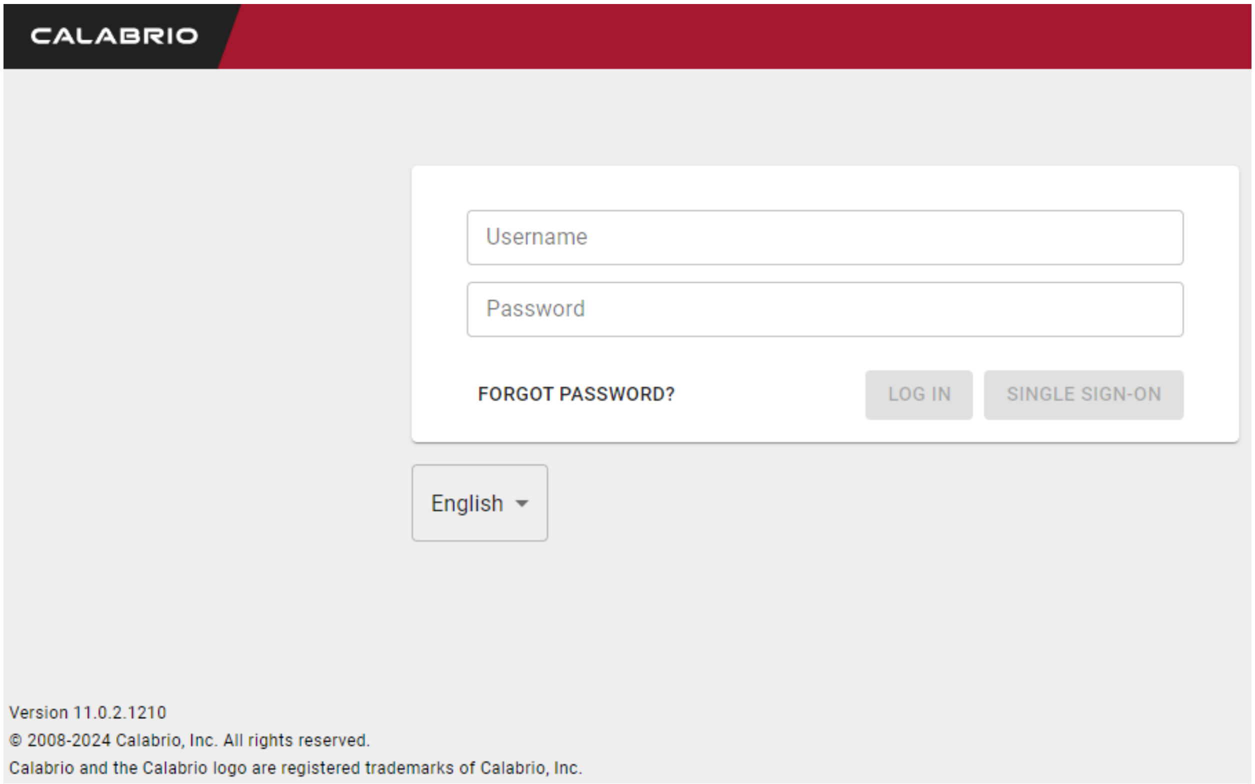
8. Configure Calabrio Quality Management

This section covers the configuration of Calabrio QM to support SMS on Application Enablement Services to retrieve station extensions, CDR used in the reconciliation process, and call recording using Avaya SBC SIPREC. This requires the following steps:

- Launch Calabrio Cloud Portal
- Administer ACD Configuration
- Administer Data Server Configuration
- Administer Telephony Groups
- Install TLS Certificates for Secure SIP Trunk to Avaya SBC
- Administer Users
- Administer Device Associations
- Restart Services

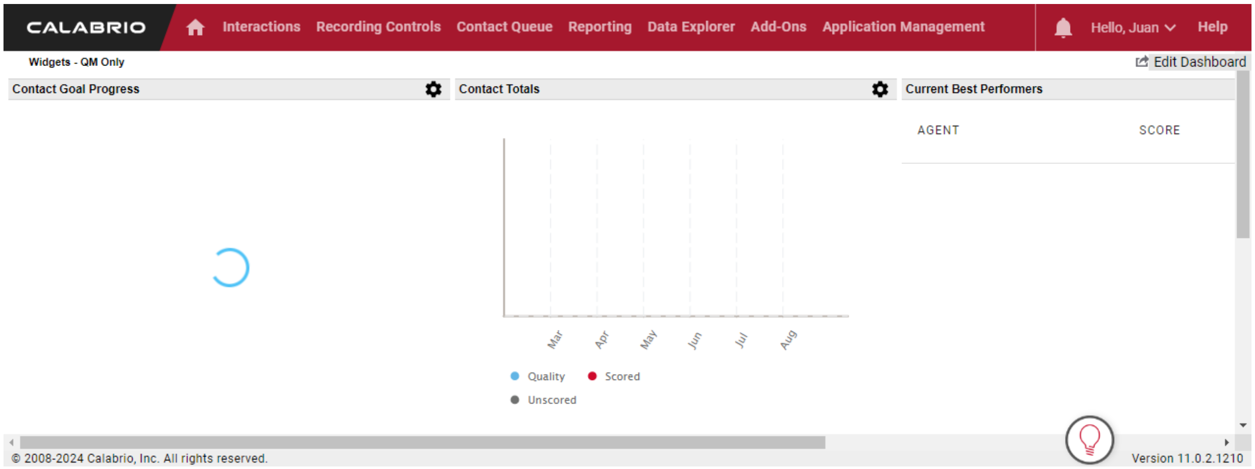
8.1. Launch Calabrio Cloud Portal

Access the Calabrio Cloud Portal by using the URL **Error! Hyperlink reference not valid.** in a web browser, where *<FQDN>* is the IP address of the Calabrio QM application server in the cloud. Log in using the appropriate credentials.



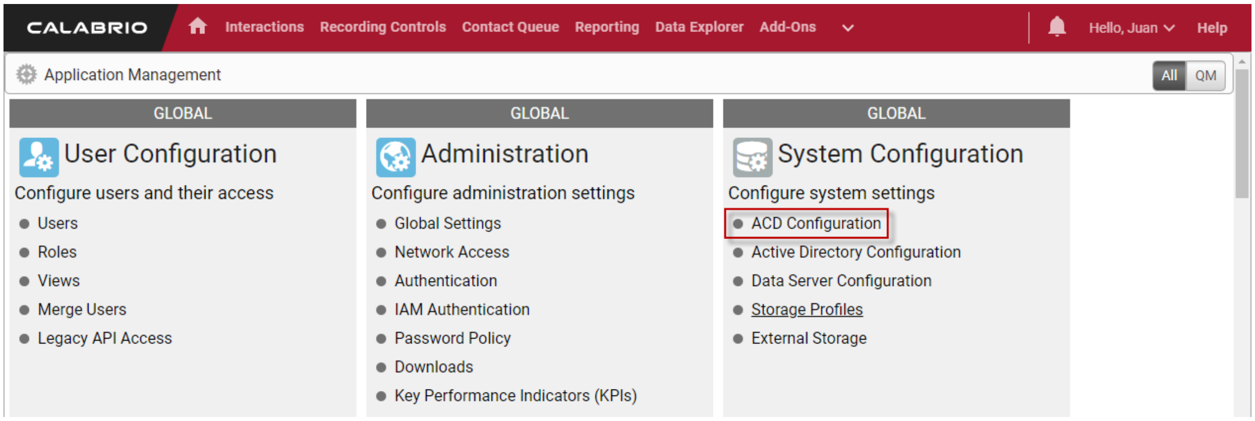
Version 11.0.2.1210
© 2008-2024 Calabrio, Inc. All rights reserved.
Calabrio and the Calabrio logo are registered trademarks of Calabrio, Inc.

The portal home page is displayed as shown below. The Calabrio QM configuration in this section is covered under **Application Management** as shown in the menu bar below.

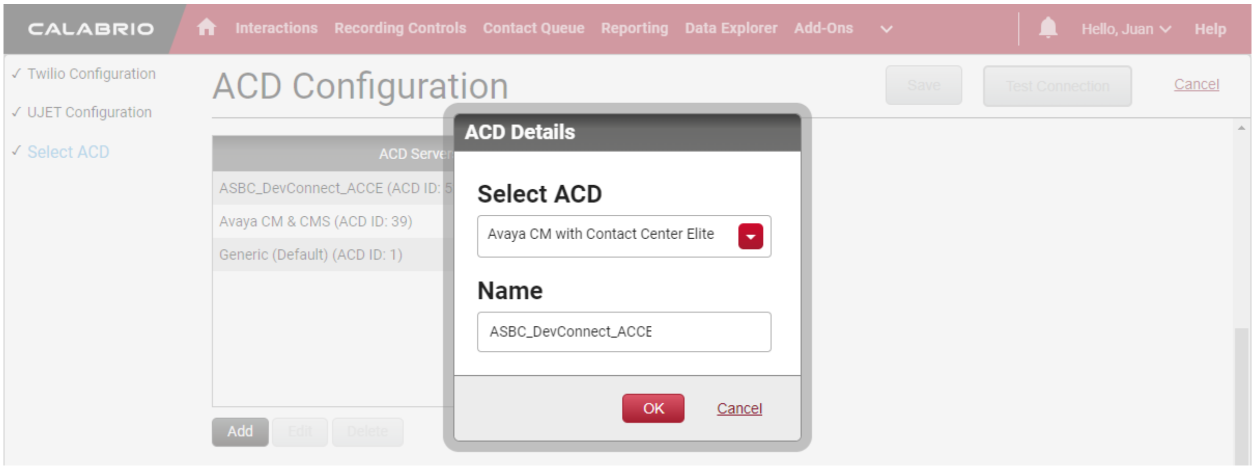


8.2. Administer ACD Configuration

Navigate to **Application Management** to display the page below. Click on **ACD Configuration** under **System Configuration**. In the **ACD Configuration** page, SMS information and CDR are configured.



In the **ACD Configuration** page, click the **Add** button to add an ACD. In the ACD Details dialog box, select *Avaya CM with Contact Center Elite* and specify an ACD name (e.g., *ASBC_DevConnect_ACCE*). Click **OK**.



ACD Configuration

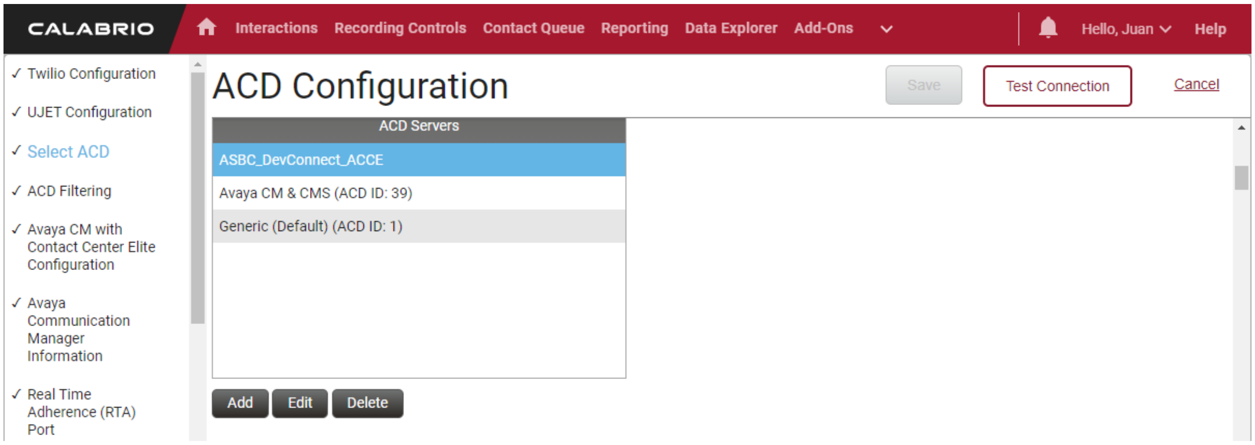
ACD Serve
ASBC_DevConnect_ACCE (ACD ID: 5
Avaya CM & CMS (ACD ID: 39)
Generic (Default) (ACD ID: 1)

ACD Details

Select ACD: Avaya CM with Contact Center Elite

Name: ASBC_DevConnect_ACCE

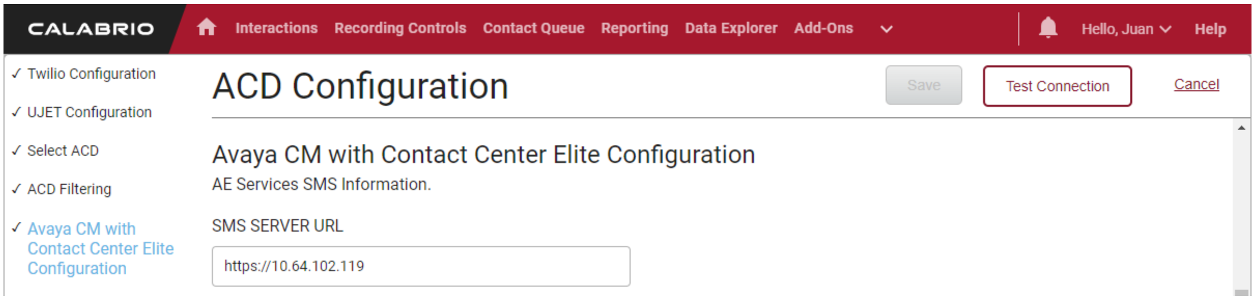
The ACD is added in the **ACD Servers** section as shown below.



ACD Configuration

ACD Servers
ASBC_DevConnect_ACCE
Avaya CM & CMS (ACD ID: 39)
Generic (Default) (ACD ID: 1)

In the **ACD Configuration** page, click on **Avaya CM with Contact Center Elite Configuration** in the left pane and to configure SMS information. Set **SMS SERVER URL** to https://**Error! Hyperlink reference not valid.**>, where <*AES-IP-Address*> is the Application Enablement Services IP address (e.g., *10.64.102.119*).



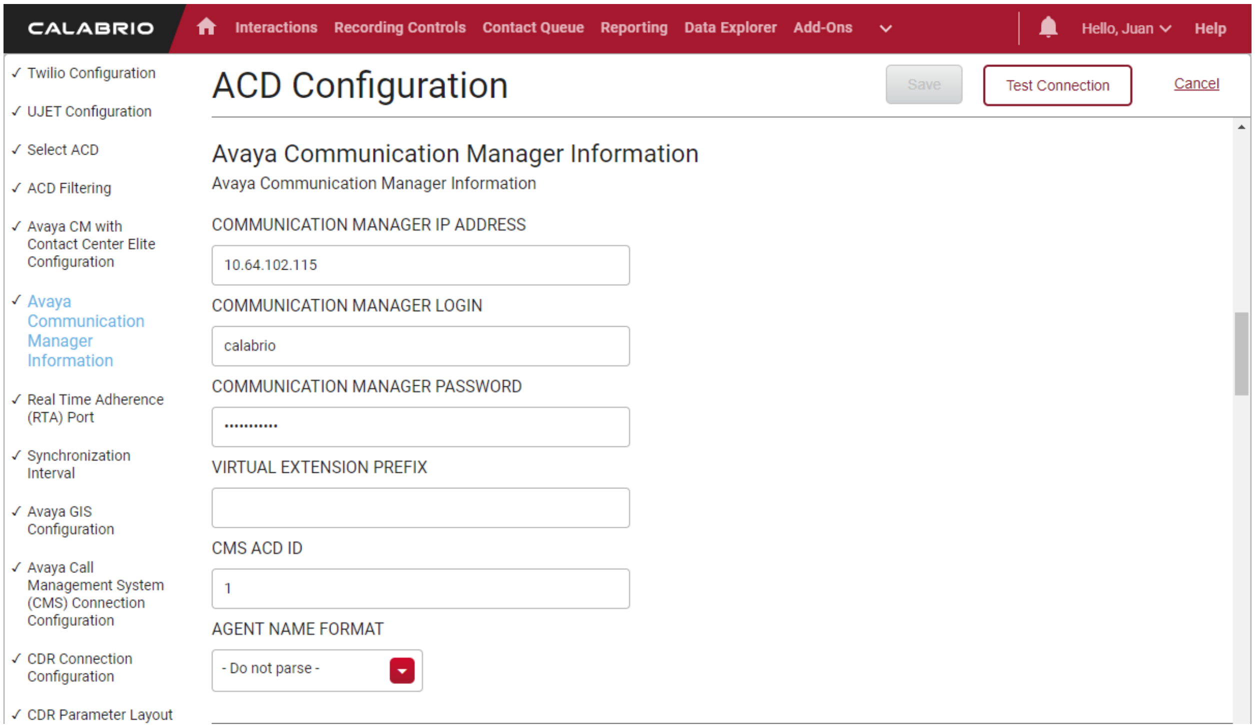
ACD Configuration

Avaya CM with Contact Center Elite Configuration

AE Services SMS Information.

