About this Guide .......................................................... ix

Overview .................................................................... ix
  Audience .................................................................. ix
  Supported SBC Platforms ........................................... ix

Related Documentation ................................................ ix

Revision History .......................................................... x

1 Overview ................................................................. 13
  Introduction ................................................................ 13
  About the ISR .......................................................... 13
  SIPREC Support ......................................................... 14
  About the ISR Dashboard ............................................ 14
    Requirements/Recommendations ................................. 14
    Security Features .................................................... 15
  ISR Third-Party Licensing ........................................... 15

2 Getting Started ......................................................... 17
  Introduction ................................................................ 17
  Logging In/Out of the ISR Dashboard ............................ 17
    User Access Levels ................................................... 20
  Editing My Settings .................................................... 21
    Dashboard Settings ................................................... 22
    Recordings List Settings ............................................. 25
    RSS View Settings ................................................... 26
    Help Link ................................................................ 27
  Dashboard Tools ......................................................... 28
    Functional Icons ..................................................... 28
    Paging Tool ............................................................ 29
3 Managing Realms/Accounts ....................................................... 41

Introduction ................................................................................. 41
Administrator Menu ................................................................. 41
Manage Realms ................................................................. 42
  How Realm-based Recording Works ............................................ 42
  Adding a Realm ........................................................................ 44
  Associating an Account to a Realm ............................................ 45
  Editing a Realm ....................................................................... 46
  Deleting a Realm .................................................................... 47
Manage Accounts ........................................................... 48
  Adding an Account .................................................................. 49
  Configuring/ Editing Details for an Account ................................. 50
    Edit General Account Information ........................................ 51
  Account Branding ................................................................. 52
  Account Route Defaults ....................................................... 53
    Recording Defaults ............................................................ 54
      Recording Editing Permissions ............................................... 55
      Announcement and Recurring Beep Defaults .......................... 55
      Conference Mode Defaults ................................................ 56
      Record and Save Mode Defaults .......................................... 57
      Custom Data Defaults ....................................................... 57
      Sessions Capacity Defaults ................................................ 58
  Viewing and Editing Account Routes, Users, Realms, and the Remote Archiver Server ............................................ 59
    Account Routes ..................................................................... 59
    Account Users ..................................................................... 59
    Account Realms .................................................................. 60
    Account Remote Archiver Server .......................................... 60
  Deleting an Account .................................................................. 61
  Importing an Account CSV File ................................................. 61
# Managing Sites

- Introduction .................................................. 103
- Manage Sites .................................................. 103
  - Adding a Site ............................................... 104
  - Managing an RSS ........................................... 105
    - Adding an RSS ........................................... 105
    - Editing an RSS ......................................... 108
    - Deleting an RSS ......................................... 109
  - RSS Handling of a 302 Response via the ISR .......... 110
  - Managing an RSS Location ................................ 110
    - Adding a Location ...................................... 110
    - Editing a Location ...................................... 112
    - Deleting a Location .................................... 113
  - Managing Archivers ....................................... 114
    - Adding an Archiver .................................... 117
    - Editing an Archiver .................................... 121
    - Deleting an Archiver ................................... 123
  - Managing Session Agents ................................ 124
    - Adding a Session Agent ................................ 124
    - Editing a Session Agent ................................ 126
    - Deleting a Session Agent ................................ 127
    - Display Events for a Session Agent ............... 128
    - Advanced Configuration for Session Agents (Site-wide) .... 129
  - Managing Web Appliances ................................ 131
    - Adding a Web Appliance ................................ 131
    - Editing a Web Appliance ................................ 134
    - Deleting a Web Appliance ............................... 135

# Viewing Live Sessions

- Introduction .................................................. 137
- Manage Live Sessions ....................................... 137
  - Viewing Live Sessions .................................... 139

# Managing Recordings

- Introduction .................................................. 141
- Manage Recordings .......................................... 141
  - Playing a Recording ...................................... 143
  - Viewing and Editing Details of a Recording ........... 144
  - Recording Details ....................................... 145
  - Archiving Recordings Permanently ....................... 147
B  ISR RMC ................................................................. 181
   About the ISR RMC ................................................. 181
   ISR RMC License ................................................ 181
      Obtaining the RMC License Key ............................ 181
      Installing the RMC License Key ............................ 182
      Testing the RMC Converter ................................ 183
   Assigning RMC Conversion to Specific Locations .......... 186

C  Remote Archival Webservice WSDL ......................... 191
   Remote Archival Webservice WSDL ......................... 191

D  ISR Database Schema Definitions and Descriptions .... 205
   Introduction ..................................................... 205
   ISR Administrator Database Schema Parameters .......... 206
   ISR Administrator Database Schema Descriptions ....... 209
About this Guide

Overview

The Interactive Session Recorder Administrator Guide provides information about accessing and using the Interactive Session Recorder (ISR) Dashboard for:

- Configuring accounts, routes, and users
- Managing sites, RSS servers, and system configurations
- Accessing recordings
- Building reports

This guide also provides a ISR software diagram and call setup sequence (Appendix A), as well as the ISR database schema definitions and descriptions (Appendix B) for additional information.

Audience

This guide is intended for the Administrator level users (Super User and Account Administrator). Available features/functions in the ISR are dependant on the administrator’s level of access. For more information about the user level privileges in the ISR, see Chapter 6, Managing Users in this guide.

Supported SBC Platforms

The following Session Director (SD) products are certified for use with the ISR software:

- C-Series (3000/4000) SDs
- E-Series (2600) SDs
- Application Session Controller (ASC)

Note: For more information on the C-Series, E-Series, and ASC hardware, see Oracle’s applicable hardware documentation.

Related Documentation

The following table lists related documents.

<table>
<thead>
<tr>
<th>Document Name</th>
<th>Document Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interactive Session Recorder Release Notes</td>
<td>Contains information about new ISR features and fixed issues in the current release of the ISR.</td>
</tr>
<tr>
<td>Interactive Session Recorder Installation Guide, Release Version 5.0</td>
<td>Provides an overview of the ISR, hardware/software requirements and recommendations, storage considerations, pre-installation information, installation procedures, post-install verification procedures, making the first call, and additional advanced topics about the ISR.</td>
</tr>
</tbody>
</table>
Interactive Session Recorder User’s Guide
Contains information about using the ISR Dashboard for all levels of users. Provides information about viewing, playing, deleting recordings, running reports, managing user profiles (Super User, Account Administrator, and Tenant Administrator only).

Interactive Session Recorder API Reference Guide
Contains information about Methods for Recording, VoiceXML Commands, representational state transfer (REST) application programming interface (API), Recording File Types/ Formats Supported, Return Codes, sendIPCRCommand.jsp Subdialog, Advanced Options, Troubleshooting.

Interactive Session Recorder Monitoring Guide
Contains information about installing and configuring the ISR Monitor. It also includes the Monitor database schema as well as the Monitor MIB.

Interactive Session Recorder Remote Archival Web Services Reference Guide
Contains information about the Remote Archival Web Service, its Control methods, WSDL definitions, DataType Definitions, sample responses to requests, and importing the Remote Archival Web Service’s certificate into the client keystore.

Revision History
This section contains the revision history for this document.

<table>
<thead>
<tr>
<th>Date</th>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 31, 2013</td>
<td>Revision 1.00</td>
<td>• Initial release of the ISR 5.1 software.</td>
</tr>
<tr>
<td>September 10, 2013</td>
<td>Revision 1.01</td>
<td>• Updates the Securing the ISR chapter.</td>
</tr>
<tr>
<td>September 11, 2013</td>
<td>Revision 1.02</td>
<td>• Updates editing the /opt/jboss/standalone/configuration/standalone.xml file in the Securing the ISR chapter.</td>
</tr>
<tr>
<td>October 31, 2013</td>
<td>Revision 1.03</td>
<td>• Updates commands in the SSL-Enabling the Remote Archival Webservice section.</td>
</tr>
<tr>
<td>November 20, 2013</td>
<td>Revision 1.10</td>
<td>• Changes Enabling Serving Pages with SSL section title to SSL-Enabling the ISR Dashboard and updates this section.</td>
</tr>
<tr>
<td>May 16, 2014</td>
<td>Revision 1.11</td>
<td>• Replaces NN-ISR with ISR.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Adds “Adding User Accounts on the RSS”.</td>
</tr>
<tr>
<td>September 2014</td>
<td>Revision 1.12</td>
<td>• Updates the Securing the ISR chapter.</td>
</tr>
<tr>
<td>May 2015</td>
<td>Revision 1.20</td>
<td>• Adds “SSL-Enabling the RSS ISR API” section to the Securing the ISR chapter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updates the “SSL-Enabling the Remote Archival Webservice” section in the Securing the ISR chapter.</td>
</tr>
<tr>
<td>Date</td>
<td>Release</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>August 2015</td>
<td>Revision 1.21</td>
<td>• Updates “Generating a PEM Format Keystore” section.</td>
</tr>
<tr>
<td>December 2015</td>
<td>Revision 1.21</td>
<td>• Adds the Interactive Session Recorder Remote Archival Web Services Reference Guide to the list of Related Documentation.</td>
</tr>
</tbody>
</table>
1 Overview

Introduction

This chapter provides an overview of the ISR. It also provides information about using the ISR Dashboard to access and configure the ISR, and includes requirements and recommendations.

About the ISR

Oracle introduces the ISR, Release Version 5.0 to the Interactive Voice Response (IVR) and Telecom industries. Awarded 2008 Communications Solutions Product of the Year Award, the ISR allows any telephony or IVR environment to handle full-duplex call recording (both pre- and post-transfer).

The ISR reliably records any phone call in carrier, enterprise, or contact center. Supporting enterprise & multi-tenant architectures, the ISR provides ad-hoc (partial call) recording allowing any call to be recorded at any point and for any duration. Call recording can be initiated automatically by SIP URI, or conditionally by any authorized VoiceXML or web application. In addition, call data such as time of call, SIP URI, account number, etc. are stored in a recording database for clients to search and review. Once recording starts, recordings can continue after being transferred to an agent or employee thereby providing continuity for recordings & call data across IVR, office, and call center telephony deployments.

Using the ISR, VoiceXML and representational state transfer (REST) application programming interface (API) developers have the ability to record every call, a percentage of calls, specific VoiceXML dialogs as well as transfers to agent conversations. With simple VoiceXML and REST API code, the VoiceXML application controls recording for any call, at any point and for a specific period of time. In addition, every recording may be indexed by key VoiceXML values or identifiers (account#, unique call identifier, SIP URI, time of call, etc.).

The ISR can scale from one call to thousands of concurrent calls and is a simple add-on to any SIP telephony network. An affordable software-based solution, the IP Call Recorder runs on standard Intel-based servers in VoIP and standard telephony environments.

Note: For more information and general specifications and hardware requirements for the ISR, see the Interactive Session Recorder Installation Guide, and the Interactive Session Recorder API Reference Guide.
SIPREC Support

In addition to session call recording via Session Replication for Recording (SRR), the ISR also supports SIPREC.

The SIPREC protocol is used to interact between a Session Recording Client (SRC) and a Session Recording Server (SRS) (a 3rd party call recorder, in this case the ISR’s Record and Store Server (RSS)). It controls the recording of media transmitted in the context of a communications session (CS) between multiple user agents.

SIPREC provides a selective-based call recording solution that increases media and signaling performance on 3rd party call recording servers, more robust failovers, and the ability to selectively record.

The SIPREC feature supports active recording, where the SRC purposefully streams media to the ISR’s RSS acting as the SRS. The SRC and SRS act as SIP User Agents (UAs). The SRC provides additional information to the SRS to describe the communication sessions, participants and media streams for the recording session to facilitate archival and retrieval of the recorded information.

The recording session metadata describes the current state of the recording session and its communication session(s). It is updated when a change of state in the communication session(s) is observed by the SRC. The ISR is responsible for maintaining call history and presenting the history and associated metadata. ISR presents this session metadata, while allowing maintenance and editing of the data along with searching for particular metadata values, through the User Dashboard.

For information on configuring SIPREC on an SBC acting as an SRC, see the Session Director Server Edition User Guide.

About the ISR Dashboard

The ISR Dashboard allows you to access, configure, manage, and monitor the ISR in your network, including:

- Manage Recordings
- Manage Reports
- Manage Settings
- Manage Administrator Functions
  - Manage Realms
  - Manage Accounts
  - Manage Routes
  - Manage Users
  - Manager Sites
  - Manage Authorization Services
- View Live Sessions

Requirements/Recommendations

To use the ISR Administrator Dashboard, the following must be met.

Browser Requirements

Any of the following JavaScript enabled Internet browsers can be used:

- Microsoft® Internet Explorer 9 (IE9) with full regression specifically on IE Version 9.0.8112.16421
• Mozilla Firefox® 8.0
• Google Chrome™ 16.0.912.63
• Other browsers (please contact Oracle Customer Service before using other browsers)

**Recording Playback Recommendations**

To listen to recordings, the following are recommended:

• Quicktime® 7.7.1 Player Plug-in (http://www.apple.com/quicktime/)
• Windows Media Player 10/11

**Note:** In some cases, developers may not include the audio file extension (.wav) on the file name when programmatically naming the file through the VoiceXML API. Windows Media Player 11 plays the file regardless of whether or not the file extension is present.

**Security Features**

The following security features have been implemented in the ISR:

• Optional configuration to force cookies through an encrypted (SSL/TLS) session. For a procedure to enable serving pages with SSL, see Appendix C, Enable Serving Pages with SSL.
• Cache-control set to 'no-cache' to avoid possible storage of sensitive data in local browser
• Enforced stronger password controls
• Ability to configure password expiration, user lockout duration, and maximum failed login attempts.
• Removed "hidden" URLs

**ISR Third-Party Licensing**

For commercial and open-source licensing information regarding the RSS components, execute the following command on any RSS host:

• From the OS-E command line, execute the command `show legal`
• From the RSS shell, execute the command `more /cxc_common/ISR/LEGAL.TXT`

**Note:** Type `q` to exit the legal text display.

For commercial and open-source licensing information regarding the CIS components, execute the following command on any CIS host:

• `more /cxc_common/ISR/LEGAL.TXT`

**Note:** Type `q` to exit the legal text display.
Introduction

This chapter provides information about logging into the ISR Dashboard, editing the Dashboard settings, and using the Dashboard tools while navigating the Dashboard. Dashboard tools include search tools, a download tool, and an import tool for managing information in the ISR database. It is recommended that you review this section before using the ISR Dashboard.