SMS SERVER URL: https://10.64.102.119

Click on **Avaya Communication Manager Information** in the left pane to configure the SAT login credentials configured in **Section 5.2.2**, including the Communication Manager IP address, login name, and password. SMS will use this SAT login to retrieve capacity and station information from Communication Manager.


CALABRIO
Interactions
Recording Controls
Contact Queue
Reporting
Data Explorer
Add-Ons
Hello, Juan
Help
✓ Twilio Configuration
✓ UJET Configuration
✓ Select ACD
✓ ACD Filtering
✓ Avaya CM with Contact Center Elite Configuration
✓ Avaya Communication Manager Information
✓ Real Time Adherence (RTA) Port
✓ Synchronization Interval
✓ Avaya GIS Configuration
✓ Avaya Call Management System (CMS) Connection Configuration
✓ CDR Connection Configuration
✓ CDR Parameter Layout
Save
Test Connection
Cancel

ACD Configuration

Avaya Communication Manager Information

Avaya Communication Manager Information

COMMUNICATION MANAGER IP ADDRESS: 10.64.102.115

COMMUNICATION MANAGER LOGIN: calabrio

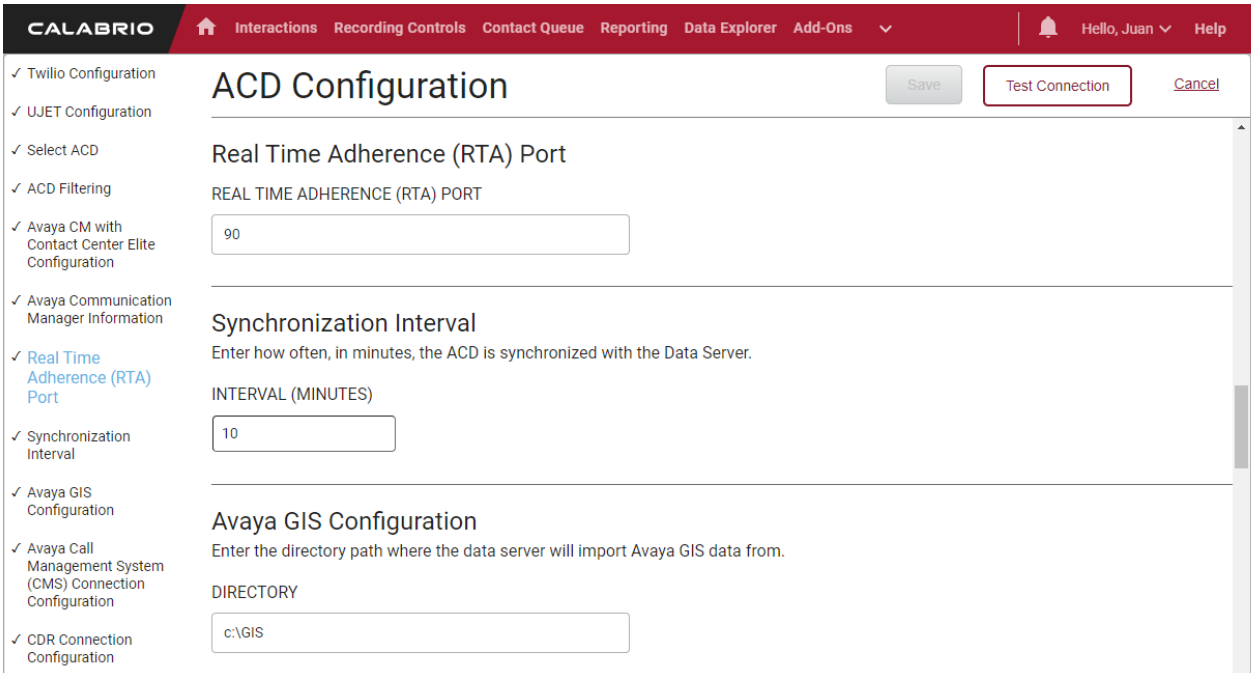
COMMUNICATION MANAGER PASSWORD: ....

VIRTUAL EXTENSION PREFIX:

CMS ACD ID: 1

AGENT NAME FORMAT: - Do not parse -

Scroll down to the **Synchronization Interval** section to specify how often to synchronize the station information in the Calabrio QM Data Server. In the example below, **INTERVAL (MINUTES)** was set to *10*.


CALABRIO
Interactions
Recording Controls
Contact Queue
Reporting
Data Explorer
Add-Ons
Hello, Juan
Help
✓ Twilio Configuration
✓ UJET Configuration
✓ Select ACD
✓ ACD Filtering
✓ Avaya CM with Contact Center Elite Configuration
✓ Avaya Communication Manager Information
✓ Real Time Adherence (RTA) Port
✓ Synchronization Interval
✓ Avaya GIS Configuration
✓ Avaya Call Management System (CMS) Connection Configuration
✓ CDR Connection Configuration
Save
Test Connection
Cancel

ACD Configuration

Real Time Adherence (RTA) Port

REAL TIME ADHERENCE (RTA) PORT: 90

Synchronization Interval

Enter how often, in minutes, the ACD is synchronized with the Data Server.

INTERVAL (MINUTES): 10

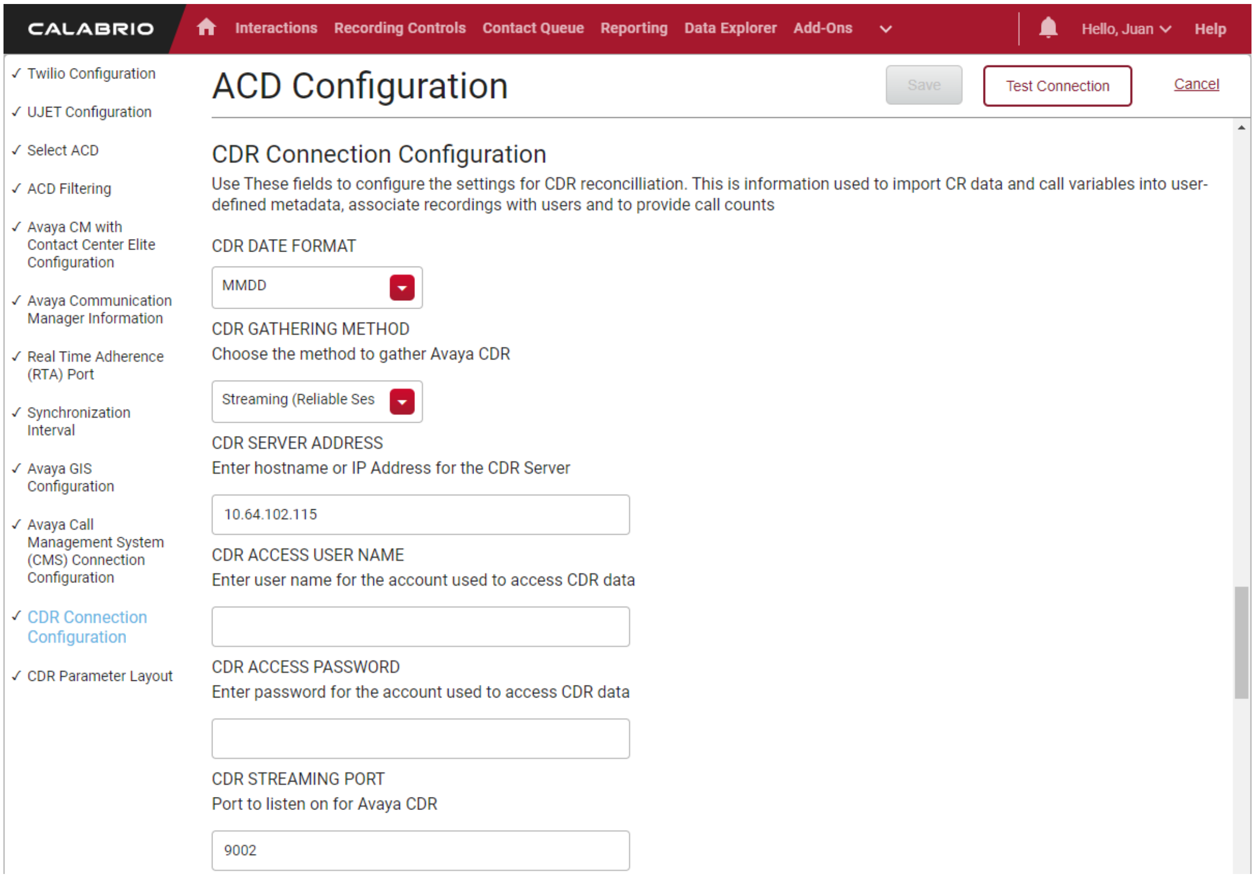
Avaya GIS Configuration

Enter the directory path where the data server will import Avaya GIS data from.

DIRECTORY: c:\GIS

Click **CDR Connection Configuration** in the left pane to set up the CDR link to Communication Manager. Set the following parameters as follows:

- **CDR DATE FORMAT:** Set to *MMDD* for the date format specified in **Section 5.3.3**.
- **CDR GATHERING METHOD:** Set to *Streaming (Reliable Session Protocol).*
- **CDR SERVER ADDRESS:** Set to Communication Manager IP address (e.g., *10.64.102.115*).
- **CDR STREAMING PORT:** Set to port *9002* as specified in **Section 5.3.3**.


CALABRIO
Interactions
Recording Controls
Contact Queue
Reporting
Data Explorer
Add-Ons
Hello, Juan
Help
✓ Twilio Configuration
✓ UJET Configuration
✓ Select ACD
✓ ACD Filtering
✓ Avaya CM with Contact Center Elite Configuration
✓ Avaya Communication Manager Information
✓ Real Time Adherence (RTA) Port
✓ Synchronization Interval
✓ Avaya GIS Configuration
✓ Avaya Call Management System (CMS) Connection Configuration
✓ CDR Connection Configuration
✓ CDR Parameter Layout
Save
Test Connection
Cancel

ACD Configuration

CDR Connection Configuration

Use These fields to configure the settings for CDR reconcilliation. This is information used to import CR data and call variables into user-defined metadata, associate recordings with users and to provide call counts

CDR DATE FORMAT

MMDD

CDR GATHERING METHOD

Choose the method to gather Avaya CDR

Streaming (Reliable Ses

CDR SERVER ADDRESS

Enter hostname or IP Address for the CDR Server

10.64.102.115

CDR ACCESS USER NAME

Enter user name for the account used to access CDR data

CDR ACCESS PASSWORD

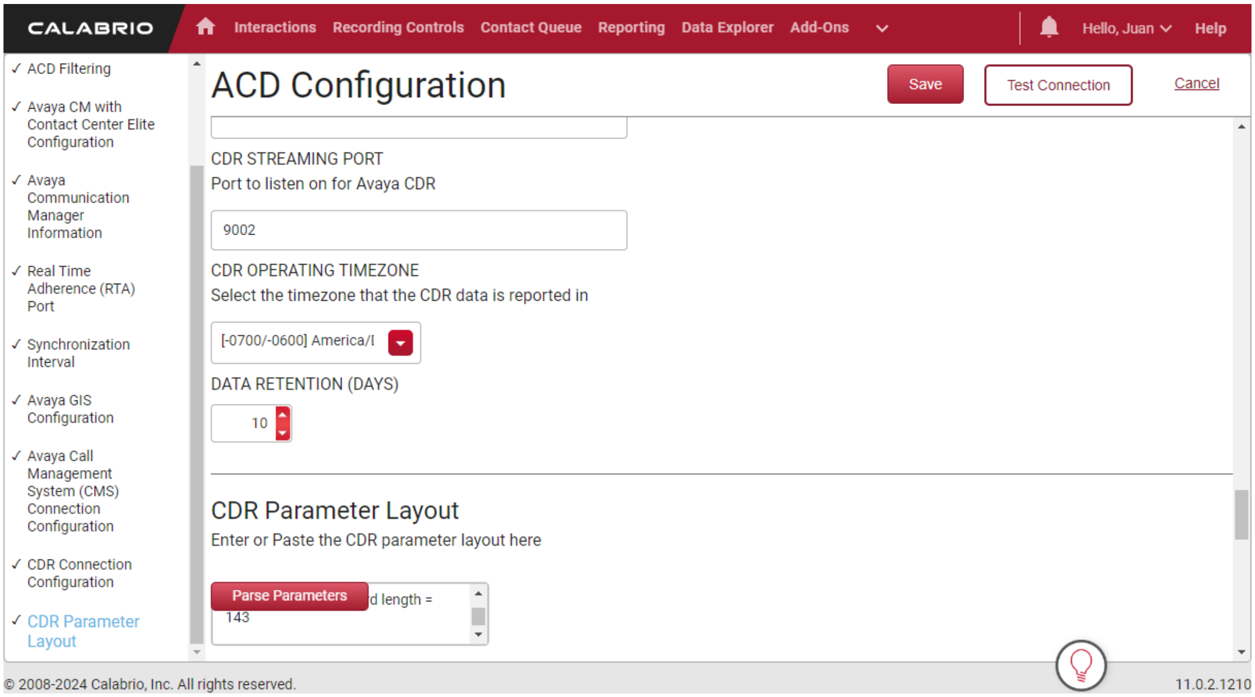
Enter password for the account used to access CDR data

CDR STREAMING PORT

Port to listen on for Avaya CDR

9002

Click on **CDR Parameter Layout** in the left pane to configure the CDR record format. Copy the CDR record format on page 2 of the **system-parameters cdr** form shown in **Section 5.3.3** and paste it in the **Parse Parameters** field as shown below. Click **Parse Parameters**.



CALABRIO
Interactions
Recording Controls
Contact Queue
Reporting
Data Explorer
Add-Ons
Hello, Juan
Help
✓ ACD Filtering
✓ Avaya CM with Contact Center Elite Configuration
✓ Avaya Communication Manager Information
✓ Real Time Adherence (RTA) Port
✓ Synchronization Interval
✓ Avaya GIS Configuration
✓ Avaya Call Management System (CMS) Connection Configuration
✓ CDR Connection Configuration
✓ CDR Parameter Layout
Save
Test Connection
Cancel
Parse Parameters
© 2008-2024 Calabrio, Inc. All rights reserved.
11.0.2.1210

ACD Configuration

CDR STREAMING PORT
Port to listen on for Avaya CDR

9002

CDR OPERATING TIMEZONE
Select the timezone that the CDR data is reported in

[-0700/-0600] America/I

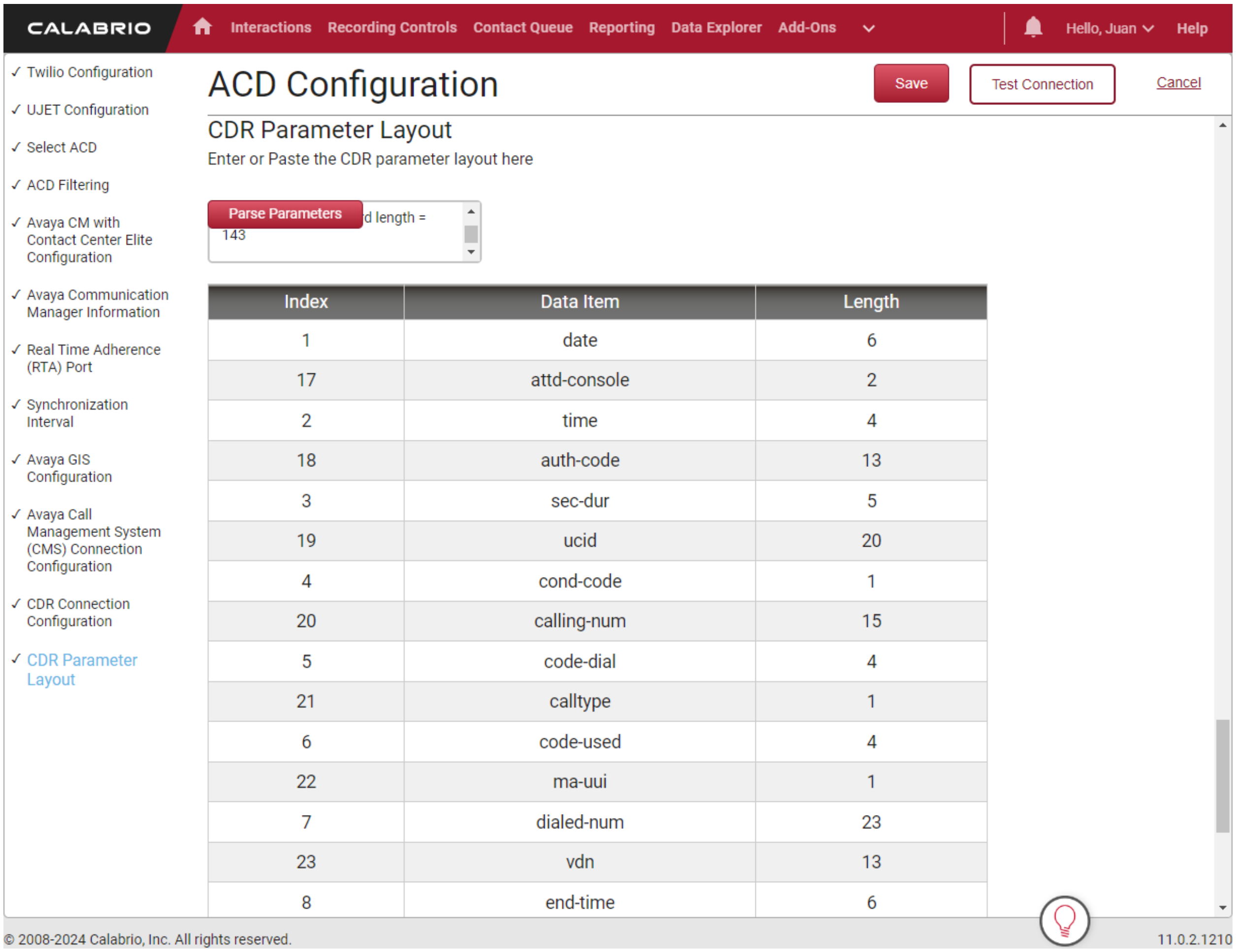
DATA RETENTION (DAYS)

10

CDR Parameter Layout
Enter or Paste the CDR parameter layout here

d length =
143

The CDR record format is displayed in the table shown below. This should match the CDR record format on page 2 of the **system-parameters cdr** form shown in **Section 5.3.3.**


CALABRIO
Interactions
Recording Controls
Contact Queue
Reporting
Data Explorer
Add-Ons
Hello, Juan
Help
✓ Twilio Configuration
✓ UJET Configuration
✓ Select ACD
✓ ACD Filtering
✓ Avaya CM with Contact Center Elite Configuration
✓ Avaya Communication Manager Information
✓ Real Time Adherence (RTA) Port
✓ Synchronization Interval
✓ Avaya GIS Configuration
✓ Avaya Call Management System (CMS) Connection Configuration
✓ CDR Connection Configuration
✓ CDR Parameter Layout
Save
Test Connection
Cancel
Parse Parameters
© 2008-2024 Calabrio, Inc. All rights reserved.
11.0.2.1210

ACD Configuration

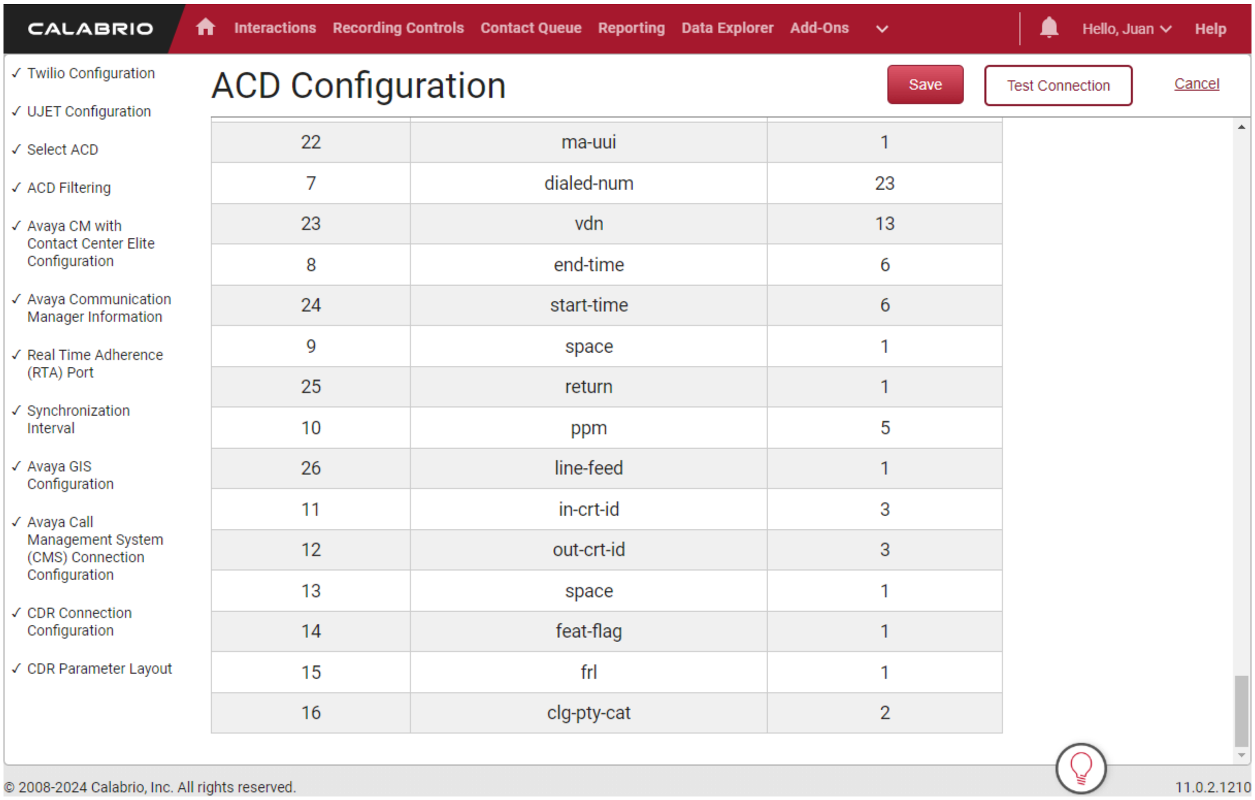
CDR Parameter Layout

Enter or Paste the CDR parameter layout here

d length =
143

Index	Data Item	Length
1	date	6
17	attd-console	2
2	time	4
18	auth-code	13
3	sec-dur	5
19	ucid	20
4	cond-code	1
20	calling-num	15
5	code-dial	4
21	calltype	1
6	code-used	4
22	ma-uui	1
7	dialed-num	23
23	vdn	13
8	end-time	6

The CDR record format is continued below. Click **Save**.

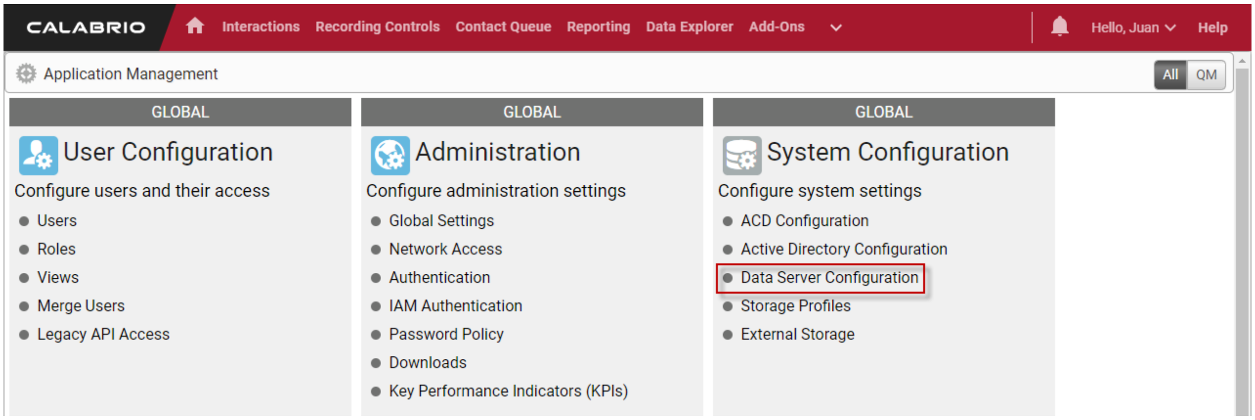

CALABRIO
Interactions
Recording Controls
Contact Queue
Reporting
Data Explorer
Add-Ons
Hello, Juan
Help
✓ Twilio Configuration
✓ UJET Configuration
✓ Select ACD
✓ ACD Filtering
✓ Avaya CM with Contact Center Elite Configuration
✓ Avaya Communication Manager Information
✓ Real Time Adherence (RTA) Port
✓ Synchronization Interval
✓ Avaya GIS Configuration
✓ Avaya Call Management System (CMS) Connection Configuration
✓ CDR Connection Configuration
✓ CDR Parameter Layout
Save
Test Connection
Cancel
© 2008-2024 Calabrio, Inc. All rights reserved.
11.0.2.1210

ACD Configuration

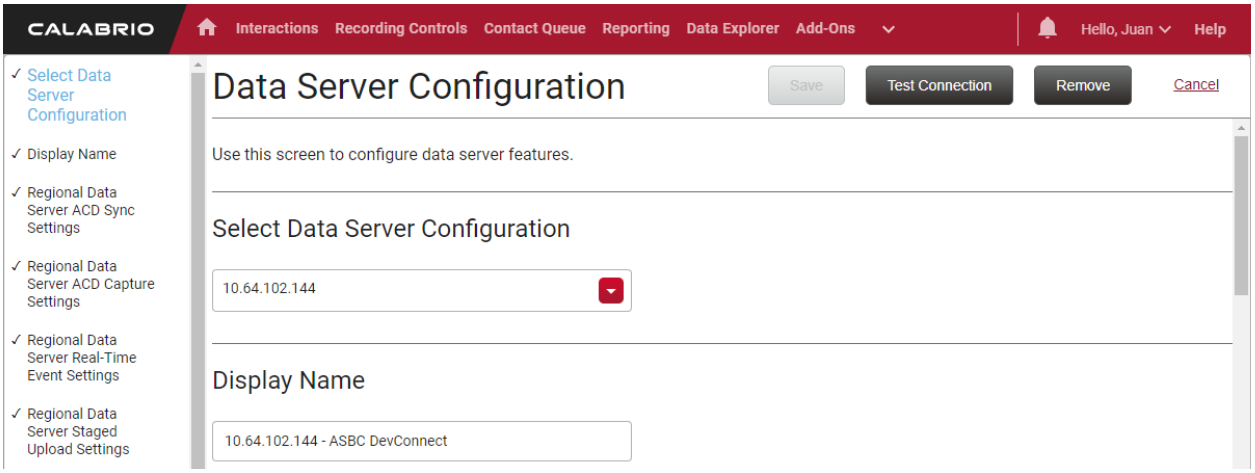
22	ma-uui	1
7	dialed-num	23
23	vdn	13
8	end-time	6
24	start-time	6
9	space	1
25	return	1
10	ppm	5
26	line-feed	1
11	in-crt-id	3
12	out-crt-id	3
13	space	1
14	feat-flag	1
15	frl	1
16	clg-pty-cat	2

8.3. Administer Data Server Configuration

Navigate to **Application Management** to display the page below. Click on **Data Server Configuration** under **System Configuration**. The SIPREC settings are configured in the **Data Server Configuration** page. For the compliance test, a single Data Server was used; hence all the relevant roles were assigned to a single server.



In the **Data Server Configuration** page, select the IP address of the Calabrio QM Data Server (e.g., *10.64.102.144*) from the drop-down field as shown below. The IP address becomes available after the Calabrio QM Data Server software is installed. Specify the **Display Name** (e.g., *10.64.102.144 – ASBC DevConnect*).


CALABRIO
Interactions
Recording Controls
Contact Queue
Reporting
Data Explorer
Add-Ons
Hello, Juan
Help
✓ Select Data Server Configuration
✓ Display Name
✓ Regional Data Server ACD Sync Settings
✓ Regional Data Server ACD Capture Settings
✓ Regional Data Server Real-Time Event Settings
✓ Regional Data Server Staged Upload Settings
Save
Test Connection
Remove
Cancel

Data Server Configuration

Use this screen to configure data server features.

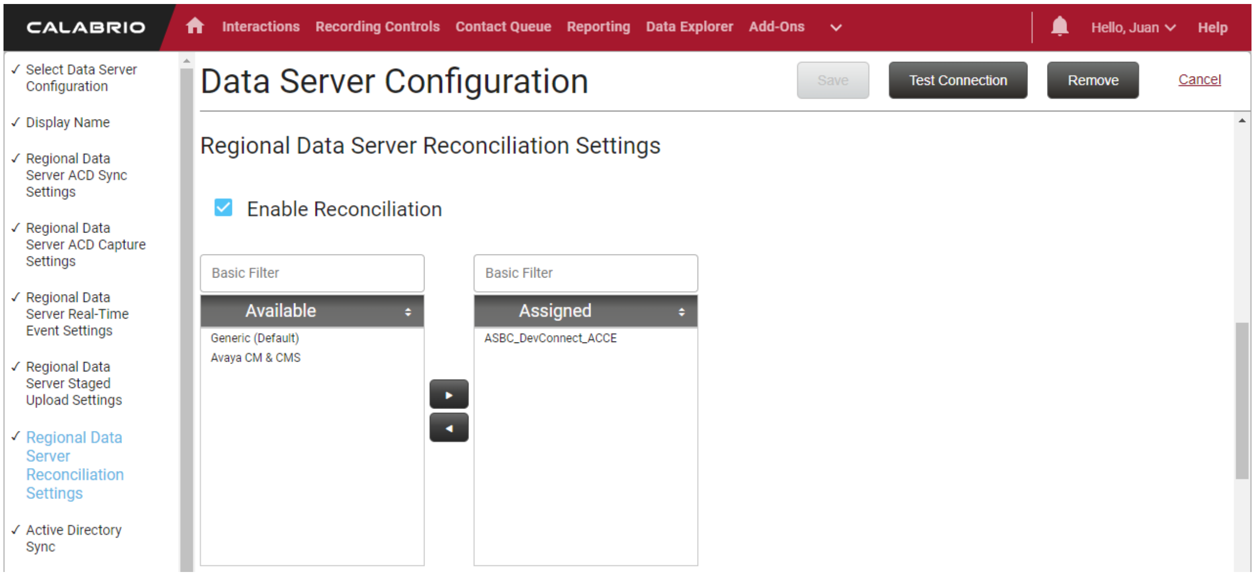
Select Data Server Configuration

10.64.102.144

Display Name

10.64.102.144 - ASBC DevConnect

Click on **Regional Data Server Reconciliation Settings** in the left pane, enable reconciliation and select the ACD configured in **Section 8.2** as shown below.


CALABRIO
Interactions
Recording Controls
Contact Queue
Reporting
Data Explorer
Add-Ons
Hello, Juan
Help
✓ Select Data Server Configuration
✓ Display Name
✓ Regional Data Server ACD Sync Settings
✓ Regional Data Server ACD Capture Settings
✓ Regional Data Server Real-Time Event Settings
✓ Regional Data Server Staged Upload Settings
✓ Regional Data Server Reconciliation Settings
✓ Active Directory Sync
Save
Test Connection
Remove
Cancel
Basic Filter
Available
Assigned

Data Server Configuration

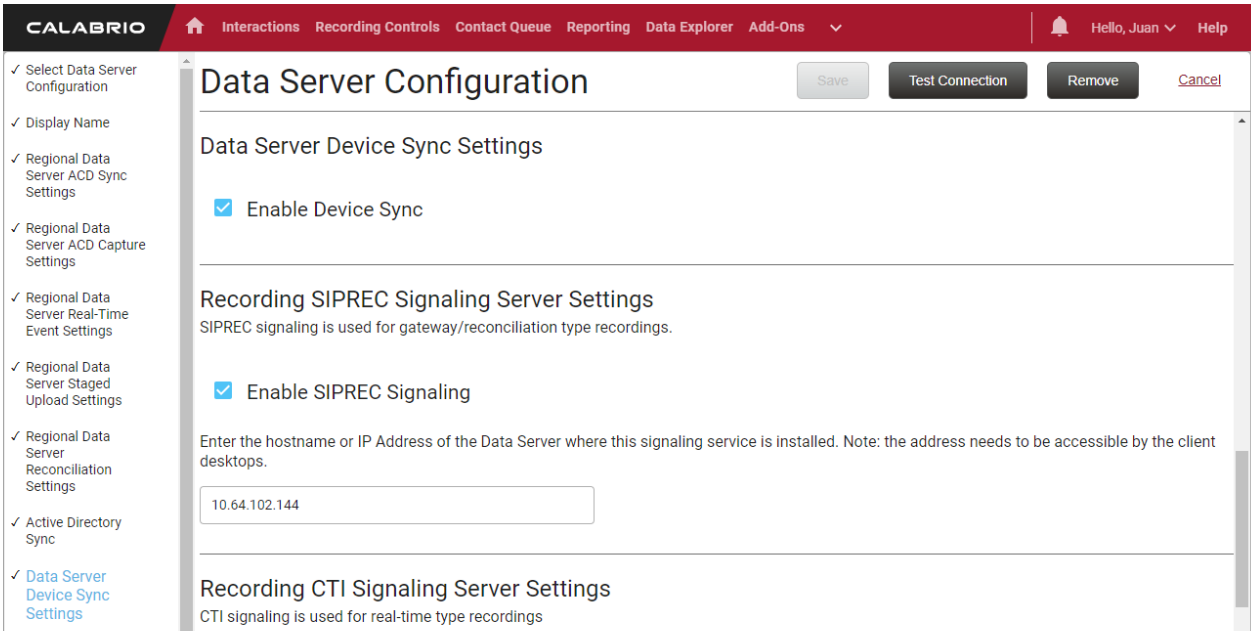
Regional Data Server Reconciliation Settings

☑ Enable Reconciliation

Available: Generic (Default), Avaya CM & CMS

Assigned: ASBC_DevConnect_ACCE

Click on **Data Server Device Sync Settings** in the left pane. **Enable Device Sync** and **SIPREC Signaling** and set the Calabrio QM Data Server IP address (e.g., *10.64.102.144*).