Logging In/Out of the ISR Dashboard

Before you can access the ISR Dashboard, you must have an email address (username) and password provided by your network administrator at the time the ISR was installed in your network. Contact your network administrator for more information.

If your email and password are not available, you can use the following default email and password, and then change the password after logging in:

**Email**: isradmin@acmepacket.com

**Password**: admin123

*Note*: When you login to the ISR Dashboard, depending on your assigned access level, you have access to only your associated ISR Dashboard information. Performance restrictions depend on your login level status. For more information about user login levels, see User Access Levels and Chapter 6, Managing Users.

To login to the ISR Dashboard:

1. Open your Internet Web browser (see compatible browser requirements in the Requirements/Recommendations section.).

2. Enter the following URL in the URL field:
   
   `http://<host name or IP>/`

   *Note*: The host name or IP address you enter here is the name or address assigned to the dashboard VM during installation.

The Login page displays.
3. **Email**—Enter your email (username).

4. **Password**—Enter the password provided by your Administrator at the time of the ISR installation. If this is the first time you are logging in, enter the following and press **Enter**.

   Email: isradmin@acmepacket.com  
   Password: admin123  

   On first-time login, the system prompts you to reset your password.

5. **New Password**—Enter a new password.

   **Note:** Your password must contain at least eight characters and one of the following characters in addition to lowercase letters: Capital letter and/or special character (e.g. @, #, $, etc.)

6. **Confirm Password**—Enter the same password again and click <Update>.

   **Note:** The number of failed attempts before a user is locked out of the ISR can be configured under the Admin > Manage Security Settings link. For more information, see Chapter 6, Managing Users. A message displays with the length of time the User has to wait before attempting to log in again. Contact your Administrator if you forgot your password.

   Upon successful login the first time, the system prompts you to change your password. For security purposes, you should change your password every 45 days.

   After changing your password, the ISR Dashboard Home page (default) displays.
The home page provides all of the options available to a user based on their user type.

This page allows you to perform the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![Find Recordings](icons/find-recordings.png) | **Find Recordings** (or “Recordings” in the main menu) — Allows you to view, play, delete and search recordings currently in the ISR database. Also allows you to download the recording metadata to a comma-separated value (CSV) file. For added convenience, after completing a recording search, you can save the search by assigning it a name. You can also create categories and add recordings to the category as applicable.  

**Note:** Displayed recordings are dependant on the level of logged in user. For more information about user levels, see User Access Levels. For more information about Recordings, see Manage Recordings. |
| ![Build a Report](icons/build-report.png) | **Build a Report** (or “Reports” in the main menu) — Allows you to generate Usage and Billing reports for routes configured on the ISR. These reports display the information in a Bar Graph as well as in a Data Graph.  

**Note:** For more information about Reports, see Manage Reports. |
To logout of the ISR Dashboard:

- Click the Logout icon in the upper-right corner of the page. The ISR Dashboard immediately logs you out.

**User Access Levels**

All users can access the ISR Dashboard. However, the functions available to the logged in user are dependant on the level of access assigned. The following table identifies the functions available at each user level.

**Note:** The “Edit System Configuration” (Admin) menu in the ISR Dashboard displays ONLY for users logged in as Super User.

<table>
<thead>
<tr>
<th>User Type</th>
<th>Find Recordings (Recordings)</th>
<th>Build Reports (Reports)</th>
<th>Edit My Settings (Settings)</th>
<th>Edit System Configurations (Admin)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super User</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (Can manage all)</td>
</tr>
<tr>
<td>Account Administrator</td>
<td>View only. (Permissions to edit/delete must be assigned.)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (Can manage all EXCEPT Super User and sites)</td>
</tr>
<tr>
<td>Tenant Administrator</td>
<td>View own recordings only. (Permissions to edit/delete must be assigned.)</td>
<td>Yes (Reports include info from own accounts only)</td>
<td>Yes</td>
<td>Yes (Can manage own Accounts, Routes, Tenant Admin, Tenant User only)</td>
</tr>
</tbody>
</table>
**Note:** A Remote Archival user is specific to the Remote Archival Webservice only and cannot log into the ISR Dashboard.

For more information about user login levels, see Chapter 6, Managing Users.

### Editing My Settings

The Edit My Settings page (**Settings** in the Main Menu) in the ISR allow you to customize specific elements of the Dashboard for your environment. These settings apply to the current logged in user only. You can configure:

- Dashboard Settings
- Recordings List Settings
- RSS View Settings

- After logging into the ISR Dashboard, click **Edit My Settings** (**Settings** in the Main Menu). The following page displays.
Dashboard Settings

Using the Dashboard Settings, you can:

- Set your preferred time zone
- Set the number of seconds that the pages in the dashboard are refreshed
- Set the number of entries you want displayed per page
- Change your current ISR login password to a new password

To configure the dashboard settings:

1. **Preferred Timezone**—Select the timezone associated with your location or location of the user. This value is an offset of Greenwich Mean Time (GMT). The following table provides the valid values and default for this field.

**Time Zone Table**

<table>
<thead>
<tr>
<th>Time Zone</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMT-11</td>
<td>NT - Nome</td>
</tr>
<tr>
<td>GMT-10</td>
<td>AHST - Alaska-Hawaii Standard</td>
</tr>
<tr>
<td></td>
<td>CAT - Central Alaska</td>
</tr>
<tr>
<td></td>
<td>HST - Hawaii Standard</td>
</tr>
<tr>
<td>GMT-9</td>
<td>YST - Yukon Standard</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Location</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| GMT-8     | PST - Pacific Standard  
Los Angeles, CA, USA |
| GMT-7     | MST - Mountain Standard |
| GMT-6     | CST - Central Standard  
Mexico City, Mexico  
Saskatchewan, Canada |
| GMT-5 (default) | EST - Eastern Standard  
Bogota  
Lima, Peru  
New York, NY, USA |
| GMT-4     | AST - Atlantic Standard  
Caracas  
La Paz |
| GMT-3     | Brasilia, Brazil  
Buenos Aires, Argentina  
Georgetown, Guyana |
| GMT-2     | AT - Azores |
| GMT-1     | WAT - West Africa  
Azores, Cape Verde Islands |
| GMT       | London, England  
Dublin, Ireland  
Edinburgh, Scotland  
Lisbon, Portugal  
Reykjavik, Iceland  
Casablanca, Morocco |
| GMT+1     | CET - Central European  
Paris, France  
Berlin, Germany  
Amsterdam, The Netherlands  
Brussels, Belgium  
Vienna, Austria  
Madrid, Spain  
Rome, Italy  
Bern, Switzerland  
Stockholm, Sweden  
Oslo, Norway |
| GMT+2     | EET - Eastern European  
Athens, Greece  
Helsinki, Finland  
Istanbul, Turkey  
Jerusalem, Israel  
Harare, Zimbabwe |
| GMT+3     | BT - Baghdad  
Kuwait  
Nairobi, Kenya  
Riyadh, Saudi Arabia  
Moscow, Russia |
| GMT+4     | Abu Dhabi, UAE |
2. **Refresh Rate (seconds)**—Select the number of seconds that the dashboard waits before refreshing the recordings list. Valid values are:

- None (default)
- 2 minutes
- 30 seconds
- 5 minutes
- 1 minute

3. **Display Entries Per Page**—Enter the number of entries per page to display on the Recordings page. For example, entering a value of “7” in this field displays 7 recording entries per page in the Recordings List. Valid values are 1 to 255. Default is 10.

4. **Current Password**—Enter the current password you use to log into the Dashboard. Valid values are up to 256 alpha-numeric characters.

5. **New Password**—Enter your new password for logging into the Dashboard. Valid values are a combination of at least 8 characters and must include either one case-sensitive letter and/or special character (e.g. @, #, $, etc.).

6. **Confirm Password**—Reenter your new password to confirm the new Dashboard password.

7. Click **Change Password** to save the changes. A message, “Successfully changed” displays when the change is successful.
8. Click **Save** to save the dashboard settings.

**Recordings List Settings**

Using the Recordings List Settings, you can customize the columns that display on the Recordings List page.

You can select the column heading(s) from the “Not Displayed” column and drag it to the “Displayed” column. After clicking <Save>, the headings in the “Displaying” column display on the Recordings List page.

To configure the Recordings List settings:

1. To add a heading to the display list, in the “Not Displayed” column (red boxes), click on a heading and drag the selection to the “Displaying” column. The red box you placed in the “Displaying” column turns green.

   To remove a heading from the display list, in the “Displaying” column (green boxes), click on a heading and drag the selection to the “Not Displayed” column. The green box you placed in the “Not Displayed” column turns red.

   **Note:** You can place a maximum of 5 headings in the “Displaying” column.

The following table describes the headings you can select to display in the Recordings list.

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time (default)</td>
<td>Displays the date and time the recording started. This column is based on the user’s GMT offset and is in the format MM/DD/YY HH:MM:SS (AM or PM).</td>
</tr>
<tr>
<td>From (default)</td>
<td>The number that the caller dialed from (i.e., Caller ID).</td>
</tr>
<tr>
<td>To (default)</td>
<td>Displays the number that the caller dialed.</td>
</tr>
<tr>
<td>Duration (default)</td>
<td>Displays the length of the recording (in seconds)</td>
</tr>
<tr>
<td>File Name</td>
<td>Displays the file name associated with the recording.</td>
</tr>
<tr>
<td>Session ID</td>
<td>Displays the Session ID derived from the X-ISR-UCID.</td>
</tr>
<tr>
<td>Agent ID</td>
<td>Displays the ID of the Agent answering the call.</td>
</tr>
<tr>
<td>RSS Egress Call ID</td>
<td>Displays the unique egress call ID derived from the call-id used in the egress call leg for the recording (only used in pass-thru mode).</td>
</tr>
<tr>
<td>RSS Ingress Call ID (default)</td>
<td>Displays the unique ingress call ID derived from the call-id received in the initial SIP INVITE.</td>
</tr>
</tbody>
</table>
2. Click **Save** to save the recordings list settings.
   The headings listed in the Displaying column (green boxes) display as column headings on the Recordings List page.

<table>
<thead>
<tr>
<th><strong>Heading</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Field 1 - 4</td>
<td>Displays the unique set of meta-data associated with the recording (i.e., Transaction ID, Account Number, Unique Call ID) for custom fields 1 through 4, as defined in the recording policy and added via API.</td>
</tr>
<tr>
<td><strong>Rating</strong></td>
<td>Displays the score assigned to a recording by a reviewer. Scoring is based on 1 to 5 stars.</td>
</tr>
<tr>
<td><strong>Account</strong></td>
<td>Displays the name of the account to which the recording belongs.</td>
</tr>
</tbody>
</table>

**RSS View Settings**

Using the RSS View Settings, you can:

- Set the maximum entries to include in the RSS error logs.

**To configure the RSS view settings:**

3. **Max Error Log Entries**—Enter the number of entries to show on each RSS error log page. Valid values are numeric characters. Default is 20.

4. Click **Save** to save the RSS view settings.
**Help Link**

Online support is available for the ISR Dashboard. You can click on the Help link in the upper right corner of any page in the Dashboard to display help.

Clicking the Help link displays the following window.

![Help Window](image)

**Note:** Help Text is customizable for each account. For more information on Dashboard branding, see Account Branding in Chapter 3.

If you can’t find answers to your questions using the *Interactive Session Recorder Administrator Guide*, please open a ticket with your question(s) using the Oracle Support Portal at [https://support.acmepacket.com](https://support.acmepacket.com). Specify the appropriate information in the ticket pertaining to your question(s) as described in the help window.
Dashboard Tools

The ISR Dashboard provides various tools that allow you to perform specific functions on each page.

- Function Icons
- Paging Tool
- Search Tools
- Column Sorting Tool
- Download Tool
- Import Tool
- Export Tool

Functional Icons

The ISR Dashboard has various icons that perform specific functions. The following table describes each functional icon.

<table>
<thead>
<tr>
<th>Functional Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logoff</td>
<td>Allows you to logout of the ISR Dashboard.</td>
</tr>
<tr>
<td>Help</td>
<td>Displays information about contacting Technical Support for help with the ISR Dashboard.</td>
</tr>
<tr>
<td>Add</td>
<td>Adds a new item to a list</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes an item from the list</td>
</tr>
<tr>
<td>Play</td>
<td>Immediately opens and plays a “.wav” file recording stored in the ISR database.</td>
</tr>
<tr>
<td>Note: When you click the “Play” icon, the Dashboard offers the file to the applicable browser you currently have open. The browser determines the file type of the file and opens the media player according to the “player plugin” settings in the browser. The Dashboard ensures the play element is recognizable by all supported browsers (Chrome, Internet Explorer, Firefox).</td>
<td></td>
</tr>
<tr>
<td>Download</td>
<td>Downloads a recording from the recording list to your PC. You can choose to immediately play the recording or save the recording file to your PC.</td>
</tr>
<tr>
<td>Details</td>
<td>Displays additional details about the item in the list. Some items allow for additional editing after clicking this tool.</td>
</tr>
</tbody>
</table>
Paging Tool

The ISR Dashboard provides a paging tool to help you navigate through pages if the data that displays is greater than the number set for the Setting->Display Entries per Page parameter.

**Note:** This paging tool displays ONLY if the elements in the list require more than one page for display. For more information about setting the display entries per page, see Editing My Settings.

You can click on “Next” to move to the next page, or “Previous” to move to the previous page. If more than one page exists, the number for each page displays with the navigation tools. You can click on any page number to display the data on that page.

Search Tools

The ISR Dashboard provides a search tool you can use to search for specific information in the ISR database. The search feature is applicable to:

- Recordings
- Routes

Basic Search for Recordings

You can search for a specific recording in the ISR database, or you can perform an advanced search for a group of recordings.

**To perform a basic search for a recording:**

1. Click Recordings in the main menu (or Find Recordings on the Home page). A list of recordings stored in the ISR database display.
2. In the drop-down box (at the top-right of the Recordings page), select the information about the recording(s) that you want to search. Valid values are:
   - From - ID of the caller for this call.
   - To - ID of the recipient for the call.
   - Session ID - Session ID derived from the X-ISR-UCID
   - File Name - File name of the recording. This is the file name assigned by the system or by the developer who invoked the recording.
   - Agent ID - ID of the agent that answered the call. This is the value set by the API, or by a User.

3. In the text box, enter the information required dependant on the selection you made in Step 2. Valid values are alpha-numeric characters.
   For example, if you selected “From” in the drop-down box, enter the ID of the caller associated with a recording for which you want to search. All the recordings associated with that caller ID display in a list.

   **Note:** You can select a recording and click on the Details icon to reference the “Session ID”, “From”, and “To” information for the recording if required.

4. Click `<Search>` to find all recordings based on the search criteria. All matching recordings display in the recordings list.

   **Note:** The result is an exact match. This feature does not support wildcard matching.

### Advanced Search for Recordings

You can perform more advanced searches for recordings to display more detailed information if required.

**To perform an advanced search for a recording:**

1. On the Recordings page, click **advanced search**.
   The following dialog box displays.
2. **Search Mode**—Select whether to perform the search using **AND** or **OR**.
   - **AND**—Returns results where recordings match **ALL** fields you specify. For example, if you specify From as “123”, File Name as “Recording1”, and Agent ID as “2”, then the results of the search show all recordings with a value of “123” in the From field, AND file name of “Recording1”, AND Agent ID of “2”.
   - **OR**—Returns results where recordings match any one of the fields you specify. For example, if you specify From as “123”, File Name as “Recording1”, and Agent ID as “2”, then the results of the search show any recordings with a value of “123” in the From field, OR a file name of names or “Recording1”, OR an Agent ID of “2” (OR a result that includes all of these).

3. **Partial Match**—When enabled, the ISR finds recordings that partially match the values entered in the search fields.

4. **Session ID**—Enter the unique Session ID derived from the X-ISR-UCID on which to perform the search.

5. **From**—Enter the From SIP URI to perform the search on. Valid values are alpha-numeric characters and may include the “@” or “:” characters.

6. **To**—Enter the To SIP URI to perform the search on. Valid values are alpha-numeric characters and may include the “@” or “:” characters.

7. **Label**—Enter the route label to perform a search on.

8. **Search Date**—Select whether you want to search for recordings **By Relative** or **By Range**:
   - **By Relative**—Allows you to perform a recording search, based on the information you specified in the previous fields AND by recordings that happened “Today” (default), the “Last 7 Days”, or the “Last 30 Days”.
   - **By Range**—Allows you to perform a recording search, based on the date range you specify.

9. If you select a Search Date by **Range**, enter the **“From Date”** and **“To Date”** in the format MM/DD/YYYY, or click on the calendar icon next to the text box to select the dates for which you want to search for recordings.

   In the “From Time” and “To time” boxes, select the time in the format HH:MM for which you want to search for recordings. Valid values for hours are 00 to 23. Valid values for minutes are 00 to 59.

   **Note:** For convenience, clicking in the text box displays a pop-up calendar for which you can select the month, day, and year.

10. Click `<Search>` to find all recordings based on the search criteria. All matching recordings display in the recordings list.
You can perform recording searches based on additional search criteria as follows.

**To perform a more advanced search for recordings:**

1. In the Advanced Search dialog box, click **More Recording Search Options** to expand the dialog box.

2. **File Name**—Enter the file name of the recording. This is the file name assigned by the system or by the developer that invoked the recording. Valid values are alpha-numeric characters and may include the "@" or "." characters.

3. **Duration Min**—Enter the beginning time, in seconds, of a recording. Valid values are numeric characters. For example, 15.

4. **Duration Max**—Enter the ending time, in seconds, of a recording. Valid values are numeric characters. For example 24.

   Using the examples in Steps 3 and 4, the results include all recordings that had a length of time between and including 15 and 24 seconds.

5. **Agent ID**—Enter the ID of the agent that answered the call. This is the value set by the API or by a User. Valid values are alpha-numeric characters.

6. **RSS Ingress Call ID**—Enter the unique ingress call ID derived from the call-id received in the initial SIP INVITE.

7. **RSS Egress Call ID**—Enter the unique egress call ID derived from the call-id used in the egress call leg for the recording, if using pass-thru mode.

8. **Custom Field [1-4] Data**—Enter the unique set of metadata associated with the recordings for which you are searching. These fields identify the customized data defined by the API (for example, Transaction ID, Account Number, Unique Call ID, etc.). The results of this field display all recordings associated with the values you enter in this field(s). Valid values are alpha-numeric characters.

9. **Categories**—Enter the name of the category for which you want to search for recordings. The category you enter in this field must already exist in the database. Valid values are alpha-numeric characters. For more information about creating and searching categories, see Recording Details.

10. Click **Search** to find all recordings based on the search criteria. All matching recordings display in the recordings list.
Recording Search by Session

You can search for recordings by session criteria if required.

To search for recordings based on session criteria:

1. In the Advanced Search dialog box, click **By Session Search Options** to expand the dialog box.

2. **SIPREC Session ID**—Enter the SIP recording session ID number for which you want to search. Valid values are alpha-numeric characters.

   **Note:** You can select a recording and click on the Details icon to reference the “SIPREC Session ID” information for the recording if required.

3. **Participant AOR**—Enter the participant’s address of record (AOR) associated with the call that was recorded. Valid values are alpha-numeric characters.

4. **apkt:ucid**—Enter the Universal Call ID (UCID) of the incoming caller. Valid values are alpha-numeric characters.

5. **extTrackingID**—Enter the external tracking ID that was used when an incoming call was transferred to another recipient. Valid values are alpha-numeric characters.

6. **ServiceProviderID**—Enter the Service Provider ID that was used on the incoming call. Valid values are alpha-numeric characters.

7. **userId**—Enter the user ID on the incoming call. Valid values are alpha-numeric characters.

8. **groupId**—Enter the group ID on the incoming call. Valid values are alpha-numeric characters.

9. **callID**—Enter the call ID of the incoming call. Valid values are alpha-numeric characters.

10. **callingPartyNumber**—Enter the source number of the incoming call. Valid values are alpha-numeric characters.

11. **calledPartyNumber**—Enter the destination number of the incoming call. Valid values are alpha-numeric characters.
12. **newExtTrackingID**—Enter the new external tracking ID that was used when an incoming call was transferred a second time to another recipient. Valid values are alpha-numeric characters.

   **Note:** The extTrackingID, ServiceProviderID, userID, groupId, callID, callingPartyNumber, calledPartyNumber, and newExtTrackingID parameters are specific to a SIPREC integration with Broadsoft’s Broadworks platform and may not be shown in all installations.

13. **apkt:in-realm**—Enter the name of the ISR realm that received the SIPREC session (in-realm). Valid values are alpha-numeric characters.

14. **apkt:P-Asserted-Identity**—Enter the remote party’s ID in the SIPREC session. The ISR uses the P-Asserted-Identity header field to convey the proven identity of the originator of a request within a trusted network. Valid values are alpha-numeric characters.

15. **apkt:Diversion**—Enter the call forwarding phone number from the SIPREC session, to which the incoming call was diverted. Diversion is a call forwarding feature that lets an incoming call to a called party be redirected to a third party. Valid values are alpha-numeric characters.

16. **apkt:request-uri**—Enter the Uniform Resource Identifier (URI) in the header of the request message of the SIPREC session. The URI in the request message contains sufficient information to initiate and maintain the SIPREC communication session. Valid values are alpha-numeric characters.

17. Click **Search** to perform the search based on the recording session parameters you specified. All matching recordings display in the recordings list.

   **Note:** Session search parameters are applied in addition to any other search options defined, including date ranges.

---

**Basic Search for Routes**

You can perform a basic search for Routes configured in the ISR database based on the route pattern.

**To perform a basic search for a route:**

1. Click **Admin** in the main menu (or **Edit System Configurations** on the Home page).
2. Click **Manage Routes**. A list of routes display in the routes list.

3. In the drop-down box (on the upper-left of the page), select the account for which you want to search for a route(s).

   **Note:** The values in the drop-down box include any accounts you’ve added to the ISR database.
4. In the text box (on the upper-right of the page), enter the route pattern for which to search. This field does not support partial matches.

5. Click **Search** to perform the search based on the criteria you specified. All matching routes display in the routes list.

**Column Sorting Tool**

In the ISR Dashboard, you can sort the list of recordings in ascending or descending order by clicking the column heading.

To sort the recording data in the recording list:

- Click any of the column headings to sort that column in ascending or descending order. The Up Arrow icon indicates the column is currently in ascending order. The Down Arrow icon indicates the column is in descending order.

**Download Tool**

You can download a single specific recording file for playing immediately, or save the recording (.wav file) to a storage location on your PC to listen to later. You can also download the metadata for all recordings in the recording list to a CSV file on your PC.

**Downloading a Single Recording File**

You can download a single recording file to play immediately, or save the recording to your PC to play later.

To download a single recording file:

1. Click **Recordings** (or **Find Recordings** on the Home page). The recordings list displays.
2. Select a recording and click the Download icon for that recording. The following dialog box displays.

![Dialog box screenshot]

This is going to be the name of the file and is not consistent. The ISR stores the file in a temporary folder on your computer.

3. Click “Open with” and select the application for which to play the .wav recording file or click “Save File” to save the .wav recording file to a location on your PC for listening to later.

**Note:** If you click the Download icon more than once for the same recording, additional copies of the same file are saved, appending a numerical digit to the file name. For example:

“rss_g711-24-1841@172.30.58.237(1).wav”,
“rss_g711-24-1841@172.30.58.237(2).wav”,
“rss_g711-24-1841@172.30.58.237(3).wav”, etc.

4. Click OK. Your browser immediately opens and plays the .wav file, or downloads it to your PC for listening later.

**Downloading a Recording List to a CSV File**

You can download the metadata for up to 10,000 recordings from the local ISR database, to a comma separated value (CSV) file (<filename>.csv), and then open the file for viewing using an application that recognizes the CSV format (i.e., Notepad®, Microsoft® Excel, etc.). The resulting file contains the details of each recording (not the actual audio recording).

**Note:** This feature limits the download to 10,000 recordings. Therefore, if the Recordings List exceeds 10,000 recordings, you must perform a search to create a list of results containing less than 10,000 recordings before downloading to a CSV file.

To download a recording list’s metadata to a CSV file:

1. On the Recordings page, click **Download as CSV file** to download the current list of recordings to a CSV file.

2. **Include Details**—Place a checkmark in the check box to include all details about the recording in the CSV file.

**Note:** If you click **Download as CSV file** without checking the **Include Details** box, the ISR Dashboard only downloads the information in the columns that currently display in the recordings list. If you place a checkmark in the **Include Details** box, the ISR Dashboard includes all column attribute information not listed in the current recording list.
The following dialog box displays.

The ISR automatically provides a filename of “recordingResults.csv” and stores the file in a temporary folder on your computer.

3. Click **Open with** and select the application for which to open the resulting CSV file. or
   Click **Save File** to save the CSV file to your PC.

   **Note:** If you choose Save File, and you click **Download as CSV file** more than once, each time the ISR generates a CSV file, it appends a numerical digit to the file name. For example:

   “recordingResults(1).csv”
   “recordingResults(2).csv”
   “recordingResults(3).csv”

4. Click **OK**. The CSV file opens with the application you specified, or saves the file to your PC for viewing later.

**Example CSV file with recordings and no detail specified**
Example CSV file with recordings and detail specified

<table>
<thead>
<tr>
<th>Column Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To</td>
<td>Specifies the To SIP URI. This is the URI from where the call session was coming.</td>
</tr>
<tr>
<td>Time</td>
<td>Specifies the starting GMT time and date of the recording in the format MM/DD/YY HH:M:SS, respectively. Note: In the date format, M = month, D = day, and Y = year. In the time format, H = hours, M = minutes, S = seconds.</td>
</tr>
<tr>
<td>Session ID</td>
<td>Specifies the Session ID assigned to the incoming call. Format is specified as xisr-ucid=&lt;session id&gt;@&lt;local host&gt;.</td>
</tr>
<tr>
<td>Rating</td>
<td>Specifies the score assigned to a recording by a reviewer and can be assigned as needed by your organization. Scoring is based on 1 to 5 stars.</td>
</tr>
<tr>
<td>RSS Ingress Call ID</td>
<td>Specifies the call ID assigned by the RSS to the incoming call.</td>
</tr>
<tr>
<td>RSS Egress Call ID</td>
<td>Specifies the call ID assigned by the RSS to the outgoing leg of the call (pass-thru mode only).</td>
</tr>
<tr>
<td>Notes</td>
<td>Specific notes, if any, entered by users through the dashboard.</td>
</tr>
<tr>
<td>Hours</td>
<td>Specifies the length of time, in hours, a user spent reviewing, transcribing, and commenting on the recording.</td>
</tr>
<tr>
<td>From</td>
<td>Specifies the From SIP URI. This is the URI from where the call session was coming.</td>
</tr>
<tr>
<td>File Name</td>
<td>Specifies the name of the recording file.</td>
</tr>
<tr>
<td>Duration</td>
<td>Specifies the length of the recording (in milliseconds).</td>
</tr>
<tr>
<td>Custom Fields 1 - 4</td>
<td>Specifies a unique set of meta-data associated with the recording (i.e., Transaction ID, Account Number, Unique Call ID).</td>
</tr>
<tr>
<td>Completed</td>
<td>Specifies whether or not this recording resulted in a complete transaction, added by the dashboard user.</td>
</tr>
<tr>
<td>Agent ID</td>
<td>Specifies the ID of the Agent answering the call.</td>
</tr>
</tbody>
</table>
Import Tool

The ISR allows administrators to specify account and/or route parameters in a comma separated value (CSV) file, save the file, and then import the information into the ISR database using the ISR Dashboard. An administrator can use any application that can save to a CSV file (i.e., Microsoft® Excel, Notepad®, etc.) when inputting the account and/or route information into the file.

**Note:** The import tool is for Super User and Account Administrators only.
Managing Realms/Accounts

Introduction

This chapter introduces the functions available to the Administrator in the ISR Dashboard. It also includes information about adding, editing, and deleting realms and accounts from the ISR database.