CALABRIO
Interactions
Recording Controls
Contact Queue
Reporting
Data Explorer
Add-Ons
Hello, Juan
Help
✓ Select Data Server Configuration
✓ Display Name
✓ Regional Data Server ACD Sync Settings
✓ Regional Data Server ACD Capture Settings
✓ Regional Data Server Real-Time Event Settings
✓ Regional Data Server Staged Upload Settings
✓ Regional Data Server Reconciliation Settings
✓ Active Directory Sync
✓ Data Server Device Sync Settings
Save
Test Connection
Remove
Cancel

Data Server Configuration

Data Server Device Sync Settings

☑ Enable Device Sync

Recording SIPREC Signaling Server Settings

SIPREC signaling is used for gateway/reconciliation type recordings.

☑ Enable SIPREC Signaling

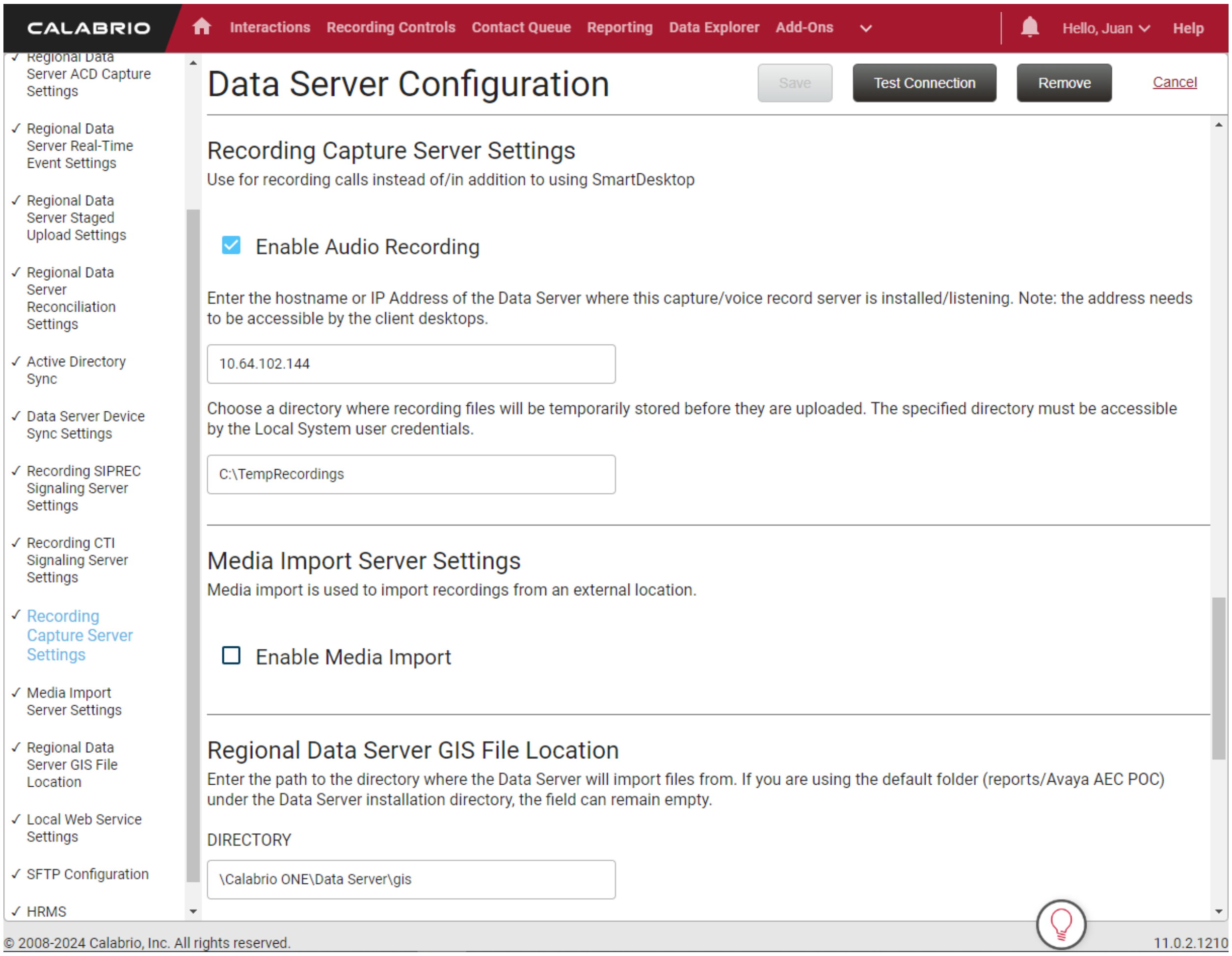
Enter the hostname or IP Address of the Data Server where this signaling service is installed. Note: the address needs to be accessible by the client desktops.

10.64.102.144

Recording CTI Signaling Server Settings

CTI signaling is used for real-time type recordings

Click on **Recording Capture Server Settings** in the left pane. **Enable Audio Recording**, set the Calabrio QM Data Server IP address (e.g., *10.64.102.144*), and set the directory for storing recordings temporarily (e.g., *C:\TempRecordings*).


CALABRIO
Interactions
Recording Controls
Contact Queue
Reporting
Data Explorer
Add-Ons
Hello, Juan
Help
✓ Regional Data Server ACD Capture Settings
✓ Regional Data Server Real-Time Event Settings
✓ Regional Data Server Staged Upload Settings
✓ Regional Data Server Reconciliation Settings
✓ Active Directory Sync
✓ Data Server Device Sync Settings
✓ Recording SIPREC Signaling Server Settings
✓ Recording CTI Signaling Server Settings
✓ Recording Capture Server Settings
✓ Media Import Server Settings
✓ Regional Data Server GIS File Location
✓ Local Web Service Settings
✓ SFTP Configuration
✓ HRMS
Save
Test Connection
Remove
Cancel

Data Server Configuration

Recording Capture Server Settings

Use for recording calls instead of/in addition to using SmartDesktop

☑ Enable Audio Recording

Enter the hostname or IP Address of the Data Server where this capture/voice record server is installed/listening. Note: the address needs to be accessible by the client desktops.

10.64.102.144

Choose a directory where recording files will be temporarily stored before they are uploaded. The specified directory must be accessible by the Local System user credentials.

C:\TempRecordings

Media Import Server Settings

Media import is used to import recordings from an external location.

☐ Enable Media Import

Regional Data Server GIS File Location

Enter the path to the directory where the Data Server will import files from. If you are using the default folder (reports/Avaya AEC POC) under the Data Server installation directory, the field can remain empty.

DIRECTORY

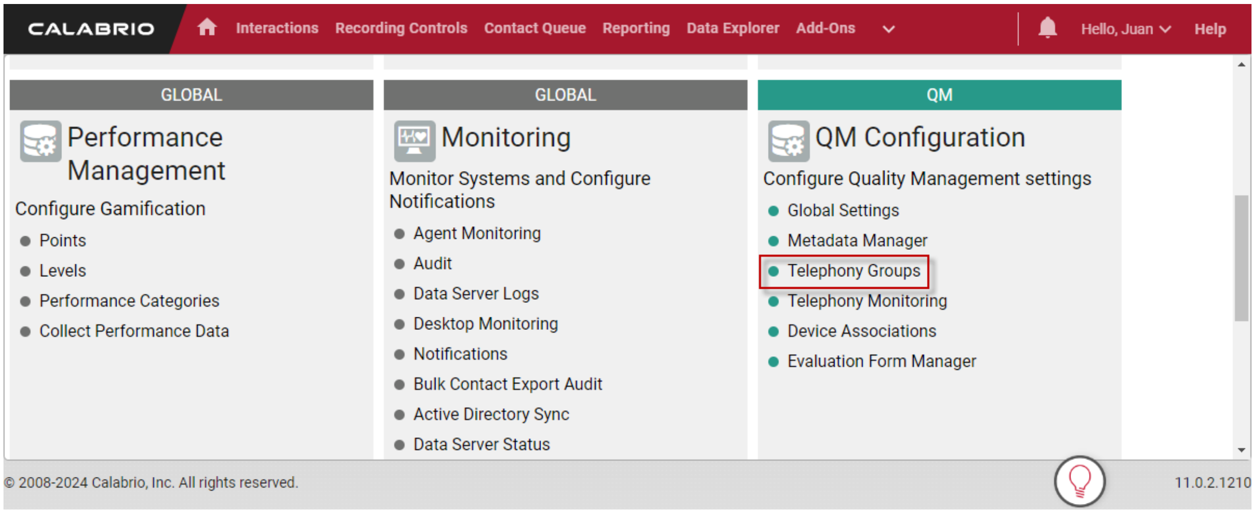
\Calabrio ONE\Data Server\gis

© 2008-2024 Calabrio, Inc. All rights reserved.

11.0.2.1210

8.4. Administer Telephony Groups

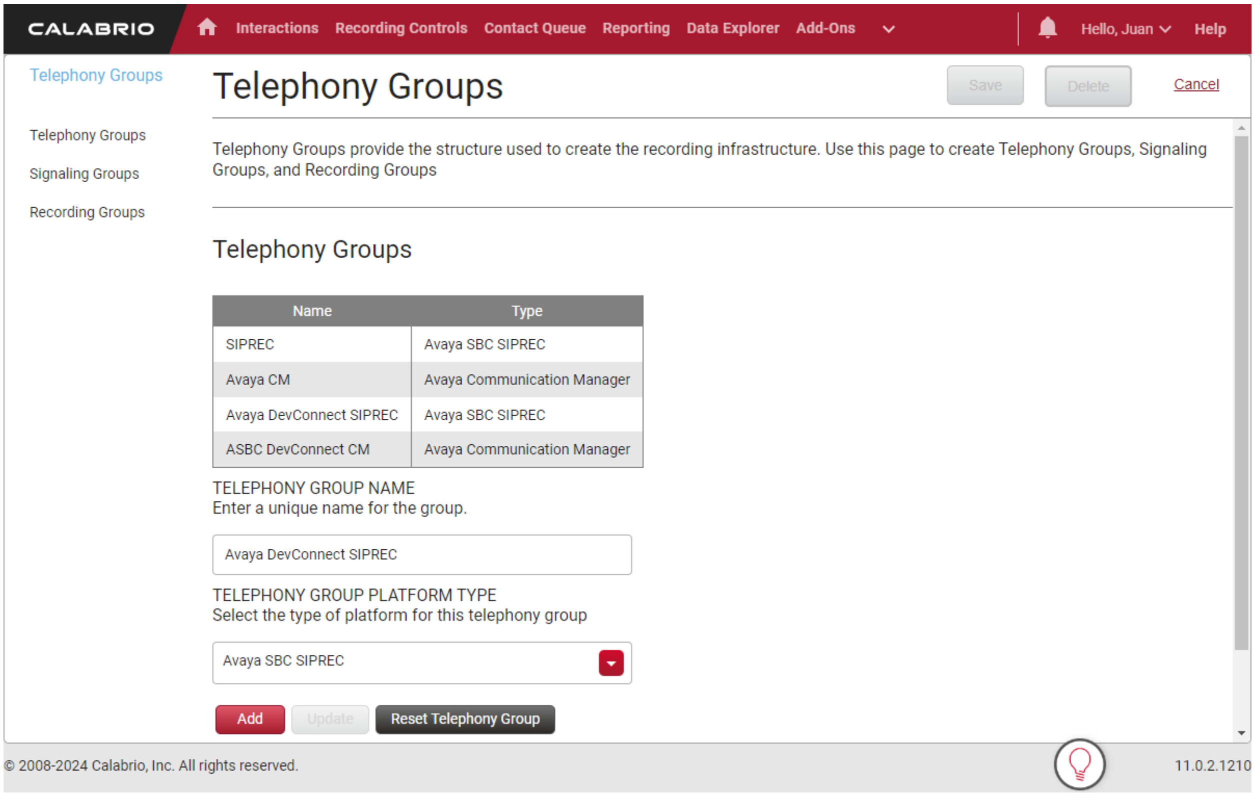
Navigate to **Application Management** to display the page below. Click on **Telephony Groups** under **QM Configuration**. Two telephony groups will be added for Avaya SBC SIPREC and one for Communication Manager.



8.4.1. Telephony Group for Avaya SBC SIPREC

This section covers the **Telephony Group** configuration for Avaya SBC SIPREC, which includes one signaling group and one recording group.

In the **Telephony Groups** page, specify a **TELEPHONY GROUP NAME** (e.g., *Avaya DevConnect SIPREC*) and set **TELEPHONY GROUP PLATFORM TYPE** to *Avaya SBC SIPREC* as shown below. Click **Add**.



Telephony Groups

Telephony Groups provide the structure used to create the recording infrastructure. Use this page to create Telephony Groups, Signaling Groups, and Recording Groups

Telephony Groups

Name	Type
SIPREC	Avaya SBC SIPREC
Avaya CM	Avaya Communication Manager
Avaya DevConnect SIPREC	Avaya SBC SIPREC
ASBC DevConnect CM	Avaya Communication Manager

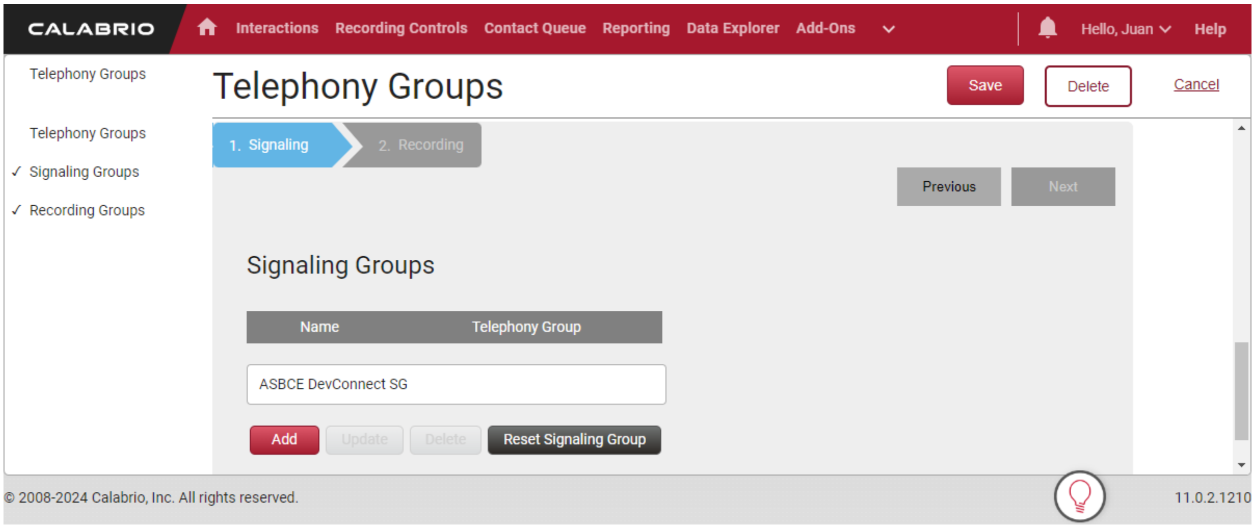
TELEPHONY GROUP NAME
Enter a unique name for the group.