Administrator Menu

The ISR Dashboard provides a menu that allows Administrators to manage realms, accounts, routes, users, sites, authorization services, and live sessions on the ISR.

This menu displays for a Super User, Account Administrator, and a Tenant Administrator only. However, the Admin menu is limited for the Account Administrator and the Tenant Administrator.

The following table describes the Administrator features available for each level of administrator.
### Administrator Menu by User Level

<table>
<thead>
<tr>
<th>Superuser</th>
<th>Account Administrator</th>
<th>Tenant Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Manage Realms</td>
<td>• Manage Realms</td>
<td>• N/A</td>
</tr>
<tr>
<td>• Manage Accounts</td>
<td>• Manage Accounts</td>
<td>• Manage Accounts (own accounts only)</td>
</tr>
<tr>
<td>• Manage Routes</td>
<td>• Manage Routes</td>
<td>• Manage Routes (own routes only)</td>
</tr>
<tr>
<td>• Manage Recording Format Profiles</td>
<td>• Manage Recording Format Profiles</td>
<td>• N/A</td>
</tr>
<tr>
<td>• Manage Authorization Services</td>
<td>• Manage Authorization Services</td>
<td>• N/A</td>
</tr>
<tr>
<td>• Manage Users</td>
<td>• Manage Users (Account Admin, Tenant Admin, and Tenant User only)</td>
<td>• Manage Users (Tenant Admin and Tenant User only)</td>
</tr>
<tr>
<td>• Manage Security Settings</td>
<td>• Manage Security Settings</td>
<td>• N/A</td>
</tr>
<tr>
<td>• Manage Sites</td>
<td>• Manage Sites</td>
<td>• N/A</td>
</tr>
<tr>
<td>• Live Sessions</td>
<td>• Live Sessions</td>
<td>• N/A</td>
</tr>
</tbody>
</table>

The following paragraph provides information and procedures for adding, editing, and deleting a realm(s).

### Manage Realms

A realm is a logical way of identifying a domain, a network, a collection of networks, or a set of addresses. Realms are used when a SBC communicates with multiple network elements over a shared intermediate connection. Realms allow for flows to pass through a connection point between two networks.

From an external perspective, a realm is a collection of systems that generates realtime interactive communication sessions comprised of signaling messages and media flows, or a group of multiple networks containing these systems.

From an internal perspective, a realm is associated with SBC configurations to define interfaces and resources in a logical way. Realms are used to support policies that control the collection of systems or networks that generate media sessions.

In the ISR Dashboard, an Administrator can now add, edit, and delete realms using the “Manage Realms” option on the Admin Menu. After adding a realm, you can then associate an account to that realm. An account can have multiple associated realms and a realm can have multiple associated accounts.

**Note:** The configured realm must already exist in the SBC before adding it to the ISR.

### How Realm-based Recording Works

The ISR performs recording affiliation and route-matching based on the configured route pattern and the associated realm. The ISR only inspects incoming SIPREC INVITEs for the inclusion of a realm label within the SIPREC extension data. If a realm label exists, it is used to search any configured routes associated with an account(s) in the matching
realm. The RSS looks for a To/From match (similar to the way lookups are performed) in the realm's configured accounts and routes.

The following flow diagram illustrates how the ISR perform realm-based recording.

When **adding** a realm, the ISR checks for a wildcard “%” character in the “Realm Label”. If the wildcard exists, an error message displays. If a wildcard does not exist, the realm is added.

**Deleting** a realm removes all associations to accounts in the ISR database. The ISR compares the deleted routes of the realm with the routes not in a realm. If there are routes of the same type and pattern in both locations, an error displays and the delete function fails.

In Realm **edit** view, the associated account(s) in the realm display. In the Accounts edit view, the realm(s) associated with the account display only after adding an associated realm(s) to the ISR.

The following rules apply when associating an account(s) to a realm:

- You can associate multiple accounts to a single realm. Routes created on these accounts must have unique route patterns across the related accounts.
- Wildcard routes:
  - are treated like normal 'pattern' routes. They are unique across realms and accounts.
  - can have any priority.
  - if set with a higher priority than a 'distinct' route, the Dashboard displays a warning that the user is about to set a wildcard route higher than the list of lower priority routes, and prompts the user to confirm whether or not to continue.
- You cannot configure wildcard realms.
• Associating a realm with an account(s) is optional. Routes created across accounts with no realms must be unique. This allows the ISR to support legacy (non-SIPREC) installations, as well as maintain compatibility with other SIPREC compliant Session Recording Clients (SRCs).

Use the **Manage Realms** option on the Admin page to manage Realms.

![Realms Page](image)

The following table describes the columns on the Realms page.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Label name assigned to the Realm.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the Realm.</td>
</tr>
<tr>
<td></td>
<td>Displays details about a Realm and allows you to edit the details if required.</td>
</tr>
<tr>
<td></td>
<td>Deletes the Realm.</td>
</tr>
</tbody>
</table>

**Adding a Realm**

You can add a realm to the ISR database using the **New Realm** link on the Realm page. You can then associate an account to that realm.

**To add a realm:**
1. After logging into the ISR Dashboard, click **Admin** in the main menu (or **Edit System Configurations** on the Home page).

2. Click **Manage Realms**. The Realms page displays.

3. Click **New Realm**. The following dialog box displays.

4. **Label**—Enter the name of the realm to add to the ISR database. Valid values are alpha-numeric characters.

5. **Realm Description**—(optional) Enter a description for the realm you are adding. Valid values are alpha-numeric characters.

6. Click **Create**. The realm you added displays in the Realms page.

**Associating an Account to a Realm**

You can associate an account to any realm that exists in the ISR database.

**To associate an account to a realm:**
1. On the Realms page, select a realm and click the Details icon. The Edit Realm dialog box displays.

2. Click **Realm Accounts** to expand the realms page.

3. **Select an Account to add**—Select an account from the drop-down box and click the Add icon. The following prompt displays.

   “Are you sure you want to add this account?”

4. To add the account to the realm, click **Yes, Continue** or to cancel the add function, click the X in the upper-right corner of the prompt box.

   If you add an account, the account information displays in the “Realm Accounts” page. All routes associated with the account also display in the “Realm Routes” page.

   ![Realm Accounts and Realm Routes](image)

   You can edit these routes if required. For more information about editing routes, see Configuring/Editing Details of a Route.

**Editing a Realm**

You can edit the realm label and description if required.

**To edit a realm:**

- On the Realms page, select the realm you want to edit and click the Details icon.
- Click **Edit** in the realm details.
- Make the necessary changes to the realm label and description.
- Click **Update** to save the changes.

![realm edit screen](image)
1. On the Realm list page, select a realm and click the Details icon. The Edit Realm dialog box displays.

2. **Label**—Edit the name of the realm. Valid values are alpha-numeric characters.

3. **Realm Description**—Edit the description of the realm. Valid values are alpha-numeric characters.

4. Click **Update**. The following message displays when an updated is successful. “Applied updated successfully”.

Deleting a Realm

You can delete a realm if required.

**To delete a realm:**

1. On the Realm list page, select a realm and click the Delete icon.

The following message displays:

“Are you sure you want to delete this Realm?”

2. Click **Continue** to delete the selected realm or click the X in the upper right corner of the box to cancel the delete function.

   If you clicked **Continue**, the Realm deletes from the ISR database and from the Realm list page.
Manage Accounts

Use the **Manage Accounts** on the Admin Menu of the ISR Dashboard to manage accounts in the ISR network.

The Accounts page in the ISR Dashboard allows you to add new Account(s) and configure account parameters. This function also allows you to view, edit, and delete existing Accounts on the ISR.

For each account, you can configure account branding and configure route defaults. You can configure multiple accounts (supports multi-tenancy) if required, and assign specific users or edit user parameters for each account.

**Note:** A default “System” Account exists under the Accounts page and should not be renamed or deleted. This account includes all users and routes configured on the ISR. Users assigned as Super Users and Account Administrators can edit the System Account. For more information about users, see Chapter 6, Managing Users.

You can also use other applications (i.e., Microsoft® Excel, Notepad®) to specify the parameters for an account, and then import the contents of the file into the ISR Dashboard.
The following table describes the columns on the Accounts page.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the account.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the account.</td>
</tr>
<tr>
<td>Number of Routes</td>
<td>Number of routes configured for the account.</td>
</tr>
<tr>
<td>Record</td>
<td>Identifies whether or not recording is enabled or disabled on the account.</td>
</tr>
<tr>
<td></td>
<td>- Recording is enabled.</td>
</tr>
<tr>
<td></td>
<td>- Recording is disabled.</td>
</tr>
<tr>
<td>Sessions Capacity</td>
<td>Total number of available sessions currently allowed for this account.</td>
</tr>
<tr>
<td></td>
<td>- Displays details for the account and allows you to edit the details.</td>
</tr>
<tr>
<td></td>
<td>- Deletes the account.</td>
</tr>
</tbody>
</table>

### Adding an Account

You can add an account(s) in the ISR Dashboard using the **New Account** link on the Accounts Page. After adding an account, the settings are applied as the default settings for all routes under that account.

**Note:** You can create an account using any application that can save to a comma separated value (CSV) file (i.e., Microsoft® Excel, Notepad®, etc.). Using the ISR Dashboard, you can then import the account information from the file (`<filename>.csv`) to the ISR database.

For more information about importing account information into the ISR database, see Chapter2, Importing an Account CSV File.

**Note:** Only a Superuser and Account Administrator can add new accounts.

**To add an account:**

1. After logging into the ISR Dashboard, click **Admin** in the main menu (or **Edit System Configurations** on the Home page).
2. Click **Manage Accounts**. The Accounts page displays.
3. Click **New Account**. The following dialog box displays.

![New Account Dialog Box]

4. **Account Name**—Enter an account name for this account. Valid values are alphanumeric characters.

5. **Account Description**—Enter a description for this account. Valid values are alphanumeric characters.

6. **Account Miscellaneous**—(optional) Enter any miscellaneous notes about the account. Valid values are alphanumeric characters.

7. **Recording is**—Select whether or not to enable recordings on this account. Valid values are:
   - Enabled (default)
   - Disabled

8. **Sessions Capacity**—Enter the maximum number of call recording sessions simultaneously available for routes to use on this account. When the maximum session capacity is reached across all routes on the account, a recording may indicate to the caller that all lines are busy and to call back at another time. Valid values are:
   - 1 to 999999999 (must indicate total number of licensed sessions)
   - -1 indicates no limit (default)

   **Note:**
   - After you create an account, you can also set the number of additional ports available for routes to use (Additional Burst Ports) after the maximum number of ports have been used up. For more information about setting Additional Burst Ports, see Account Route Defaults.
   - The Session Limit for New Account data and the Additional Burst Session data are shown separately in Recording Usage Reports and are subject to your licensing agreement.

9. Click **Create** to create the new account. The new account displays on the Accounts page.

### Configuring/Editing Details for an Account

Superusers and Account Administrators can configure or edit the details for any of the accounts on the Accounts page. Tenant Administrators can configure or edit the details for their own accounts only.

After selecting an account on the Accounts page, you can perform the following:

- Edit general account information
- Configure or edit branding features to the account
- Configure or edit account route defaults
- View the routes associated with the account (if any)
**Edit General Account Information**

You can edit the general information for an account when required.

**To edit the general account information:**

1. On the Admin page, click **Manage Accounts**. The Accounts page displays.
2. Select an account from the list and click the Details icon. The following dialog box displays.

3. **Account Name**—Edit the account name. Valid values are alpha-numeric characters.
4. **Account Description**—Edit the description for this account. Valid values are alpha-numeric characters.
5. **Account Miscellaneous**—(optional) Edit any miscellaneous notes about the account. Valid values are alpha-numeric characters.
6. **Recording is**—Select whether or not to enable recordings on this account. Valid values are:
   - Enabled (default)
   - Disabled
7. **Session Capacity**—Edit the maximum number of call recording sessions simultaneously available for routes to use on this account. When the maximum session capacity is reached across all routes on the account, a recording may indicate to the caller that all lines are busy and to call back at another time. Valid values are:
   - 1 to 999999999 (must indicate total number of licensed sessions)
   - -1 indicates no limit (default)

**Note:**

- The maximum session limits for an Account are subject to your licensing agreement.
- After you create an account, you can set the “Additional Burst Sessions” available for routes to use after the maximum number of sessions have been used up. For more information about setting Additional Burst Ports, see Route Capacity Defaults.
- The maximum session limit and the available burst session data is included in the Usage and Billing Reports. For more information about generating reports, see Chapter 10, Managing Reports.

8. Click **Update** to save the changes to the account.

**Account Branding**

You can customize the ISR Dashboard for each account if required, using the Account Branding feature. Branding the ISR Dashboard includes:

- customizing the Dashboard’s header and footer color.
- specifying a logo to display for each account.

**To apply branding to an account:**

1. On the Admin page, click **Manage Accounts**.
2. Select an account from the Accounts page and click the Details icon for that account.
3. Click **Account Branding** to expand the branding information.

4. In the **Header/Footer Color** field, click on [ ] and select the company color to apply to the Header and Footer, as well as all the button names in the ISR Dashboard. Or enter the Company’s color code, in Hex format, in the text box. For example, #F4AB00.

5. **Logo**—Enter the file name of the Company logo you want to apply to the header of all the screens in the ISR Dashboard. If required, you can specify the path name where the file is currently stored. For example, images/Company.png.

6. **Admin Help**—Enter any help information that you want to display when an Administrator clicks the Help icon from any page in the ISR Dashboard. Valid values are alpha-numeric text characters or HTML code. For example:

   “For help or support, contact ABC, Inc. via support@abc.com”.

   The default message in the ISR is:

   “Online Support is available for this product. For questions and problems that cannot be answered by our documentation, please open a ticket through the Oracle Support Portal: https://support.acmepacket.com”.

   **Note:** In the “Admin Help” and “User Help” fields, you can resize the text box as required by right-clicking and holding your mouse button on the bottom-right corner of the box, and dragging it to the size you require.
7. **User Help**—Enter any help information that you want to display when a User clicks the Help icon from any page in the ISR Dashboard. Valid values are alpha-numeric text characters or HTML code. For example:

“For help or support, contact ABC, Inc. via support@abc.com”.

The default message in the ISR is:

“Online Support is available for this product.
For questions and problems that cannot be answered by our documentation, please open a ticket through the Oracle Support Portal:

https://support.acmepacket.com”.

8. **Max Recording Entries in List View**—The maximum number of recording entries that the Dashboard searches for in the Recordings List View. The default value is 10000.

9. **Max Recording Entries in CSV Download**—The maximum number of recording entries that the Dashboard searches for when preparing a CSV file for download. The default value is 10000.

10. Click **Preview** to verify the color and logo changes before saving.

11. Click **Update** to save the changes. The color and logo you specify display on the screens in the ISR Dashboard. The following screen illustrates the branding configuration.

---

**Account Route Defaults**

The Account Route Defaults on the Accounts page is applied as the default settings for all routes under the selected account. This page allows you to configure:

- Recording Defaults
- Recording Editing Permissions
- Announcement and Recurring Beep Defaults
- Conference Mode Defaults
- Record and Save Mode Defaults
- Custom Data Defaults
- Sessions Capacity Defaults
Recording Defaults

The recording defaults allow you to specify whether or not recording is enabled for the route on the account. You can also specify the Route mode to use for the recording, the percent of recordings allowed, and the recording format.

To configure recording defaults:

1. On the Admin page, click Manage Accounts.
2. Select an account from the Accounts page and click the Details icon for that account.
3. Click Account Route Defaults to expand the route default information.
4. **Route Mode**—Select the type of recording you want this account to perform by default. Valid values are:
   - Default Pass-Through—The ISR operates between the incoming Public Service Telephone Network (PSTN)/SIP Gateway and the Private Branch Exchange (PBX) Interactive Voice Response (IVR), and handles incoming SIP INVITEs by forwarding them on to the PBX/IVR for processing.
   - Conference (default)—The ISR operates as a SIP User Agent Client (UAC). Once invited in this mode, the ISR "listens" to the call audio bridged to it, and is available for recording at any time.
   - Record and Save—The ISR records calls and only saves them if the Record and Save on DTMF key (see Record and Save Mode Defaults) is pressed by one of the parties on the call. If no key is pressed, the recording is automatically discarded. When you select this option, the Percent to Record, Route Can Record, and Default Recording State parameters become grayed-out.
   - Call Parking—The ISR parks the call after the caller listens to a recorded announcement. When a line becomes available to take the call, the ISR forwards the call to the appropriate destination.
   - VAM SIP Test—This method is used for testing purposes only.

   **Note:** Choosing the correct application type is critical to the ISR performance.

5. **Route Can Record**—Select whether or not calls on this route are recorded. Valid values are:
   - Yes (default) - Recording is enabled for all calls on this route.
   - No - Recording is disabled for all calls on this route.

   Use this field to enable/disable recordings on a specific route.

6. **Percent to Record**—Specify a value for the percentage of calls to record on this route. Default is 25. Valid values are:
   - 0 to 100

7. **Always Record As Raw RTP**—Select Yes when multiple transmission codecs are present in a session. If set to No with multiple transmission codecs present in a session, the ISR does not record the call properly.

8. **Recording Format Profile**—Select the recording format profile you want to assign to this account. The default value is Use System Account’s Profile.
Recording Editing Permissions

Recordings in the ISR Administrator Dashboard have specific metadata information that is stored with the actual recording. Some of this information includes Agent ID, rating, notes, and whether or not the recording was completed. (For more information about recordings, see Viewing, Editing, and Playing Recordings.

The Recording Editing Permissions allows an administrator to assign permissions to users for editing this metadata information related to recordings. If enabled, all users for the current account can edit the recording information. If disabled, all users for the current account cannot edit recording information. Default is enabled.

You specify whether or not users for an account can edit recording information by setting the Recording Editing Permissions parameters.

To set recording editing permissions:

1. **Allow Editing of Agent ID?**—Select whether or not you want users for this route to edit the Agent ID for a recording. Valid values are:
   - Yes - Allow editing of Agent ID for a recording.
   - No (default) - Prevent editing of Agent ID for a recording.

2. **Allow Editing of Rating?**—Select whether or not you want users for this route to edit the Rating assigned to a recording. Valid values are:
   - Yes - Allow editing of rating for a recording.
   - No (default) - Prevent editing of rating for a recording.

3. **Allow Editing of Completed Transaction?**—Select whether or not you want users for this route to edit a recording transaction that has been completed. Valid values are:
   - Yes - Allow editing of completed transaction information for a recording.
   - No (default) - Prevent editing of completed transaction information for a recording.

4. **Allow Editing of Notes?**—Select whether or not you want users for this route to edit the Notes specified for a recording. Valid values are:
   - Yes - Allow editing of notes specified for a recording.
   - No (default) - Prevent editing of notes specified for a recording.

Announcement and Recurring Beep Defaults

A recurring beep is an audio tone that is played during the recording of a call that indicates the call is being recorded. You can use the default beep tone or you can use a customized beep tone. You can also specify the duration between each beep tone.

To configure announcements and recurring beep defaults:
1. **Announcement**?—Select whether or not an audio announcement is played for this route before the caller is directed to their end destination (for example, “Your call will be monitored or recorded.”) Valid values are:
   - Yes - Allows announcement to play before call is redirected to destination.
   - No (default) - Prevents announcement from playing before call is redirected to destination.

2. **Announce Audio File**—(optional) Enter the URL where the file is located, that you want to use as the default announcement file to play for all calls to this account. The filename must have a “.wav” extension (for example, *announcement.wav*) AND must be in 8 bit 8kHz ulaw format to guarantee proper playback.

   **Note:** If providing a custom announce audio file, the file must be an 8-bit 8kHz .wav file, and be placed in your ISR install directory (/cxc_common/ISR/Cache/).

3. **Beep During Recording**?—(optional) Select whether or not an audio tone is played during the recording of a call on a recurring basis to indicate the call is being recorded. Valid values are:
   - Yes - Allows an audio tone to play during the recording of a call on a recurring basis as the call is recorded.
   - No (default) - Prevents an audio tone from playing during the recording of a call.

4. **Beep Audio File**—(optional) When the **Beep During Recording**? field is set to **Yes**, Enter the name of the file that contains a customized audio tone that you want to play during the recording of a call on a recurring basis to indicate the call is being recorded. The filename must have a “.wav” extension (for example, *beep.wav*). Default is *beep.wav*.

   **Note:** If providing a custom audio tone, the file must be an 8-bit 8kHz .wav file and be placed in your ISR install directory (/cxc_common/ISR/Cache/).

5. **Beep Interval**—(optional) When the **Beep During Recording**? field is set to **Yes**, specify the amount of time, in seconds, between each recurring beep tone. Default is 30. Valid values are:
   - 1 through 9999

**Conference Mode Defaults**

You can set specific parameters on the ISR to apply to recordings when using the conference mode method.

**To set the conference mode default:**

1. **Terminate on DTMF**?—Select whether or not a recording should stop when a Dual-tone Multi-frequency (DTMF) (keypress) is received. Valid values are:
   - Yes - Allows a recording to stop when a DTMF tone is received.
   - No (default) - Prevents a recording from stopping when a DTMF tone is received.

2. **Play Beep Before Record**?—Select whether or not an audio tone plays to alert the caller that a recording is about to start. Valid values are:
   - Yes - Allows an audio tone to play to alert the caller that a recording is starting.
   - No (default) - Prevents an audio tone from playing before a recording starts.
Record and Save Mode

Defaults

When the **Route Mode** is set to **Record and Save** (see Recording Defaults), you can set the DTMF key that indicates the recording is to be saved. If any other key is pressed, or no key press is received, the recording is discarded.

**Note:** The **Route Mode** parameter MUST be set to **Record and Save** to enable this **Record and Save on DTMF** parameter.

To set the record and save mode defaults:

- **Record and Save on DTMF**—Select the type of keypress that allows the caller to save their recording from their phone’s keypad. This parameter allows you to assign a specific DTMF key (keypress), that when pressed by the caller, stores the recording at their location. The value **disable dtmf** disables this feature. Valid values are:
  - dtmf-pound # (default)
  - dtmf-star *
  - dtmf-0
  - dtmf-1
  - dtmf-2
  - dtmf-3
  - dtmf-4
  - dtmf-5
  - dtmf-6
  - dtmf-7
  - dtmf-8
  - dtmf-9
  - dtmf-0
  - dtmf-7
  - dtmf-1
  - dtmf-8
  - dtmf-9
  - dtmf-disabled

Custom Data Defaults

For routes associated with an account, you can specify up to four (4) elements of data that a User or Developer can tag to a recording using the ISR VXML or REST APIs. Alternatively, these fields can be populated manually by Dashboard users.

For example, if a caller calls into the IVR and enters an account number and elects to transfer to billing because of a billing question, a Developer can invoke the APIs to add two elements (account number and reason for inquiry) to the **Custom Data Default** fields. These elements are then added to the recording index.

You can set the custom data elements to always be used on a specific account, or you can allow Administrators to define their own elements as required.

To set custom data defaults:

1. **This Account’s Routes will**—(optional) Select how you want the custom data fields to be handled by the ISR on routes for this account. Valid values are:
   - **use these as defaults.** - The information in the “Display Label” and “API Variable” fields are used as the defaults for custom data on all routes for this account. These defaults can be customized on a route-by-route basis.
   - **always use the following.** - The information in the “Display Label” and “API Variable” fields are always used for custom data on all routes for this account and cannot be changed.
The ability to set or change these options are dependant on your Administrator level.

<table>
<thead>
<tr>
<th>IF</th>
<th>THEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>you are a Super User or Account Administrator</td>
<td>you CAN set/change the &quot;This Account's Routes will:&quot; field for all accounts.</td>
</tr>
<tr>
<td></td>
<td>you CAN specify/change the &quot;Display Label&quot; and &quot;API Variable&quot; for all accounts.</td>
</tr>
<tr>
<td>you are a Tenant Administrator</td>
<td>you CANNOT set/change the &quot;This Account's Routes will:&quot; field for your own accounts.</td>
</tr>
<tr>
<td></td>
<td>you CAN specify/change the &quot;Display Label&quot; and &quot;API Variable&quot; for your own accounts.</td>
</tr>
</tbody>
</table>

2. **Display Label**—(Optional) Enter the custom data label you want the route to use to identify custom data stored in this field. For example, enter “Billing” as a label to identify the route used for Billing. Valid values are alpha-numeric characters.

3. **API Variable**—(Optional) Enter the variable that the API uses to identify the “Display Label” field. The API variable must match the name passed in the API. For example, if the Display Label is “Billing”, enter the API variable as `billing`. If the Display Label is “Account Number”, enter the API variable as `accountnumber`. Valid values are alpha-numeric characters.

4. (optional) For the remaining **Display Label** fields and **API Variable** fields, repeat steps 2 and 3. You can specify up to 4 display labels and API variables.

### Sessions Capacity Defaults

The ISR allows you to set the maximum number of sessions available for the current account. When the maximum session capacity is reached across all routes on the account, a recording may indicate to the caller that all lines are busy and to call back at another time.

You can also set the number of additional call recording sessions available for routes to use after the maximum number of sessions has been depleted. The additional burst sessions are used ONLY when the maximum session capacity is reached.

1. **Session Capacity**—(Optional) Enter the maximum number of sessions to assign to the current route that can be used for call recording. Default is 24. Valid values are:
   - -1 to 999999999 (must indicate total number of licensed sessions)
   - -1 indicates no limit (default)

   **Note:**
   - The maximum session limits for an Account are subject to your licensing agreement.
   - The maximum session limit data is included in the Usage and Billing Reports. For more information about generating reports, see Chapter 10, Managing Reports.

2. **Additional Burst Session Capacity**—(Optional) Enter the number of additional call recording sessions available for the current account to use after the maximum number of sessions has been depleted. Default is 6. Valid values are:
   - -1 to 999999999 (must indicate total number of licensed sessions)
• -1 indicates no limit (default)

Note:

• The additional burst session limits for an Account are subject to your licensing agreement.

• The additional burst session data is included in the Usage and Billing Reports. For more information about generating reports, see Chapter 10, Managing Reports.

3. Click Update to save the default route parameters. The Accounts page displays.

Viewing and Editing Account Routes, Users, Realms, and the Remote Archiver Server

The Edit Accounts page also has tabs to allow you to view and edit routes, users, realms, and the remote archiver server associated with that account.

Account Routes

To view and edit routes associated with this account:

1. Click Account Routes.

All routes associated with the account appear.

2. Click on a route to edit it. You are brought to the Edit Route page.

Account Users

To view and edit users associated with this account:

1. Click Account Users.
All users associated with the account appear.

2. Click on a user to edit it. You are brought to the Edit User page.

**Account Realms**

To view and edit realms associated with this account:

1. Click **Account Realms**.

   All realms associated with the account appear.

2. Click on a realm to edit it. You are brought to the Edit Realm page.

**Account Remote Archiver Server**

To view and edit the remote archiver server associated with this account:

1. Click **Account Remote Archiver Server**.

   The remote archiver server associated with the account appears.

2. **Client IP Address**—Enter the Remote Archival client’s IP address.

3. **Remove Recordings**—When set to On, the files are deleted from the source RSS/NAS/SAN after a successful push. Valid values are On and Off. The default value is Off.

4. **Max Allowed Attempts**—The maximum number of attempts the Webservice client can make when requesting a recording. The default value is 3.

5. Click **Update**.
Deleting an Account

You can delete accounts in the ISR Dashboard as required.

**Note:** The System account is the default account in the Dashboard and cannot be deleted.

**To delete an account:**

1. On the Admin page, click **Manage Accounts**.
2. Select an account from the Accounts page and click the Delete icon for that account.

The following message and prompt displays.

“Deleting this account will delete all recordings, routes, and user types associated with it! Are you sure you want to delete this account?”

3. Click **OK** to continue and delete the account and all associated recordings, routes, and user types or click **Cancel** to cancel the delete function.

**Warning:** Once you delete an account, it cannot be recovered. All routes, users, and recordings associated with the account are lost.

Importing an Account CSV File

You can define accounts in a CSV file and import the data from the file into the ISR database.

**To import account information from a CSV file:**

1. Using any application that can save to a CSV file, create a file that contains the parameters required for creating an account.