Avaya DevConnect SIPREC

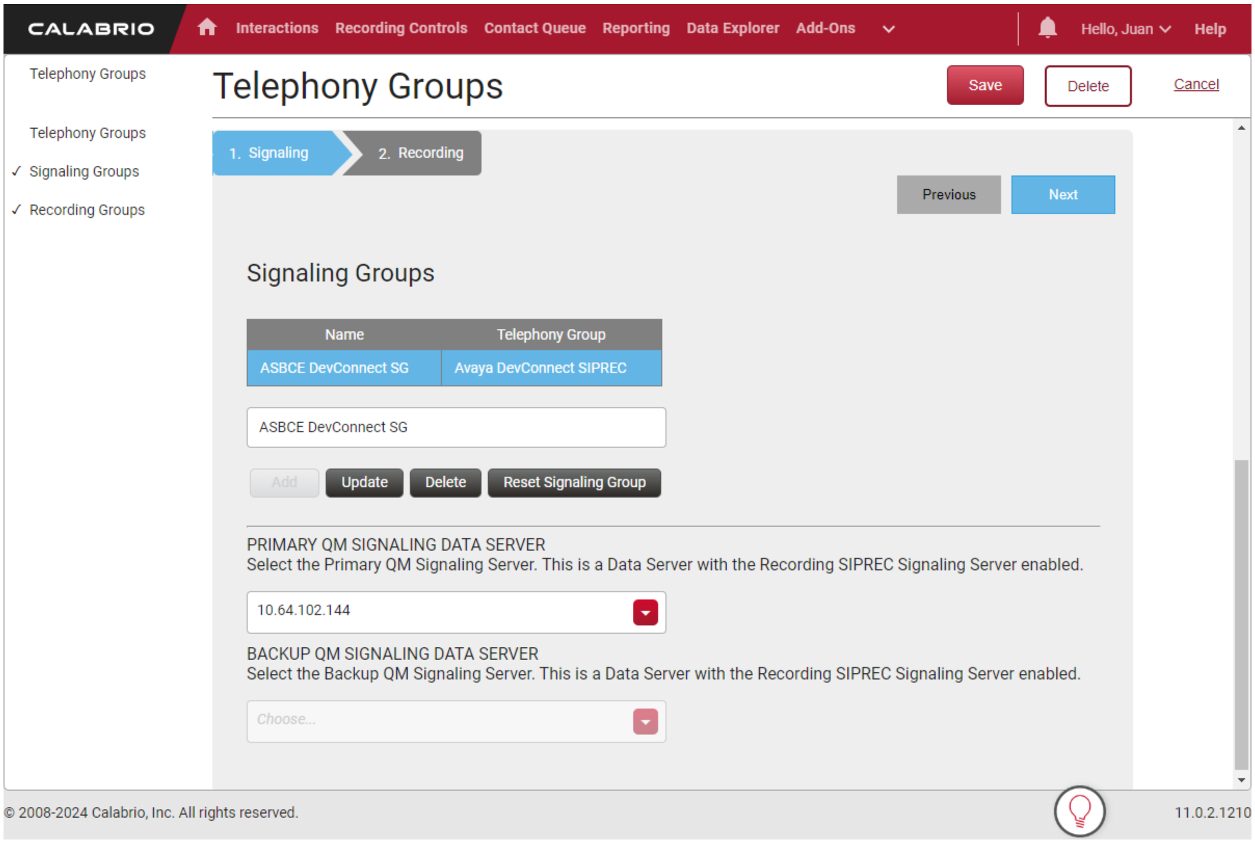
TELEPHONY GROUP PLATFORM TYPE
Select the type of platform for this telephony group

Avaya SBC SIPREC

Scroll down to the **Signaling Groups** section. Specify a Signaling Group **Name** (e.g., *ASBCE DevConnect SG)* and click **Add**.



Next, set **PRIMARY QM SIGNALING DATA SERVER** to the Calabrio QM Data Server IP address (e.g., *10.64.102.144*). Click **Next** to add a **Recording Group**.



Name	Telephony Group
ASBCE DevConnect SG	Avaya DevConnect SIPREC

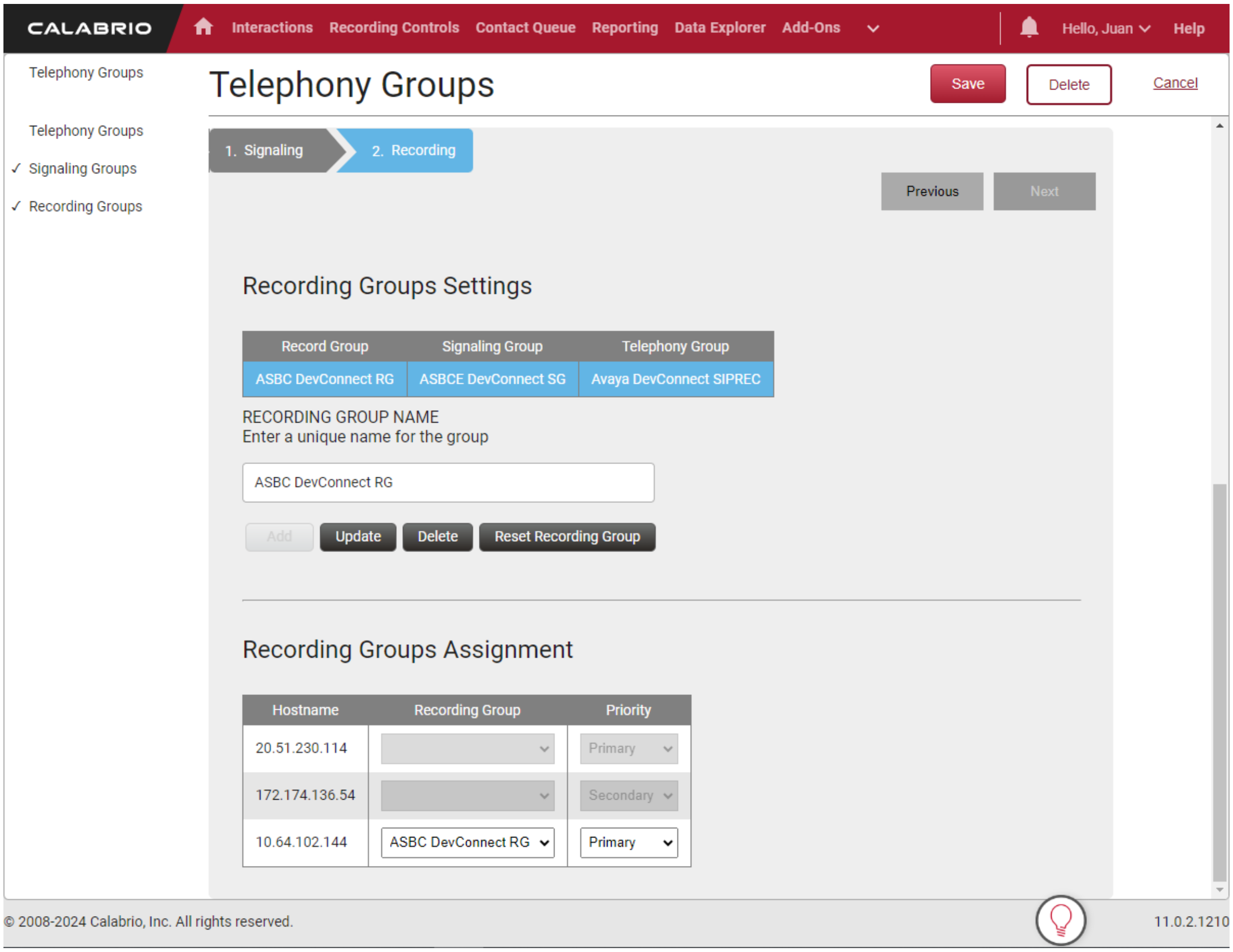
ASBCE DevConnect SG

PRIMARY QM SIGNALING DATA SERVER
Select the Primary QM Signaling Server. This is a Data Server with the Recording SIPREC Signaling Server enabled.

10.64.102.144

BACKUP QM SIGNALING DATA SERVER
Select the Backup QM Signaling Server. This is a Data Server with the Recording SIPREC Signaling Server enabled.

In the **Recording Group** page, specify a **RECORDING GROUP NAME** (e.g., *ASBC DevConnect RG*) as shown below. In the **Recording Groups Assignment** section, select the **Recording Group** (e.g., *ASBC DevConnect RG*) and **Priority** (e.g., *Primary*) by the Calabrio QM Data Server IP address (e.g., *10.64.102.144*). Click **Save**.



Telephony Groups

Recording Groups Settings

Record Group	Signaling Group	Telephony Group
ASBC DevConnect RG	ASBCE DevConnect SG	Avaya DevConnect SIPREC

RECORDING GROUP NAME
Enter a unique name for the group

ASBC DevConnect RG

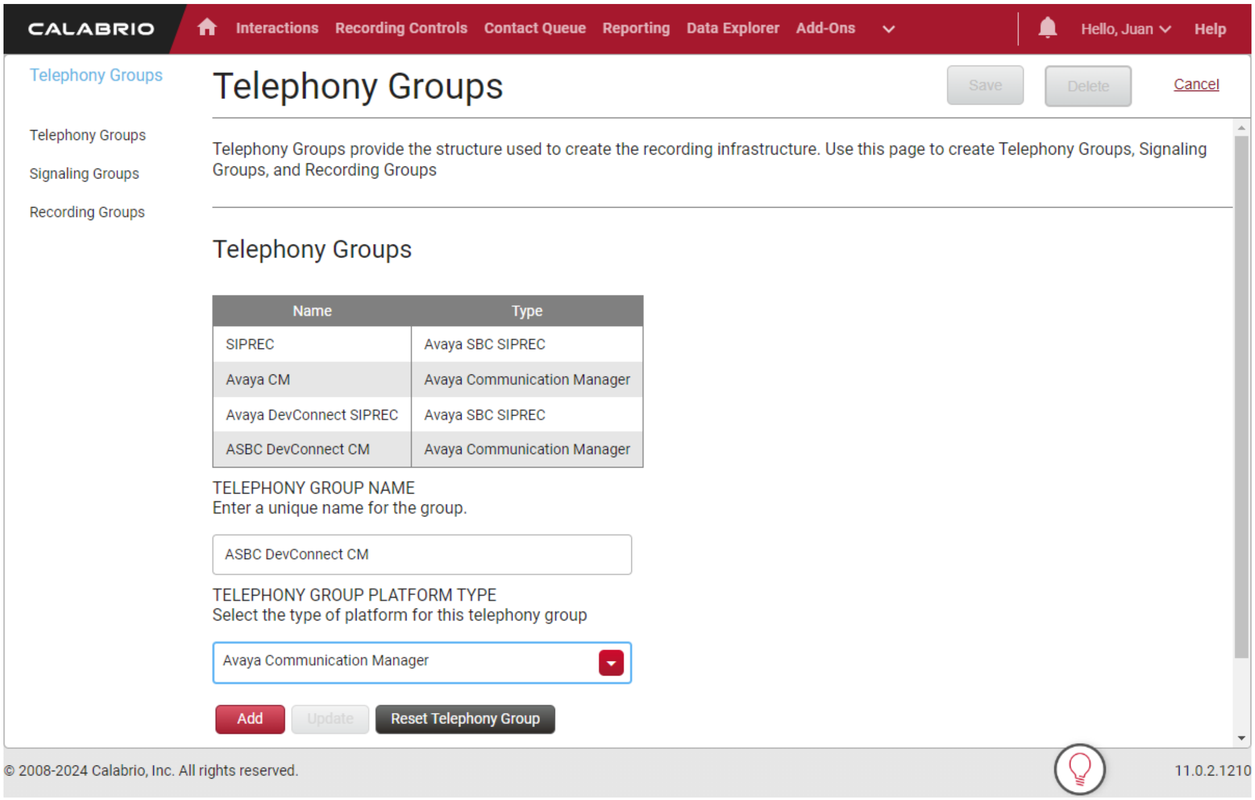
Recording Groups Assignment

Hostname	Recording Group	Priority
20.51.230.114		Primary
172.174.136.54		Secondary
10.64.102.144	ASBC DevConnect RG	Primary

8.4.2. Telephony Group for Communication Manager

This section covers the **Telephony Group** configuration for Communication Manager, which includes one signaling group and one recording group.

In the **Telephony Groups** page, specify a **TELEPHONY GROUP NAME** (e.g., *ASBC DevConnect CM*) and set **TELEPHONY GROUP PLATFORM TYPE** to *Avaya Communication Manager* as shown below. Click **Add**.



Telephony Groups

Telephony Groups provide the structure used to create the recording infrastructure. Use this page to create Telephony Groups, Signaling Groups, and Recording Groups

Telephony Groups

Name	Type
SIPREC	Avaya SBC SIPREC
Avaya CM	Avaya Communication Manager
Avaya DevConnect SIPREC	Avaya SBC SIPREC
ASBC DevConnect CM	Avaya Communication Manager

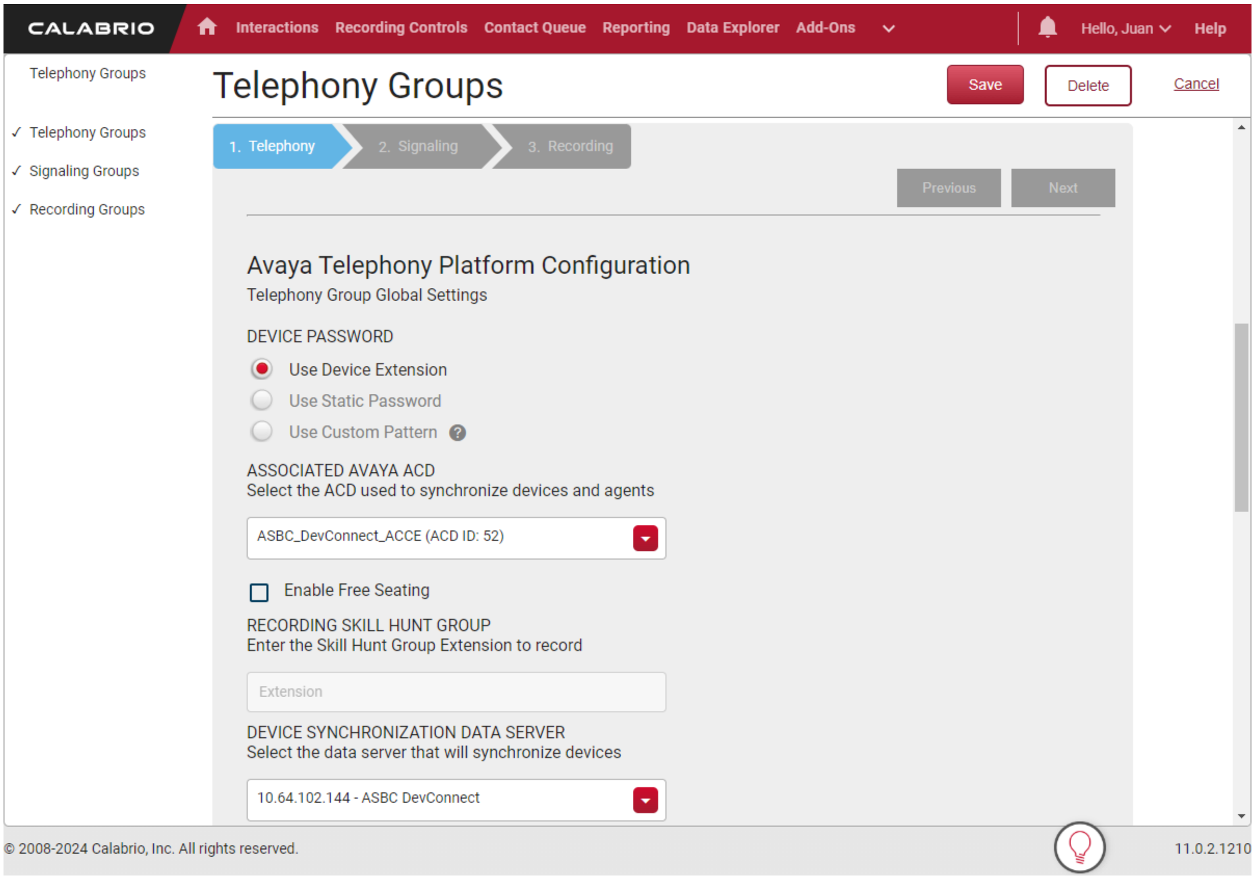
TELEPHONY GROUP NAME
Enter a unique name for the group.

ASBC DevConnect CM

TELEPHONY GROUP PLATFORM TYPE
Select the type of platform for this telephony group

Avaya Communication Manager

Scroll down to the **Avaya Telephony Platform Configuration** section. Set **DEVICE PASSWORD** to *Use Device Extension*, **ASSOCIATED AVAYA ACD** to the ACD added in **Section 8.2**, and **DEVICE SYNCHRONIZATION DATA SERVER** to the Calabrio QM Data Server added in **Section 8.3**. Click **Save**.



Telephony Groups

Avaya Telephony Platform Configuration

Telephony Group Global Settings

DEVICE PASSWORD

● Use Device Extension

○ Use Static Password

○ Use Custom Pattern

ASSOCIATED AVAYA ACD

Select the ACD used to synchronize devices and agents

ASBC_DevConnect_ACCE (ACD ID: 52)

□ Enable Free Seating

RECORDING SKILL HUNT GROUP

Enter the Skill Hunt Group Extension to record

Extension

DEVICE SYNCHRONIZATION DATA SERVER

Select the data server that will synchronize devices

10.64.102.144 - ASBC DevConnect

© 2008-2024 Calabrio, Inc. All rights reserved.