**Notes:**

- Boolean (yes/no) values must be entered using 0 (yes or enabled) and/or 1 (false or disabled).
- All parameters must be entered with no spaces (use underscores instead of spaces).

The following table provides the parameters you must enter in the CSV file. Parameters must be entered in the same order presented below.
<table>
<thead>
<tr>
<th>Parameter Heading</th>
<th>Valid Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>account_name</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>account_description</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>account_m misc</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>percent_to_record</td>
<td>0 to 100</td>
</tr>
<tr>
<td>recording_enabled</td>
<td>0</td>
</tr>
<tr>
<td>recorder_state</td>
<td>0</td>
</tr>
<tr>
<td>default_recording_type</td>
<td>1 None: Account or System default (default)</td>
</tr>
<tr>
<td></td>
<td>2 WAVE Linear/8bit/8KHz stereo</td>
</tr>
<tr>
<td></td>
<td>3 WAVE Linear/16bit/8KHz stereo</td>
</tr>
<tr>
<td></td>
<td>4 WAVE Linear/8bit/8KHz mono</td>
</tr>
<tr>
<td></td>
<td>5 WAVE Linear/16bit/8KHz mono</td>
</tr>
<tr>
<td></td>
<td>6 WAVE uLaw 8bit/8KHz stereo</td>
</tr>
<tr>
<td></td>
<td>7 WAVE aLaw 8bit/8KHz stereo</td>
</tr>
<tr>
<td></td>
<td>8 WAVE uLaw 8bit/8KHz mono</td>
</tr>
<tr>
<td></td>
<td>9 WAVE aLaw 8bit/8KHz mono</td>
</tr>
<tr>
<td></td>
<td>10 Raw uLaw 8bit/8KHz mono</td>
</tr>
<tr>
<td></td>
<td>11 Raw aLaw 8bit/8KHz mono</td>
</tr>
<tr>
<td></td>
<td>12 Raw PCM 8bit/8KHz mono</td>
</tr>
<tr>
<td></td>
<td>13 WAVE ADPCM 4bit/8KHz mono</td>
</tr>
<tr>
<td></td>
<td>14 WAVE ADPCM 8bit/8KHz stereo</td>
</tr>
<tr>
<td>agent_id_editable_flag</td>
<td>0</td>
</tr>
<tr>
<td>rating_editable_flag</td>
<td>0</td>
</tr>
<tr>
<td>completed_editable_flag</td>
<td>0</td>
</tr>
<tr>
<td>notes_editable_flag</td>
<td>0</td>
</tr>
<tr>
<td>announce_enabled</td>
<td>0</td>
</tr>
<tr>
<td>default_announce_audio_text</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>custom_data_1_name</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>custom_data_1_friendly_name</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>custom_data_1_editable_flag</td>
<td>0</td>
</tr>
<tr>
<td>custom_data_2_name</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>custom_data_2_friendly_name</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>custom_data_2_editable_flag</td>
<td>0</td>
</tr>
<tr>
<td>custom_data_3_name</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>custom_data_3_friendly_name</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>custom_data_3_editable_flag</td>
<td>0</td>
</tr>
<tr>
<td>custom_data_4_name</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>custom_data_4_friendly_name</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>custom_data_4_editable_flag</td>
<td>0</td>
</tr>
</tbody>
</table>
Example File with Parameters and Values

<table>
<thead>
<tr>
<th>parameter</th>
<th>values</th>
</tr>
</thead>
<tbody>
<tr>
<td>application</td>
<td>pass_through, conference, record_and_save,</td>
</tr>
<tr>
<td></td>
<td>call_parking, vam_sip_test</td>
</tr>
<tr>
<td>maximum number of ports</td>
<td>digits (-1 for no limit)</td>
</tr>
<tr>
<td>number_of_burst_ports</td>
<td>digits (-1 for no limit)</td>
</tr>
<tr>
<td>acct_port_limit</td>
<td>digits</td>
</tr>
</tbody>
</table>

2. Save the file as a `<filename>.csv` file (for example, `AccountB.csv`).

3. Login to the ISR Dashboard.

4. Click Admin in the main menu (or Edit System Configurations on the Home page).

5. Click Manage Accounts. The Accounts page displays.

6. Click Import. The following dialog box displays.

7. **CSV File to Upload**—Enter the name of the account CSV file you want to import into the ISR database. Valid values are alpha-numeric characters. For example, `Account1.csv`.

   **Note:** To find the file stored on your PC, click `<Browse>`, navigate to the file you want to upload, and click on the file to automatically populate the text field with the name of the file.
8. Click **Upload** to upload the account CSV file to the ISR database.

**Note:** The new accounts are added to your Accounts page and displays the values that correspond to the values you specified in the CSV file.

The dashboard also provides guidelines for creating your file and a working sample. Click on **Guidelines** to display the parameter names you can use in a CSV file when creating an account.

Click on **Sample File**, and then click on **accounts.csv** to download an example of an accounts CSV file you can use as a guideline.
Managing Routes

Introduction

This chapter describes how to manage Routes in your ISR network. You can add, edit, and delete routes for accounts as required. You can also assign a route to a Route Group(s).

Manage Routes

Use the Manage Routes on the Admin Menu of the ISR Dashboard to manage routes in the ISR network.

A route on the ISR defines the parameters to evaluate and invoke recording, as well as the recording rules to apply for all calls received by the ISR. You can set a specific account to have one route or multiple routes, depending on the subscriber’s business requirements.

Note:

- If you make changes to a route associated with an account, the changes apply to that route only and do not affect other routes associated with the same account.
- Super Users and Account Administrators can add routes to all existing accounts. Tenant Administrators can add routes to their own accounts only.
The following table describes the columns on the Routes page.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account</td>
<td>Name of the Account associated with the route.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the type of route:</td>
</tr>
<tr>
<td></td>
<td>From - The incoming call’s From SIP URI is compared with the value in the</td>
</tr>
<tr>
<td></td>
<td>Route Pattern field and must match.</td>
</tr>
<tr>
<td></td>
<td>To (default) - The incoming call’s To SIP URI is compared with the value in</td>
</tr>
<tr>
<td></td>
<td>the Route Pattern field and must match.</td>
</tr>
<tr>
<td></td>
<td>From/To - The incoming call’s From and To SIP URIs are compared with the</td>
</tr>
<tr>
<td></td>
<td>value in the Route Pattern field and both must match.</td>
</tr>
<tr>
<td>Pattern</td>
<td>Specifies the value to match an incoming call’s From, To or From/To value,</td>
</tr>
<tr>
<td></td>
<td>for applying the appropriate rules of the route and account.</td>
</tr>
<tr>
<td>Virtual Pattern</td>
<td>Specifies the destination where the calls matching the route pattern</td>
</tr>
<tr>
<td></td>
<td>are forwarded once recording rules have been evaluated.</td>
</tr>
<tr>
<td>Record</td>
<td>Identifies whether or not recording is enabled or disabled on the account.</td>
</tr>
<tr>
<td></td>
<td>![Recording enabled](Recording enabled.png) ![Recording disabled](Recording disabled.png)</td>
</tr>
<tr>
<td>Percent to Record</td>
<td>Percentage of calls that are allowed to be recorded on this route for this</td>
</tr>
<tr>
<td></td>
<td>account. Valid values are 0% to 100%.</td>
</tr>
<tr>
<td></td>
<td>Displays details for the route and allows you to edit the details.</td>
</tr>
<tr>
<td></td>
<td>Deletes the route.</td>
</tr>
</tbody>
</table>
Adding a Route

You can add a route or multiple routes to a specific account(s) using the **New Route** link on the Routes page. When adding a new route to an account, by default, the parameters on the Route page are defined from the focused account’s Account page details. For example, if you are adding a route to Account A (which already exists with details configured), by default, the new route takes on the configured details from Account A.

**Note:** You can create a route using any application that can save to a comma separated value (CSV) file (i.e., Microsoft® Excel, Notepad®, etc.). Using the ISR Dashboard, you can then import the route information from the file (<filename>.csv) to the ISR database.

For more information about importing route information into the ISR database, see Chapter2, Importing a Route CSV File.

**Note:** A Superuser and Account Administrator can add new routes to all accounts. A Tenant Administrator can add new routes to their own accounts only.

Use the following procedure to add a route and associate an account with that route.

**To add a route:**

1. After logging into the ISR Dashboard, click **Admin** in the main menu (or **Edit System Configurations** on the Home page).
2. Click **Manage Routes**. The Routes page displays.

3. Click the **New Route** link in the upper right corner of the page. The following dialog box displays.

4. **Account**—Select the account name to associate with this new route. Valid values are dependent on the accounts currently configured in the ISR database, and the User’s permission level. The default is **System**.
Note: Once a route is added and assigned to an account, it cannot be reassigned to other accounts. If you attempt to reassign a route to another account, the following message displays:

“Another route with this pattern already exists.”

5. **Route Type**—Select the type of route to use for this account. This field is used to compare with the value in the “Route Pattern” field. Valid values are:
   - **From** - The incoming call’s From SIP URI is compared with the value in the “Route Pattern” field and must match.
   - **To** (default) - The incoming call’s To SIP URI is compared with the value in the “Route Pattern” field and must match.
   - **From/To** - The incoming call’s From and To SIP URIs are compared with the value in the “Route Pattern” field and both must match.

6. **Route Pattern**—Specify the route pattern to use for this account. This field is based on the “Route Type” selected in step 5 (the SIP URI that triggers this rule set). Use the route pattern value to match an incoming call’s From, To or From/To value, and apply the appropriate rules of the route and account. For examples of route patterns, see Examples of Route Patterns.

7. **Virtual Route Pattern**—Clicking this field automatically updates the field with the value from the **Route Pattern** field. To change this value, specify the virtual route pattern to use for the current route. This value specifies the destination where the calls matching the route pattern are forwarded once recording rules have been evaluated. The Virtual Route Pattern is used in conjunction with the Session Agent defined in Managing Sites. A full SIP URI can be provided to override this value. Valid values for this field are alpha-numeric characters. For examples of virtual route patterns, see Examples of Route Patterns.

Note: Use the **Virtual Route Pattern** field for application types of Default Pass-Through and Record and Save routes only.

8. **Route Label**—Enter a name to assign to this route. The route label replaces the “To” value for display so customers can switch the called number from the number given by their service provider, to one more familiar to the users. Valid values are alpha-numeric characters. The Route Label overrides the “From” value in the recordings view.

9. **Route Priority**—Select a priority to assign to this route. Routes with a higher priority number are matched before routes with a lower priority number. Valid values are 1 through 9. Default is 5.

10. Click **Create**. The new route displays on the Routes page.

### Examples of Route Patterns

SIP INVITES arrive with the following information:

To: user@hostname:port
From: user@hostname:port

You can create routes based on either the From value, the To value, or both, by specifying only the user portion of the URI. The following are examples for setting up route patterns.

**Example 1.** You want to set up recording rules for calls that come in on a specific 800 number for your billing department, which are answered by a queue at extension 4334.
Since you are evaluating the address the call is sent TO. You need to know what To value your 800 number maps to in your telephony environment. Often, the To is the last 4 digits of the 800 number. To 1234 is the number used in the following example that the 800 number maps to.

a. Select the Account for which this route applies.
b. Select Route Type of To.
c. Set Route Pattern as 1234.
d. Set Virtual Route Pattern to 4334.

For calls that arrive on To 1234, the ISR applies the rules defined in this route, and then forwards the caller to the value in the virtual route pattern field, extension 4334.

**Example 2.** You have a high priority customer that you want to make sure gets exceptional service. You know their primary phone number is (333) 555-1234 and you want to be sure to record any call from that number and send that call to your high priority queue at 5445.

Since you want to set the rules based on where the incoming call is coming FROM.

a. Select the Account for which this route applies.
b. Select Route Type of From.
c. Set Route Pattern as 3335551234.
d. Set Virtual Route Pattern to 5445 (high priority queue).

**Example 3.** Your largest customer is disputing the number of support tickets they've called in to date, so you'd like to start recording them for future reference. You know their main number is (866) 444-1234 and your customer service To value is 9988. You want to be sure to record any call from that number and send that call to your high priority queue at 5445.

Since you're only interested in calls from a particular number made to your support line, this is a From/To route.

a. Select the Account for which this route applies.
b. Select Route Type of From/To
c. Set Route Pattern as 8664441234/9988.
d. Set Virtual Route Pattern to 5445 (high priority queue). To override the outbound Session Agent, use sip:5445@10.85.122.15:5060 which sends these calls out their own Session Agent.

**Example 4.** You want to set up general recording rules for all calls that come in with To numbers to your billing department, and forward them to a destination in your network.

a. Select the Account for which this route applies.
b. Select Route Type of To.
c. Set Route Pattern as %.

The % (wild card) indicates matching of all To values on the incoming calls. Any incoming call that matches a To uses the associated route to the call destination using the Virtual Route Pattern of %To.
Note: Wild card routes are typically set to a low priority in order to allow other routes with the same route type to be matched.

Configuring/Editing Details of a Route

Superusers and Account Administrators can configure or edit the details for any of the routes on the Routes page. Tenant Administrators can configure or edit the details for their own Routes only.

After selecting a Route on the Routes page, you can perform the following:

- Edit general Route information
- Configure or edit advanced parameters for a Route
- Upgrade to a Route Group

Note: The Route configuration is applied as the default settings for all routes under the specified account.

Edit General Route Information

You can edit the general information for a route when required.

To edit the general route information:

1. On the Admin page, click Manage Routes. The Routes page displays.
2. Select a route from the list and click the Details icon. The following dialog box displays.

   ![Route Configuration Dialog Box]

3. **Route Type**—Edit the type of route to use for this account. This field is used to compare with the value in the **Route Pattern** field. Valid values are:
   - **From** - The incoming call’s From SIP URI is compared with the value in the “Route Pattern” field and must match.
   - **To** (default) - The incoming call’s To SIP URI is compared with the value in the “Route Pattern” field and must match.
   - **From/To** - The incoming call’s From and To SIP URIs are compared with the value in the “Route Pattern” field and both must match.

4. **Route Pattern**—Edit the route pattern to use for this account. This field is based on the “Route Type” selected in step 5 (the SIP URI that triggers this rule set). Use the route pattern value to match an incoming call’s From, To or From/To value, and apply the appropriate rules of the route and account. For examples of route patterns, see Examples of Route Patterns.