11.0.2.1210

8.5. Install TLS Certificates for Secure SIP Trunk to Avaya SBC

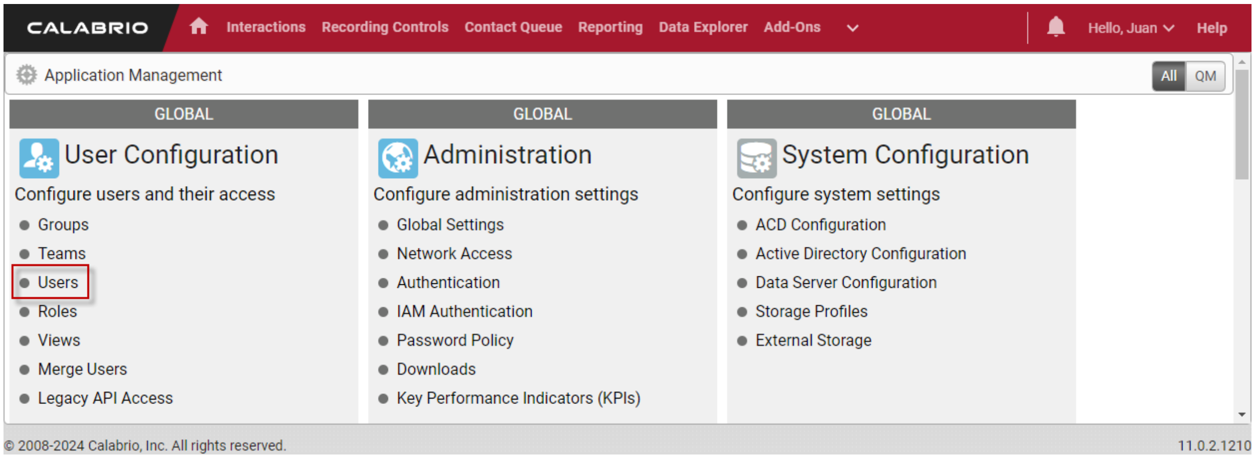
To establish a SIP trunk between Calabrio QM Data Server and Avaya SBC using TLS, the root CA certificate and an identity certificate must be installed on the Calabrio QM Data Server. The following high-level instructions describe the procedure for the compliance test, which may differ at a customer site. This section is provided for informational purposes only.

1. On the Calabrio QM Data Server, import the System Manager CA certificate via the Microsoft Management Console (MMC) Certificate Snap-in. For the compliance test, System Manager was used as the certificate authority (CA).
2. Generate a certificate signing request (CSR) via MMC certificate snap-in.
3. Provide the CSR to System Manager CA to generate a signed certificate for Calabrio QM Data Server.
4. Import the signed certificate via MMC certificate snap-in.
5. Export the certificate in PKCS #12 (.PFX) format to convert it into a **sip.keystore** file.
6. Convert PKCS #12 (.PFX) certificate into the sip.keystore to be used by Calabrio QM Data Server using the following conversion command.

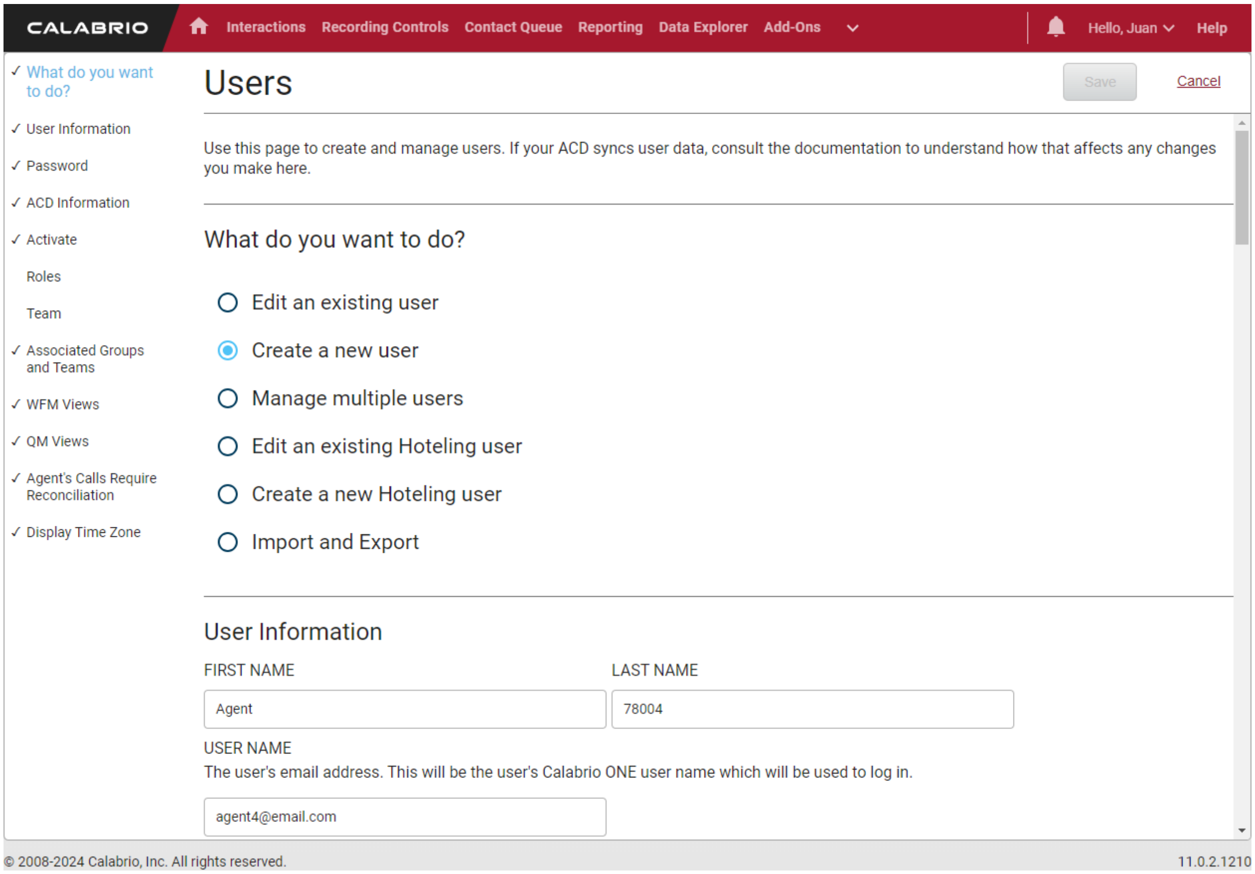
```
keytool -importkeystore -srckeystore <pfxcertfile> -
srcstoretype pkcs12 -destkeystore “C:\Program Files\Common
Files\Calabrio ONE\Data Server\config\sip.keystore”
```

8.6. Administer Users

Navigate to **Application Management** to display the page below. Click on **Users** under **User Configuration**. This section covers the configuration of agent users that will be associated with station extensions in **Section 8.7**.



In the **Users** page, select the **Create a new user** radio button. Specify **First Name**, **Last Name**, and email address for the user.



Users

Use this page to create and manage users. If your ACD syncs user data, consult the documentation to understand how that affects any changes you make here.

What do you want to do?

○ Edit an existing user
● Create a new user
○ Manage multiple users
○ Edit an existing Hoteling user
○ Create a new Hoteling user
○ Import and Export

User Information

FIRST NAME: Agent

LAST NAME: 78004

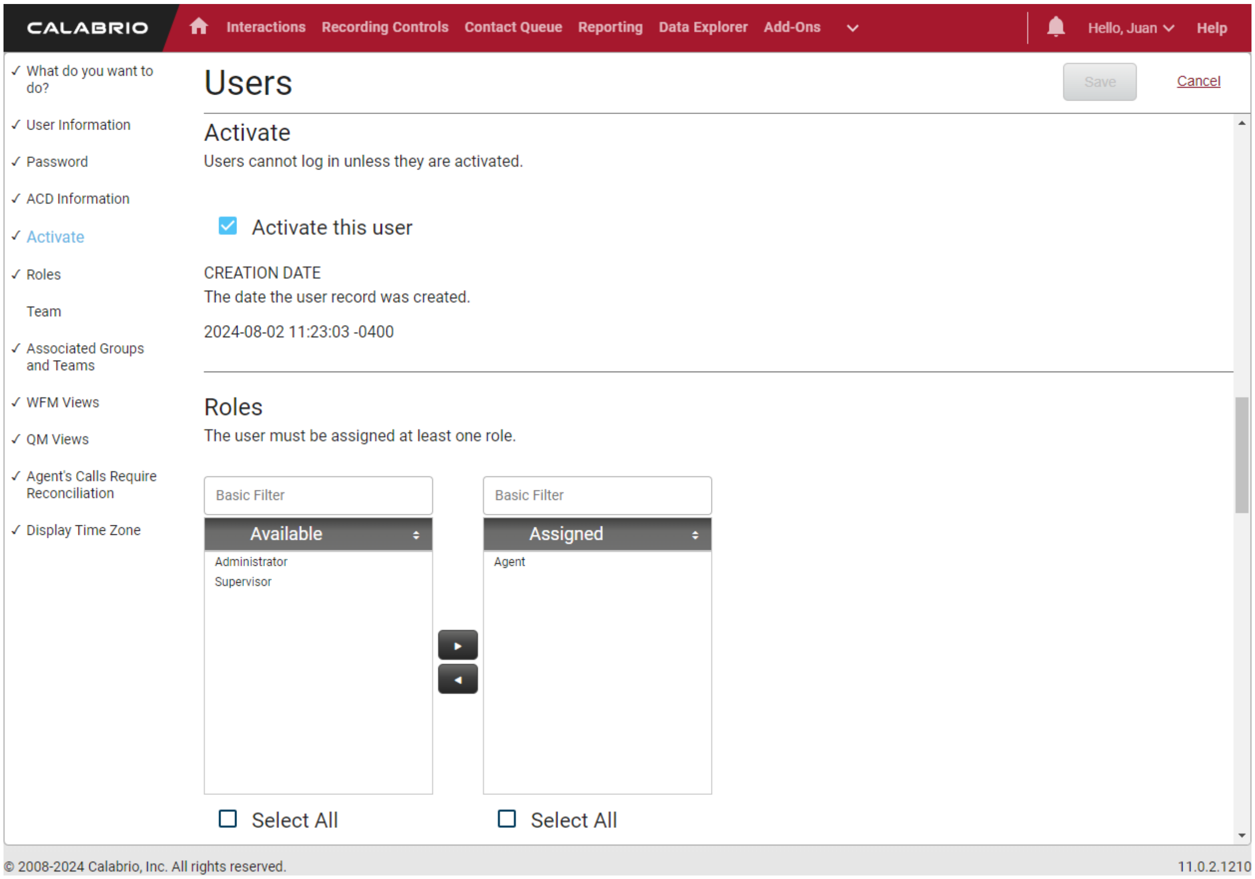
USER NAME
The user's email address. This will be the user's Calabrio ONE user name which will be used to log in.

agent4@email.com

© 2008-2024 Calabrio, Inc. All rights reserved.

11.0.2.1210

Scroll down to the **Activate** section and enable **Activate this user**. Under **Roles**, select the *Agent* role for this user as shown below.



Users

Activate

Users cannot log in unless they are activated.

☑ Activate this user

CREATION DATE

The date the user record was created.

2024-08-02 11:23:03 -0400

Roles

The user must be assigned at least one role.

Available	Assigned
Administrator Supervisor	Agent

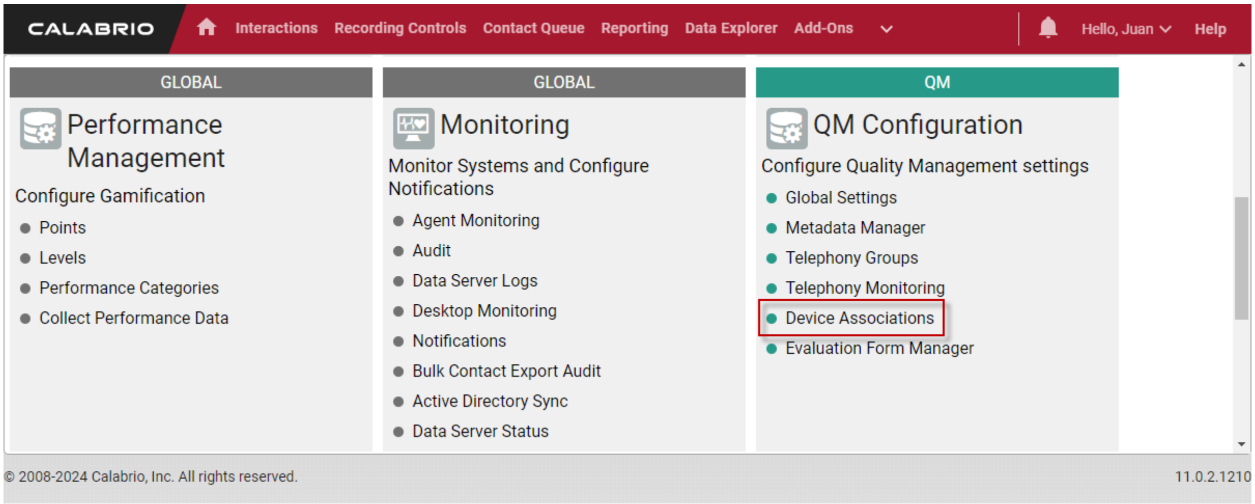
□ Select All   □ Select All

© 2008-2024 Calabrio, Inc. All rights reserved.
11.0.2.1210

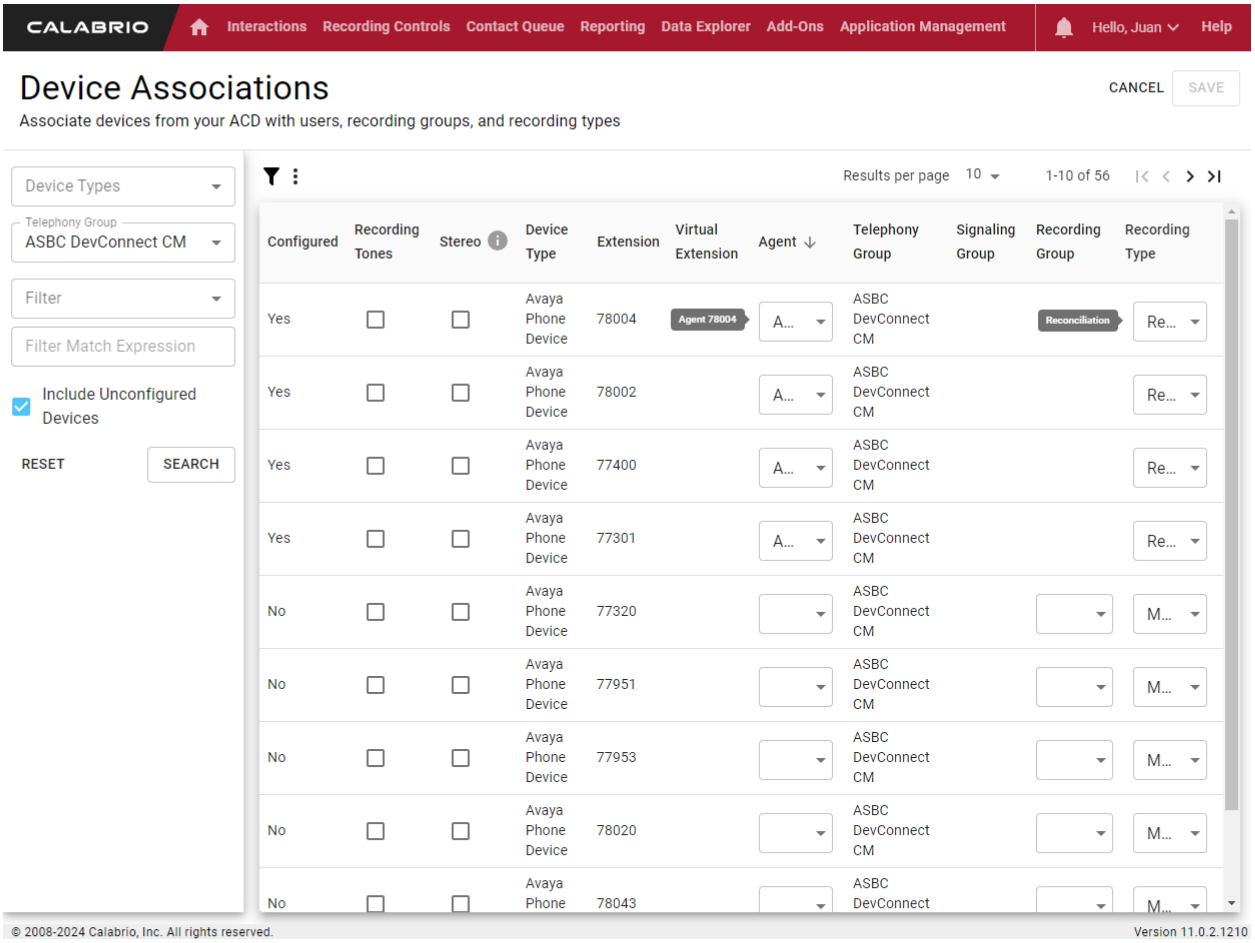
8.7. Administer Device Associations

Navigate to **Application Management** to display the page below. Click on **Device Associations** under **QM Configuration**. In the **Device Associations** page, agent users, configured in **Section 8.6**, are associated with station extensions retrieved from Communication Manager via SMS.

Note that with statically mapped agent users to station extensions, hot desking is not supported, and agent login-IDs on Communication Manager are not used in this solution.



In the **Device Associations** page, associate station extensions with an agent user by setting the **Agent** field. In addition, set **Recording Type** to *Reconciliation* as shown below for the first four station extensions. The **Agent** and **Recording Type** fields must be configured to reconcile root calls associated with an agent/station extension. Click **Save**.



Device Associations

Associate devices from your ACD with users, recording groups, and recording types

Device Types

Telephony Group: ASBC DevConnect CM

Filter

Filter Match Expression

☑ Include Unconfigured Devices

Results per page 10 1-10 of 56

Configured	Recording Tones	Stereo	Device Type	Extension	Virtual Extension	Agent	Telephony Group	Signaling Group	Recording Group	Recording Type
Yes	□	□	Avaya Phone Device	78004		Agent 78004 A...	ASBC DevConnect CM			Reconciliation Re...
Yes	□	□	Avaya Phone Device	78002		A...	ASBC DevConnect CM			Re...
Yes	□	□	Avaya Phone Device	77400		A...	ASBC DevConnect CM			Re...
Yes	□	□	Avaya Phone Device	77301		A...	ASBC DevConnect CM			Re...
No	□	□	Avaya Phone Device	77320			ASBC DevConnect CM			M...
No	□	□	Avaya Phone Device	77951			ASBC DevConnect CM			M...
No	□	□	Avaya Phone Device	77953			ASBC DevConnect CM			M...
No	□	□	Avaya Phone Device	78020			ASBC DevConnect CM			M...
No	□	□	Avaya Phone	78043			ASBC DevConnect			M...

© 2008-2024 Calabrio, Inc. All rights reserved. Version 11.0.2.1210

8.8. Restart Services

After completing the Calabrio QM configuration, restart the *Calabrio ONE Network Recording Service* and *Calabrio ONE SIPREC Service* under Windows Services.

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, Avaya SBC, and Calabrio Quality Management.

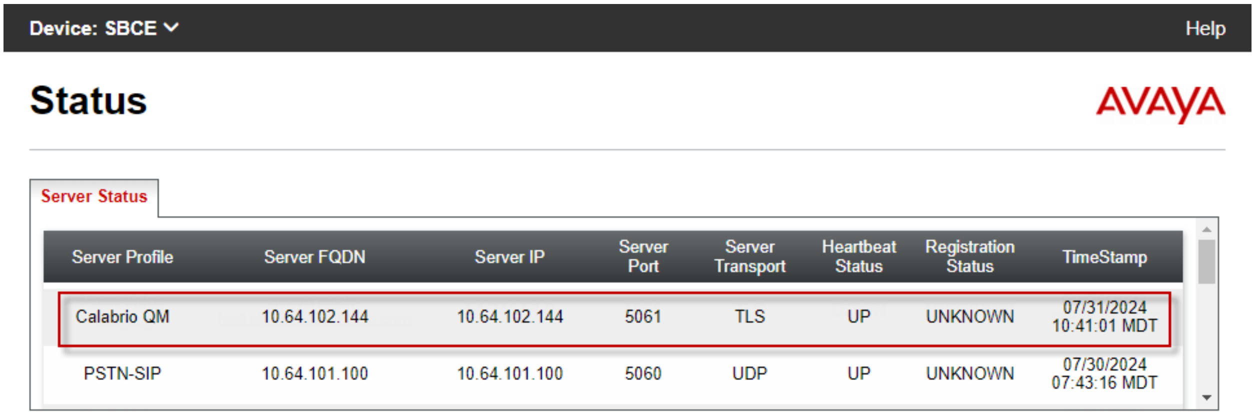
9.1. Verify Avaya Aura® Communication Manager

From the Communication Manager SAT, use the **status cdr-link** command to verify that the CDR link to the Calabrio QM Data Server is *up*.

```
status cdr-link
                                CDR LINK STATUS
                   Primary                        Secondary

       Link State: up                             CDR not administered

      Date & Time: 2024/07/31 10:41:30            0000/00/00 00:00:00
  Forward Seq. No: 20                             0
 Backward Seq. No: 0                              0
CDR Buffer % Full:   0.00                           0.00
      Reason Code: OK
```

9.2. Verify Avaya Session Border Controller

To verify that the SIP trunk between Avaya SBC and Calabrio QM Data Server is in-service, navigate to **Status → Server Status** in the Avaya SBC web interface. Verify that the **Heartbeat Status** of the SIP trunk is *UP* as shown below.



Status

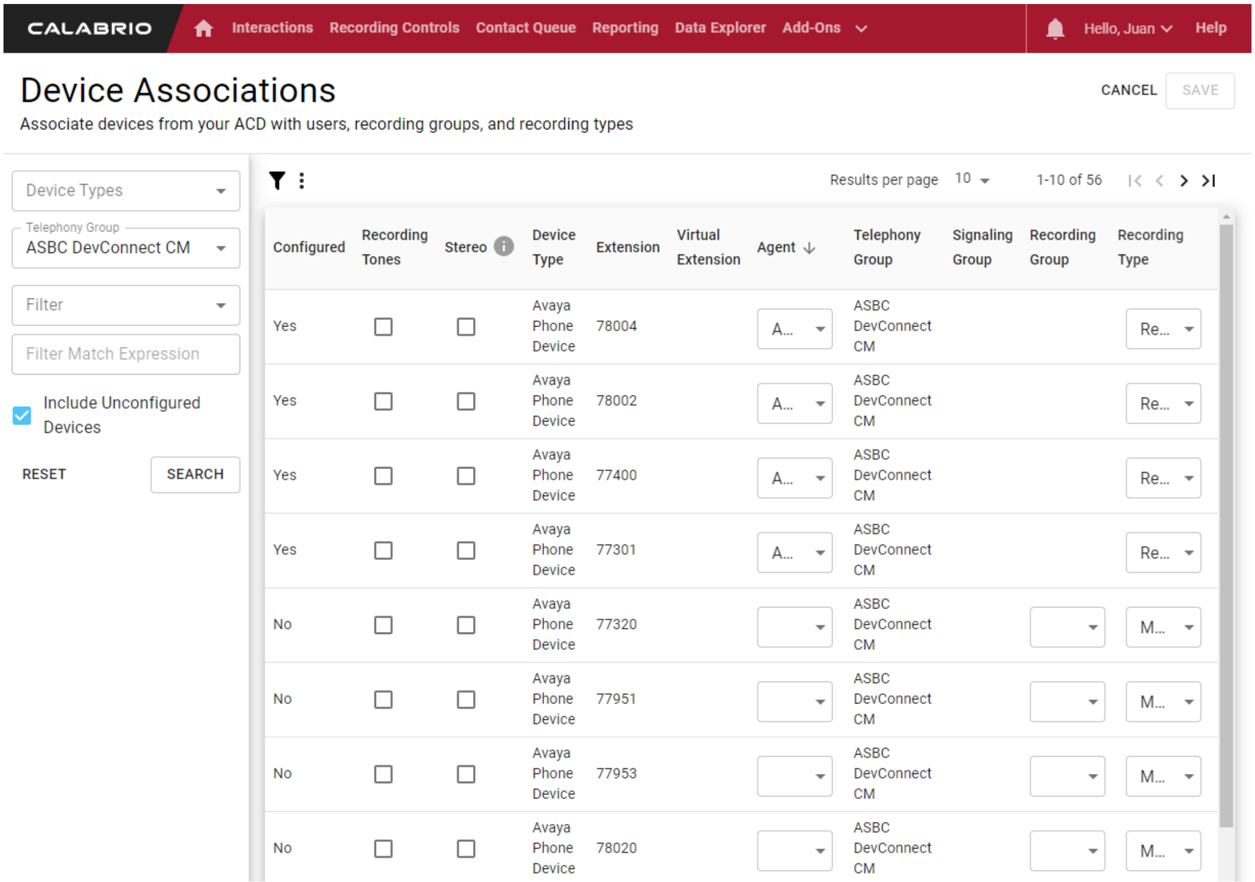
Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp
Calabrio QM	10.64.102.144	10.64.102.144	5061	TLS	UP	UNKNOWN	07/31/2024 10:41:01 MDT
PSTN-SIP	10.64.101.100	10.64.101.100	5060	UDP	UP	UNKNOWN	07/30/2024 07:43:16 MDT

9.3. Verify Calabrio Quality Management

This section covers verifying retrieving station extensions via SMS, CDR from Communication Manager, and generating call recordings.

9.3.1. Station Extensions using SMS

Navigate to **Application Management → QM Configuration → Device Associations** to verify that station extensions were retrieved from Communication Manager using SMS on Application Enablement Services.



Device Associations

Associate devices from your ACD with users, recording groups, and recording types

Device Types

Telephony Group: ASBC DevConnect CM

Filter

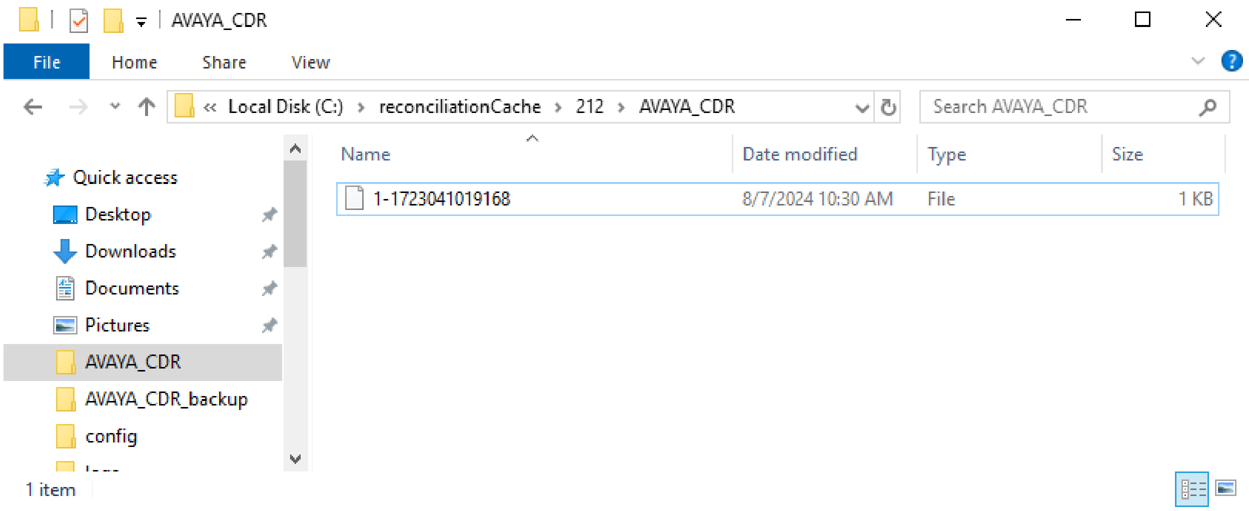
Filter Match Expression

☑ Include Unconfigured Devices

Configured	Recording Tones	Stereo	Device Type	Extension	Virtual Extension	Agent	Telephony Group	Signaling Group	Recording Group	Recording Type
Yes	☐	☐	Avaya Phone Device	78004		A...	ASBC DevConnect CM			Re...
Yes	☐	☐	Avaya Phone Device	78002		A...	ASBC DevConnect CM			Re...
Yes	☐	☐	Avaya Phone Device	77400		A...	ASBC DevConnect CM			Re...
Yes	☐	☐	Avaya Phone Device	77301		A...	ASBC DevConnect CM			Re...
No	☐	☐	Avaya Phone Device	77320			ASBC DevConnect CM			M...
No	☐	☐	Avaya Phone Device	77951			ASBC DevConnect CM			M...
No	☐	☐	Avaya Phone Device	77953			ASBC DevConnect CM			M...
No	☐	☐	Avaya Phone Device	78020			ASBC DevConnect CM			M...

9.3.2. CDR

Place a call from the PSTN (e.g., 1 732 444 1001) to an agent station (e.g., 77301) and then perform a blind transfer to another agent station (e.g., 78002). Terminate all calls. Verify that CDR was collected from Communication Manager and stored in a CDR file in the `C:\reconciliationCache\212\AVAYA_CDR` folder temporarily until is uploaded to the Calabrio Cloud. The CDR file is then moved to `C:\reconciliationCache\212\AVAYA_CDR_backup` folder, where 212 is the Calabrio tenant which would be different for each customer.



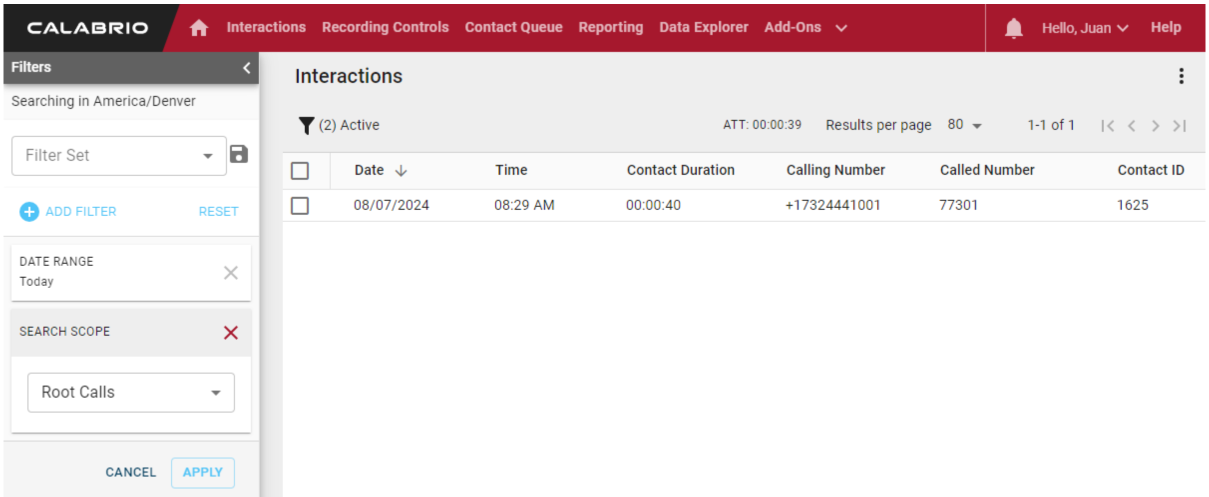
Name	Date modified	Type	Size
1-1723041019168	8/7/2024 10:30 AM	File	1 KB

Verify the accuracy of the CDR file. For this call, there are two CDR records, one for the call from the PSTN to the first agent station, and another one for the transferred call.

```
0807240829000219                          77301082948     0001    00 7
00011000031723040957    1732444100100             082927
0807240830000179                          78002083005     0001    00
00011000031723040957    1732444100100             082948
```

9.3.3. Call Recordings

Continuing with the transferred call above, verify that a root recording was created for the entire call, including the original and transferred call. Permission access to root calls must be enabled for the user's role. The root call is available under **Interactions** in the Calabrio Cloud Portal as shown below. Double-click on the root call to play back recording.