5. **Virtual Pattern**—Clicking in this field automatically updates the field with the value from the **Route Pattern** field. To change this value, specify the virtual route pattern to use for the current route. This value specifies the destination where the calls matching the route pattern are forwarded once recording rules have been evaluated. The Virtual Route Pattern is used in conjunction with the Session Agent.
defined in Manage Sites. A full SIP URI can be provided to override this value. Valid values for this field are alpha-numeric characters. For examples of virtual route patterns, see Examples of Route Patterns.

**Note:** Use the Virtual Pattern field for application types of Default Pass-Through and Record and Save routes only.

6. **Route Label**—Edit the name of this route. The route label replaces the “To” value for display so customers can switch the called number from the number given by their service provider, to one more familiar to the users. Valid values are alpha-numeric characters. The Route Label overrides the “From” value in the recordings view.

7. **Route Priority**—Edit the priority for this route. Routes with a higher priority number are matched before routes with a lower priority number. Valid values are 1 through 9. Default is 5.

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

**Route Advanced Configurations**

The Route Advanced Configurations on the Routes page is applied as the default settings for all routes under the specified account. This page allows you to configure:

- Recording parameters
- Recording Editing Permissions
- Announcement and Recurring Beep parameters
- Conference Mode parameters
- Record and Save Mode parameters
- Custom Data parameters
- Capacity parameters
- Archiving parameters

**Recording**

For information about configuring the **Recording** fields, see Recordings, starting at Step 4.

**Recording Editing Permissions**

For information about configuring the **Recording Editing Permissions** fields, see Recording Editing Permissions.
Announcement and Recurring Beep  
For information about configuring the Announcement and Recurring Beep fields, see Announcement and Recurring Beep.

Conference Mode  
For information about configuring the Conference Mode fields, see Conference Mode.

Record and Save Mode  
For information about configuring the Record and Save Mode fields, see Record and Save Mode.

Custom Data  
For routes associated with an account, you can specify up to four (4) elements of data that a User or Developer can tag to a recording using the ISR VXML or REST APIs. Alternatively, these fields can be populated manually by Dashboard users.

For example, if a caller calls into the IVR and enters an account number and elects to transfer to billing because of a billing question, a Developer can invoke the APIs to add two elements (account number and reason for inquiry) to the “Custom Data Default” fields. These elements are then added to the recording index.

You can set the custom data elements to always be used on a specific account, or you can allow Administrators to define their own elements as required.

To set custom data defaults:

1. **This Account’s Routes will**—(optional) Select how you want the custom data fields to be handled by the ISR on routes for this account. Valid values are:
   - **use these as defaults.** - The information in the “Display Label” and “API Variable” fields are used as the defaults for custom data on all routes for this account. These defaults can be customized on a route-by-route basis.
   - **always use the following.** - The information in the “Display Label” and “API Variable” fields are always used for custom data on all routes for this account and cannot be changed.

The ability to set or change these options are dependant on your Administrator level.

<table>
<thead>
<tr>
<th>IF</th>
<th>THEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>you are a Super User or Account Administrator</td>
<td>you CAN set/change the “This Account’s Routes will” field for all accounts.</td>
</tr>
<tr>
<td>you are a Tenant Administrator</td>
<td>you CAN specify/change the “Display Label” and “API Variable” for all accounts.</td>
</tr>
<tr>
<td></td>
<td>you CANNOT set/change the “This Account’s Routes will” field for your own accounts</td>
</tr>
<tr>
<td></td>
<td>you CAN specify/change the “Display Label” and “API Variable” for your own accounts.</td>
</tr>
</tbody>
</table>

2. **Display Label**—(optional) Enter the custom data label you want the route to use to identify custom data stored in this field. For example, enter “Billing” as a label to identify the route used for Billing. Valid values are alpha-numeric characters.
3. **API Variable**—(optional) Enter the variable that the API uses to identify the “Display Label” field. The API variable must match the name passed in the API. For example, if the Display Label is “Billing”, enter the API variable as `billing`. If the Display Label is “Account Number”, enter the API variable as `accountnumber`. Valid values are alpha-numeric characters.

4. **Editable by Users**—(optional) Select whether or not to allow the Display Label and the API Variable to be edited by users. To prevent the field from being edited by other users, select “No.” Valid values are:
   - Yes - Allows the Display Label/API Variable fields to be edited.
   - No (default) - Prevents the Display Label/API Variable fields from being edited.

5. (optional) For the remaining **Display Label** fields and **API Variable** fields, repeat steps 2, 3, and 4. You can specify up to 4 display labels and API variables.

### Capacity

For information about configuring the **Capacity** fields, see Capacity.

### Archiving

The ISR allows you to specify the minimum number of days to store the recordings associated with a route and account. The Recording and Storage Server (RSS) in the ISR manages the storage of the recordings.

![ArchivingMinimumStorageDays](image)

**To set the minimum number days to store recordings:**

1. **Minimum Storage Days**—Specify the number of days you want the recordings for this route and account to be stored by the RSS in the ISR database. Default is 90. Valid values are 0 to 365.

2. Click **Update** to save the advanced route configuration.

### Upgrade to Route Group

A Route Group is a group of routes for a specific account, with the same parameters that are associated with the route in focus (Master Route). You can add or delete multiple routes to/from a Route Group as required. Adding routes to a Route Group ensures that all of the routes in the group have the same rules as the Master Route. All routes in the group must be of the same type (To, From, From/To).

To set up a Route Group, you must have a Master Route previously created with the desired parameters (recording percentage, file formats, announcements, custom data fields, etc.). To create a Master Route, see Adding a Route.

---

**Warning:** All changes made to a Master Route apply to all of the routes in the Route Group.

---

**To add a route to a Route Group:**

1. Make sure you have a Master Route configured for an account.

2. On the Admin page, click **Manage Routes**. The Routes page displays.
3. Select a route from the list to add to a Route Group, and click the Details icon. The following dialog box displays.

4. Click Upgrade to Route Group. The following dialog box displays.

5. **Pattern**—Specify a route pattern to use for this route. This field is based on the “Route Type” currently set for the Master Route. Use the route pattern value to match an incoming call's From, To or From/To and apply the appropriate rules of the route and account. This member is added to the Route Group. Valid values are alphanumeric characters. For examples of route patterns, see Examples of Route Patterns.

6. **Virtual Pattern**—Specify the value of the destination where the calls matching the route pattern are forwarded once recording rules have been evaluated. This value can be a To number. If you defined a Session Agent at Manage Sites, a full SIP URI can override this number. Valid values for this field are alphanumeric characters. For example of route patterns, see Examples of Route Patterns.

   **Note:** Use the Virtual Pattern field for application types of Default Pass-Through and Record and Save routes only.

7. Click **Create** to add the Route to the Route Group. The Routes page displays. A Member Routes tab displays at the bottom of the Routes page.
8. Add the current route to additional Route Groups if required by clicking **New Member Route** and repeat Steps 5, 6, and 7.

**Deleting a Route**

You can delete routes in the ISR Dashboard as required.

**To delete a route:**

1. On the Admin page, click **Manage Routes**.
2. Select a Route from the Routes page and click the Delete icon for that Route.

The following message and prompt displays.

*By deleting this route you will delete any associated webservice appliance and data. Are you sure you want to delete this route?*

3. Click **OK** to continue and delete the route and all associated web service appliances and data or click **Cancel** to cancel the delete function.

**Warning:** Once you delete a route, it cannot be recovered. All associated Web Service appliances and data, as well as any associated route group members are deleted.
Managing Recording Format Profiles

With the addition of wideband codec support, the ISR now supports 16 KHz sampling and recording in addition to 8 KHz. To support mixed sampling rates for transmission codecs and recording formats, you can now create and manage your recording format preferences. Managing your recording format profiles also helps you choose the appropriate recording format when multiple transmission codecs are present in a session.

The new Manage Recording Format Profiles link under the Admin tab allows you to make decisions about file sizes and recording quality so you can apply them to accounts and routes.

There are four Recording Format Profiles:

- Best Quality
- Default
- Small
- Smallest

By clicking on a codec profile, you can edit its name, provide it a description, select a recording preference for instances where multiple transmission codecs are used in a session, and configure a recording format mapping.

You can configure a recording preference for each recording format profile. This means in cases where multiple transmission codecs are present within one raw RTP file and the codec mappings for each are not the same recording format, the ISR converts the raw RTP into a recorded file based on the profile’s size versus recording preferences setting. This is an integer value from 0-100 and in the ISR’s GUI, this is configured using a sliding bar which you can drag to your desired position between Small File Size and Best Quality. The ISR selects the recording format with the weighted size to quality ratio closest to your size versus recording preference.

When handling particular transmission codecs which do not match the bit-size or sampling rate of the recording format, the ISR performs up-sampling or down-sampling to conform the audio to the chosen destination format.

Within a recording format profile, you can also configure recording format mappings. This allows you to select a recording format for each of the four supported transmission codecs, g.711 mulaw, g.711 alaw, g.722, and g.729.

To edit a recording format profile:

1. After logging into the ISR Dashboard, click Edit System Configurations or click Admin in the top menu bar.
2. Click Manage Recording Format Profiles.
   - A list of all four recording format profiles displays.
3. Click the recording format profile you want to edit.
The Edit Recording Format Profile page appears.

4. **Name**—*(Optional)* Enter a name for this recording format profile.

5. **Description**—*(Optional)* Enter a brief description of this recording format profile.

6. **Recording Preference**—*(Optional)* Drag the slide-bar to the appropriate space between Small File Size and Best Quality based on the recording preference for this recording format profile.

**To configure Recording Format Mappings:**

1. Click **Recording Format Mappings** in the Edit Codec Profile page.

2. Beside each Transmission Codec, select a Recording Format from the drop-down list.

3. Click **Update**.

**Applying Recording Format Profiles to Accounts**

1. After logging into the ISR Dashboard, click **Edit System Configurations** or click **Admin** in the top menu bar.

2. Click **Manage Accounts**.

   A list of all accounts configured on the ISR displays.
3. Click the account on which you are applying a recording format profile. Click Account Route Defaults.

4. **Always Record as Raw RTP**—Select Yes when multiple transmission codecs are present in a session. If set to No with multiple transmission codecs present in a session, the ISR will not record the call properly.

5. **Recording Format Profile**—Select the recording format profile you want to assign to this account. The default value is Use System Account’s Profile.

6. Click Update.

**Applying Recording Format Profiles to Routes**

1. After logging into the ISR Dashboard, click Edit System Configurations or click Admin in the top menu bar.

2. Click Manage Routes.

   A list of all routes configured on the ISR displays.

3. Click the route on which you are applying a recording format profile.

4. Click Route Advanced Configurations.

5. **Always Record as Raw RTP**—Select Yes when multiple transmission codecs are present in a session. If set to No with multiple transmission codecs present in a session, the ISR will not record the call properly.

6. **Recording Format Profile**—Select the codec profile you want to assign to this account. The default value is default.

7. Click Update.
You can create routes for an account(s) in a CSV file and import the data from the file into the ISR database.

To import route information from a CSV file:

1. Using any application that can save to a CSV file, create a file that contains the parameters required for creating a route.

**Notes:**

- Boolean (yes/no) values must be entered using 0 (yes or enabled) and/or 1 (false or disabled).
- All parameters must be entered with no spaces (use underscores instead of spaces).

The following table provides the parameters you must enter in the CSV file. Parameters must be entered in the same order presented below.

<table>
<thead>
<tr>
<th>Parameter Heading</th>
<th>Valid Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>route_type</td>
<td>0 To, 1 From, 3 From/To</td>
</tr>
<tr>
<td>route_pattern</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>virtual_route_pattern</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>label</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>priority</td>
<td>1 to 9</td>
</tr>
<tr>
<td>account_name</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>percent_to_record</td>
<td>0 to 100</td>
</tr>
<tr>
<td>recording_enabled</td>
<td>0</td>
</tr>
<tr>
<td>default_recording_type</td>
<td>1 None: Account or System default (default), 2 WAVE Linear/8bit/8KHz stereo,</td>
</tr>
<tr>
<td></td>
<td>3 WAVE Linear/16bit/8KHz stereo, 4 WAVE Linear/8bit/8KHz mono, 5 WAVE Linear/16bit/8KHz mono,</td>
</tr>
<tr>
<td></td>
<td>6 WAVE uLaw 8bit/8KHz stereo, 7 WAVE uLaw 8bit/8KHz stereo, 8 WAVE uLaw 8bit/8KHz mono,</td>
</tr>
<tr>
<td></td>
<td>9 WAVE uLaw 8bit/8KHz mono, 10 Raw uLaw 8bit/8KHz mono, 11 Raw uLaw 8bit/8KHz mono,</td>
</tr>
<tr>
<td></td>
<td>12 Raw PCM 8bit/8KHz mono, 13 WAVE ADPCM 4bit/8KHz mono, 14 WAVE ADPCM 8bit/8KHz stereo</td>
</tr>
<tr>
<td>agent_id_editable_flag</td>
<td>0</td>
</tr>
<tr>
<td>rating_editable_flag</td>
<td>0</td>
</tr>
<tr>
<td>completed_editable_flag</td>
<td>0</td>
</tr>
<tr>
<td>notes_editable_flag</td>
<td>0</td>
</tr>
<tr>
<td>custom_data_1_name</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>custom_data_1_friendly_name</td>
<td>alpha-numeric characters</td>
</tr>
</tbody>
</table>
2. Save the file as a `<filename>.csv` file (for example, `RouteB.csv`).
3. Login to the ISR Dashboard.
4. Click **Admin** in the main menu (or **Edit System Configurations** on the Home page).
5. Click **Manage Routes**. The Route page displays.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>custom_data_1_editable_flag</td>
<td>0</td>
</tr>
<tr>
<td>custom_data_2_name</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>custom_data_2_friendly_name</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>custom_data_2_editable_flag</td>
<td>0</td>
</tr>
<tr>
<td>custom_data_3_name</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>custom_data_3_friendly_name</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>custom_data_3_editable_flag</td>
<td>0</td>
</tr>
<tr>
<td>custom_data_4_name</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>custom_data_4_friendly_name</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>custom_data_4_editable_flag</td>
<td>0</td>
</tr>
<tr>
<td>application</td>
<td>pass_through, conference, record_and_save, call_parking, vam_sip_test</td>
</tr>
<tr>
<td>maximum number of ports</td>
<td>digits (-1 for no limit)</td>
</tr>
<tr>
<td>number_of_burst_ports</td>
<td>digits (-1 for no limit)</td>
</tr>
<tr>
<td>minimum_storage_days</td>
<td>0 to 365</td>
</tr>
</tbody>
</table>

**Example File with Parameters and Values**

![Example File](image)
6. Click **Import**. The following dialog box displays.