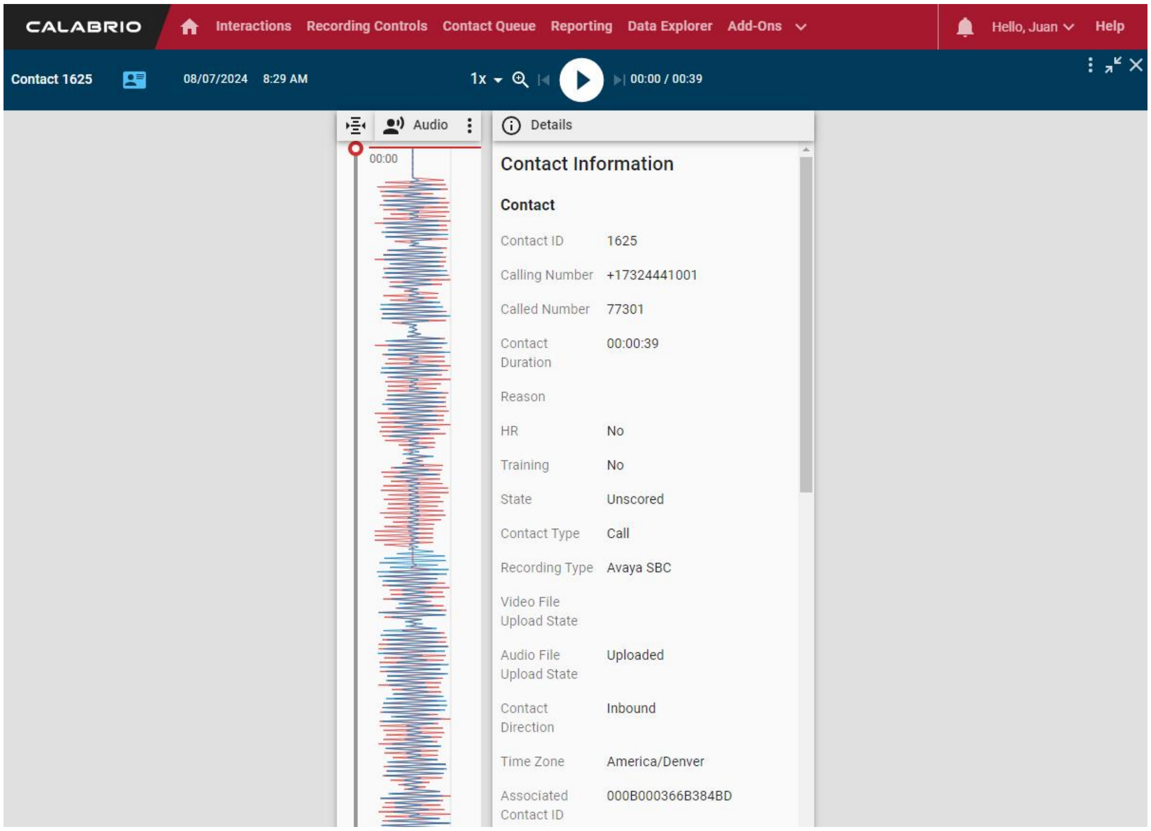


DATE RANGE
Today

SEARCH SCOPE
Root Calls

Date	Time	Contact Duration	Calling Number	Called Number	Contact ID
08/07/2024	08:29 AM	00:00:40	+17324441001	77301	1625

The root recording is displayed with its metadata. Click the play button to listen to the recording.

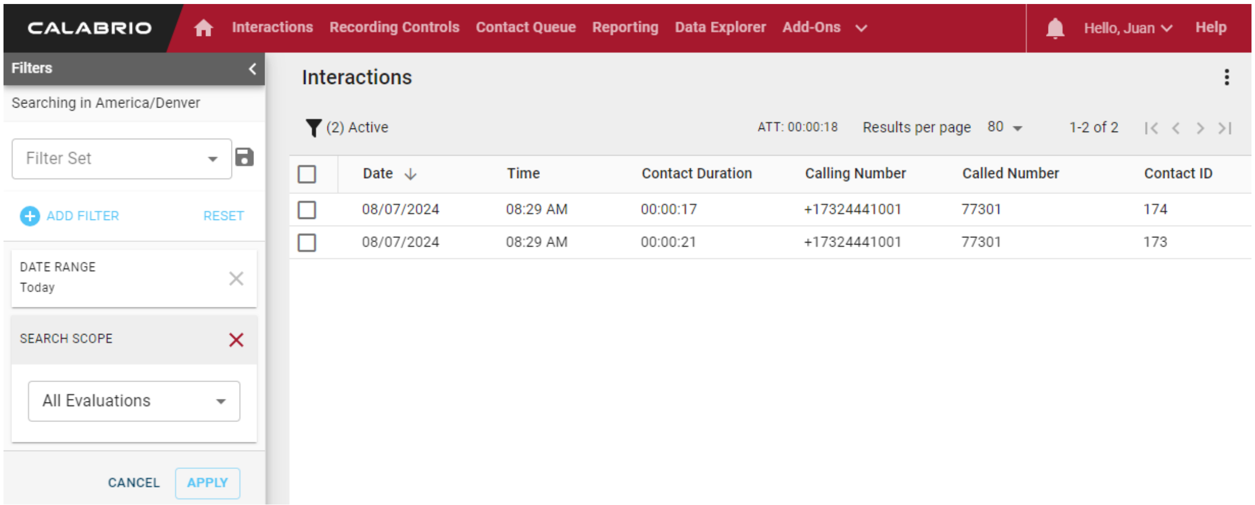


Contact Information

Contact

Contact ID	1625
Calling Number	+17324441001
Called Number	77301
Contact Duration	00:00:39
Reason	
HR	No
Training	No
State	Unscored
Contact Type	Call
Recording Type	Avaya SBC
Video File Upload State	
Audio File Upload State	Uploaded
Contact Direction	Inbound
Time Zone	America/Denver
Associated Contact ID	000B000366B384BD

After 15-20 minutes, the reconciliation process should be completed and the root call should be segmented into separate call legs and associated with agent extensioins, one for the original call and another one for the transferred call, as shown below. Set the **Search Scope** to *All Evaluations* to view call recordings after reconciliation.



Searching in America/Denver

DATE RANGE
Today

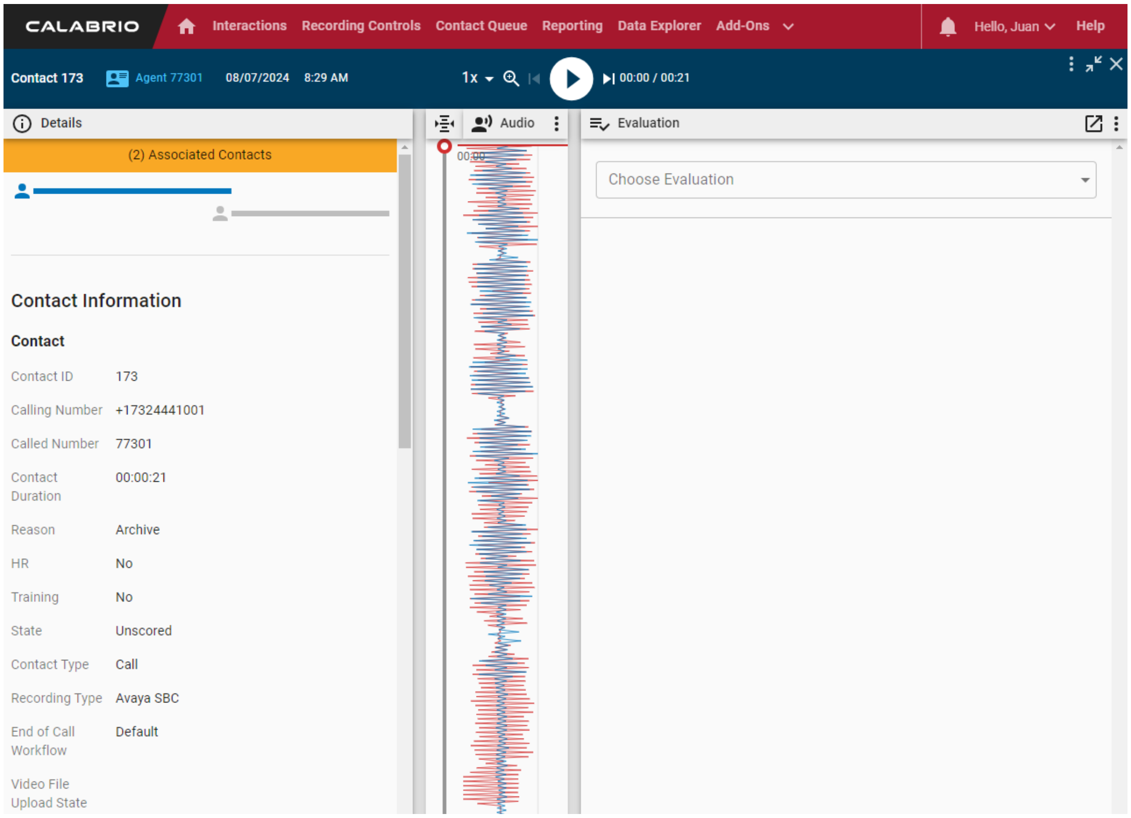
SEARCH SCOPE
All Evaluations

Interactions

(2) Active   ATT: 00:00:18   Results per page 80   1-2 of 2

Date	Time	Contact Duration	Calling Number	Called Number	Contact ID
08/07/2024	08:29 AM	00:00:17	+17324441001	77301	174
08/07/2024	08:29 AM	00:00:21	+17324441001	77301	173

Double-click on a recording to view and play back the recording. Note that both recordings are associated with the same root call. The following recording is for the original call.



Contact 173   Agent 77301   08/07/2024   8:29 AM   00:00 / 00:21

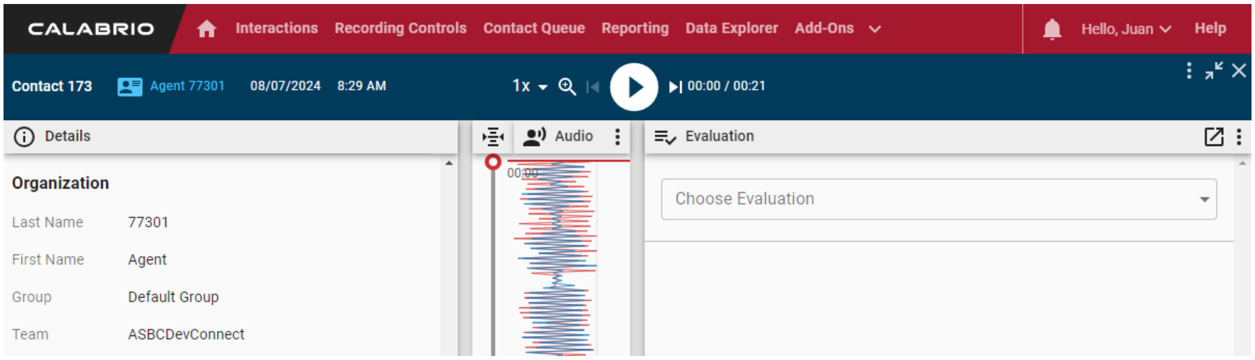
(2) Associated Contacts

Contact Information

Contact

Contact ID	173
Calling Number	+17324441001
Called Number	77301
Contact Duration	00:00:21
Reason	Archive
HR	No
Training	No
State	Unscored
Contact Type	Call
Recording Type	Avaya SBC
End of Call Workflow	Default
Video File Upload State	

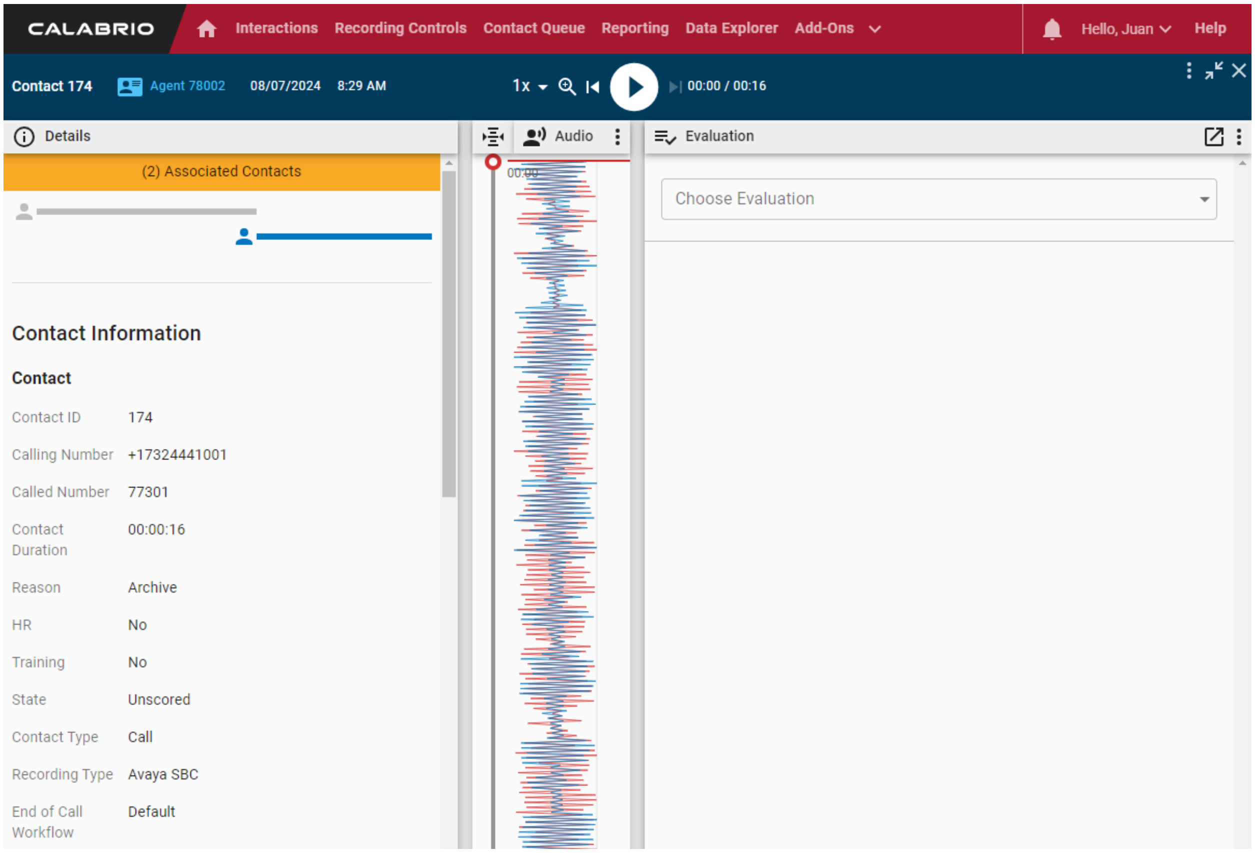
Scroll down to the **Organization** section to view the agent station associated with the call.



Organization

Last Name	77301
First Name	Agent
Group	Default Group
Team	ASBCDevConnect

Click on the second recording associated with the transferred call to view and play back the recording.

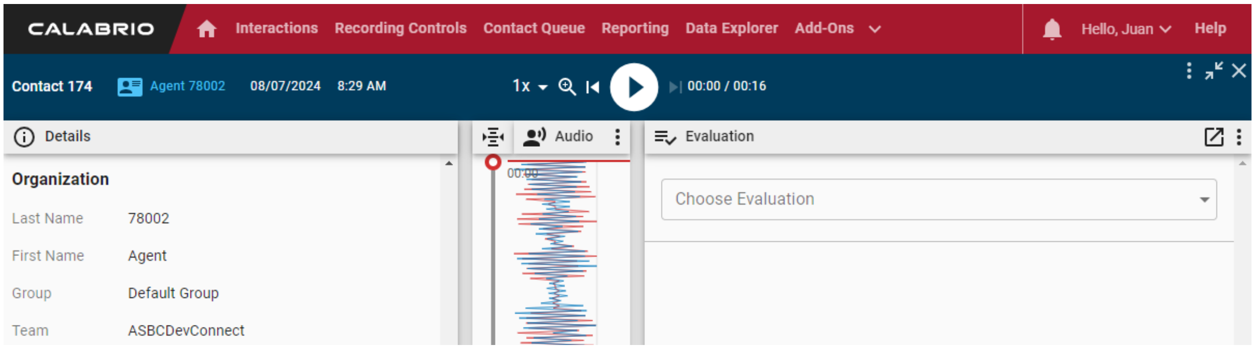


Contact Information

Contact

Contact ID	174
Calling Number	+17324441001
Called Number	77301
Contact Duration	00:00:16
Reason	Archive
HR	No
Training	No
State	Unscored
Contact Type	Call
Recording Type	Avaya SBC
End of Call Workflow	Default

Scroll down to the Organization section to view the agent station associated with the call.



Organization

Last Name	78002
First Name	Agent
Group	Default Group
Team	ASBCDevConnect

10. Conclusion

These Application Notes described the configuration steps required for Calabrio Quality Management to interoperate with Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services using SMS, and Avaya Session Border Controller using SIPREC. Calabrio Quality Management successfully retrieved station extensions and CDR from Avaya Aura® Communication Manager using SMS and Avaya Reliable Session Protocol, respectively, and recorded PSTN calls routed through Avaya Session Border Controller using SIPREC. Stereo call recordings were logged and played back via the Calabrio Cloud Portal. All test cases passed with observations noted in **Section 2.2**.

11. Additional References

This section references the product documentation relevant to these Application Notes.

[1] *Administering Avaya Aura® Communication Manager*, Release 10.2.x, Issue 4, May 2024, available at https://support.avaya.com.

[2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 10.2.x Issue 2, April 2024, available at https://support.avaya.com.

[3] *Administering Avaya Aura® Application Enablement Services*, Release 10.2.x, Issue 1, December 2023, available at https://support.avaya.com.

[4] *Administering Avaya Session Border Controller*, Release 10.2.x, Issue 3, July 2024, available at https://support.avaya.com.

[5] *Calabrio Help Center for Administrators*, available at https://help.calabrio.com/doc/container-home.htm.

©2024 Avaya LLC. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.