![Import dialog box]

7. **CSV File to Upload**—Enter the name of the route CSV file you want to import into the ISR database. Valid values are alpha-numeric characters. For example, `Route1.csv`.

   **Note:** To find the file stored on your PC, click **Browse**, navigate to the file you want to upload, and click on the file to automatically populate the text field with the name of the file.

8. Click **Upload** to upload the route CSV file to the ISR database.

   **Note:** The new route is added to your Routes page and displays the values that correspond to the values you specified in the CSV file.

The dashboard also provides guidelines for creating your file and a working sample. Click on **Guidelines** to display the parameter names you can use in a CSV file when creating a route..

![Guidelines]

Click on **Sample File**, and then click on `routes.csv` to download an example of a route CSV file you can use as a guideline.
5 Managing Authorization Services

Introduction

This chapter provides information about using Authorization Services (3rd party servers) in your ISR network for users to log into when accessing the ISR Dashboard. It also includes information about adding, editing, and deleting Authorization Services.

Manage Authorization Services

Use Manage Authorization Services on the Admin Menu of the ISR Dashboard to manage 3rd party servers in the ISR network.

The ISR supports 3rd party authorization services, sometimes referred to as “single sign-on.” Once a third-party authorization service is properly configured on the ISR, users registered with the third-party platform log into the ISR Dashboard with authorization from the added service. The user’s account is then associated with unique fields and values returned from the authorization service. These fields and values can also be found in the metadata of certain sessions stored in the ISR. When the user requests the recordings listing in the Dashboard, only the recordings with matching metadata are shown and playable.

Once the registered third-party user has logged in successfully through the ISR Dashboard, the user’s account is registered with the local INN-SR platform as well. This enables administrative features for that user, such as changing ISR Dashboard settings, specific permissions (ie., allowing recording edits and deletes) or level of access.

As a default security measure, third-party authorization users have only Tenant User privileges when they first log in. For example, in a deployment enabled for Broadworks third-party authorization, a successful Broadworks log in returns a user ID and group ID unique to that user. Initially the user can only see and hear recordings specific to their user and group ID. However, an administrator can update a user’s privileges and level of access. If given Account Administrator status, the third-party authorization user can see and hear their own recordings, as well as recordings for everyone within their group. For more information on user level access, see Chapter 6, Managing Users.

Note: Only Super Users and Account Administrators have access to managing Authorization Services for other users.
The following table describes the columns on the Routes page.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Authorization Service.</td>
</tr>
<tr>
<td>Service URL</td>
<td>Specifies the Uniform Resource Locator (URL) of the Authorization Service. This is the URL associated with the Authorization Service.</td>
</tr>
<tr>
<td>Status</td>
<td>Identifies the current status of the Authorization Service on the ISR. Values can be:</td>
</tr>
<tr>
<td></td>
<td>![-checked] Authorization Service is enabled.</td>
</tr>
<tr>
<td></td>
<td>![crossed-out] Authorization Service is disabled.</td>
</tr>
<tr>
<td></td>
<td>![triangle] Authorization Service has an error(s).</td>
</tr>
<tr>
<td>SRC Type</td>
<td>Session Recording Client (SRC) type associated with the 3rd Party server. For example, Broadworks. Default is “default”.</td>
</tr>
<tr>
<td></td>
<td>![search] Displays details of the Authorization Service and allows you to edit the details.</td>
</tr>
<tr>
<td></td>
<td>![trash-can] Deletes the Authorization Service.</td>
</tr>
</tbody>
</table>
Adding an Authorization Service

You can add an Authorization Service associated with a 3rd party server (such as the Broadworks server) that controls the secure login and authorization of users using the ISR and logging into the ISR Dashboard. Add an Authorization Service using the New Authorization Service link on the Authorization Services page.

**Note:** Access to an Authorization Service is dependant on your access privileges (Super Users and Account Administrators only).

Use the following procedure to add an Authorization Service to the ISR.

**To add an Authorization Service:**

1. After logging into the ISR Dashboard, click **Admin** in the main menu (or **Edit System Configurations** on the Home page).

2. Click **Manage Authorization Services**. The Authorization Services page displays.

3. Click the **New Authorization Service** link in the upper right corner of the page. The following dialog box displays.

4. **Name**—Enter the name of the Authorization Service (3rd party server). Valid values are alpha-numeric characters.

5. **Service**—Enter the Uniform Resource Locator (URL) of the Authorization Service (3rd party server). Valid values are alpha-numeric characters, and must be entered in a typical URL format. For example, `http://ews.xdp.broadsoft.com/webservice/services/ProvisioningService?wsdl`

6. **Enabled**—Select whether or not to enable the Authorization Service (3rd party server) in the ISR network. Valid values are:
   - Yes (default) - Enable the Authorization Service (3rd party server) to be used in the ISR network.
   - No - Prevents the Authorization Service (3rd party server) from being used in the ISR network.

7. **SRC Type**—Select the Authorization Service (3rd party server) currently deployed in your ISR network. Valid values depend on the type of Session Recording Client (SRC) you are using in your ISR network. Default value is “default” which uses any SRC type having the URL specified for the “Service” parameter.

**Editing an Authorization Service**

You can edit the details of an Authorization Service (3rd party server) as required.

**Note:** Access to an Authorization Service is dependant on your access privileges (Super Users and Account Administrators only).

**To edit an Authorization Service:**

1. Click **Admin** in the main menu (or **Edit System Configurations** on the Home page).
2. Click **Manage Authorization Services**. The Authorization Services page displays.

![Authorization Services Page](image)

4. Edit the parameters for the Authorization Service as applicable using the procedures defined in Adding an Authorization Service, starting at Step 4.
5. When you are finished editing the Authorization Service, click **Update**. The changes are saved to the ISR database and display on the Authorization Service page.

**Deleting an Authorization Service**

You can delete an Authorization Service(s) (3rd party server) from the ISR database as required.

**Note:** Access to an Authorization Service is dependant on your access privileges (Super Users and Account Administrators only).

**To delete an Authorization Service:**

1. Click **Admin** in the main menu (or **Edit System Configurations** on the Home page).
2. Click **Manage Authorization Services**. The Authorization Services page displays.

![Authorization Services page](image)

3. Choose an Authorization Service and click the Delete icon for that Service. The following prompt displays:

   “Are you sure you want to delete this Authorization Service?”

4. Click **Continue** to delete the Authorization Service from the ISR database or click the X in the upper-right corner of the box to cancel the delete function.
Managing Users

Introduction

This chapter provides information about the various user access levels you can assign to Users of the ISR Dashboard. It also provides information about adding, editing, and deleting User profiles, and displaying a User Audit log of tasks performed by each User.

Manage Users

Use Manage Users on the Admin Menu of the ISR Dashboard to manage User profiles in the ISR network.

An Administrator can add, delete, edit, and view users on the ISR. Applicable user functions are dependant on the user access level assigned to the Administrator. Superusers, Account Administrators, and Tenant Administrators can manage Users by accessing the Admin Menu in the ISR Dashboard.
The following table describes the columns on the Users Page.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Name currently assigned to each User.</td>
</tr>
<tr>
<td>Email</td>
<td>Email address of the User. The User enters this email address on the login page. Email address is usually a domain name in the format: <code>&lt;username&gt;@&lt;host server&gt;.&lt;domain name system (.com, .org, .net, .edu, etc.)&gt;</code></td>
</tr>
<tr>
<td>Status</td>
<td>Indicates the current status of the User. Status can be:</td>
</tr>
<tr>
<td></td>
<td>- Status is active. User can log into the ISR Dashboard.</td>
</tr>
<tr>
<td></td>
<td>- Status is inactive. User cannot log into the ISR Dashboard.</td>
</tr>
<tr>
<td></td>
<td>- Status detected that an error occurred for this User profile.</td>
</tr>
<tr>
<td>Account</td>
<td>Primary Account name for which the user is associated.</td>
</tr>
<tr>
<td>Type</td>
<td>User level assigned to this user (Super User, Account Administrator, Tenant Administrator, Tenant User).</td>
</tr>
<tr>
<td></td>
<td>Displays profile details about the User and allows you to edit the details.</td>
</tr>
<tr>
<td></td>
<td>Displays details about the actions of the user in the ISR Dashboard.</td>
</tr>
<tr>
<td></td>
<td>Information includes:</td>
</tr>
<tr>
<td></td>
<td>- Time - Time of the action.</td>
</tr>
<tr>
<td></td>
<td>- Action - Description of the action.</td>
</tr>
<tr>
<td></td>
<td>- Object - Object that was used during the action.</td>
</tr>
<tr>
<td></td>
<td>- IP Address - IP address that was accessed during the action.</td>
</tr>
<tr>
<td></td>
<td>Deletes the User profile.</td>
</tr>
</tbody>
</table>
User Access Levels

The display of information in the ISR Dashboard is dependant on your user level access. Each user has specific permissions and privileges based on their level of access.

The following table indicates the Dashboard features available for each User type.

<table>
<thead>
<tr>
<th>DASHBOARD FEATURE</th>
<th>Super User</th>
<th>Account Administrator</th>
<th>Tenant Administrator</th>
<th>Tenant User</th>
<th>Remote Archiver User</th>
</tr>
</thead>
<tbody>
<tr>
<td>View/ Play Recordings</td>
<td>X</td>
<td>X</td>
<td>Own Recordings only</td>
<td>Own Recordings only</td>
<td>X</td>
</tr>
<tr>
<td>Generate Reports</td>
<td>X</td>
<td>X</td>
<td>Reports for own Accts only</td>
<td>Reports for own Accts only</td>
<td>X</td>
</tr>
<tr>
<td>Edit Dashboard Settings</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Manage Realms</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Manage Accounts</td>
<td>X</td>
<td>X</td>
<td>Own Accts only</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>Manage Routes</td>
<td>X</td>
<td>X</td>
<td>Routes for own Accts only</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>Manage Authorization Services</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>Manage Users</td>
<td>X</td>
<td>X</td>
<td>Users for own Accts only</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>Manage Sites</td>
<td>X</td>
<td>View only</td>
<td>-</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>View Live Sessions</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>X</td>
</tr>
</tbody>
</table>

Note: A Remote Archival user is specific to the Remote Archival Webservice only and cannot log into the ISR Dashboard.

Adding a User

You can add a user or multiple users to all accounts or to a specific account using the New User link on the Users page. Adding a User to the ISR is dependant on your access level permissions. Superusers and Account Administrators can add Users to any account. Tenant Administrators can add Users for their own accounts only. Tenant Users cannot access the Administrator features of the ISR Dashboard.

Use the following procedure to add a user to an account(s).

Note: You can create a User profile using any application that can save to a comma separated value (CSV) file (i.e., Microsoft® Excel, Notepad®, etc.). Using the ISR Dashboard, you can then import the User profile information from the file (<filename>.csv) to the ISR database.

For more information about importing a User profile into the ISR database, see Chapter2, Importing a User Profile CSV File.

To add a user:

1. After logging into the ISR Dashboard, click Admin in the main menu (or Edit System Configurations on the Home page).
2. Click **Manage Users**. The Users page displays.

3. Click **New User**. The following dialog box displays.

4. **Primary Account**—Select the primary account to assign to this User. Valid values are dependant on the accounts currently configured in the ISR, and the permission level of the User. Default is “System.”

5. **User Name**—Enter a name for the user. Valid values are alpha-numeric characters.

6. **Email**—Enter the user’s email address. This is the value the User enters in the “Email” field on the login page. Valid values are alpha-numeric characters, and is usually a domain name in the format:

   `<username>@<host server>.<domain name system (.com, .org, .net, .edu, etc)>`

   For example, smith@acmepacket.com.

7. **Description**—(optional) Enter a description for the user. Valid values are alpha-numeric characters.

8. **Password**—Enter a password for the user to specify when logging into the ISR Dashboard. By default, the password must contain letters and numbers, have at least one uppercase letter, and be at least 8 characters long. Valid values are alpha-numeric characters.
Note: When the user logs in using the assigned password, the Dashboard prompts the user to change it for security purposes.

9. **Confirm Password**—Re-enter the password from Step 8 to verify you entered the password correctly.

10. **Preferred Time Zone**—Select the time zone associated with the location of the user. This value is an offset of Greenwich Mean Time (GMT). The following table provides the valid values and default for this field.

**Time Zone Table**

<table>
<thead>
<tr>
<th>Time Zone</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMT-12 (default)</td>
<td>IDLW - International Date Line West</td>
</tr>
<tr>
<td>GMT-11</td>
<td>NT - Nome</td>
</tr>
<tr>
<td>GMT-10</td>
<td>AHST - Alaska-Hawaii Standard CAT - Central Alaska HST - Hawaii Standard</td>
</tr>
<tr>
<td>GMT-9</td>
<td>YST - Yukon Standard</td>
</tr>
<tr>
<td>GMT-8</td>
<td>PST - Pacific Standard Los Angeles, CA, USA</td>
</tr>
<tr>
<td>GMT-7</td>
<td>MST - Mountain Standard</td>
</tr>
<tr>
<td>GMT-6</td>
<td>CST - Central Standard Mexico City, Mexico Saskatchewan, Canada</td>
</tr>
<tr>
<td>GMT-5</td>
<td>EST - Eastern Standard Bogota Lima, Peru New York, NY, USA</td>
</tr>
<tr>
<td>GMT-4</td>
<td>AST - Atlantic Standard Caracas La Paz</td>
</tr>
<tr>
<td>GMT-3</td>
<td>Brasilia, Brazil Buenos Aires, Argentina Georgetown, Guyana</td>
</tr>
<tr>
<td>GMT-2</td>
<td>AT - Azores</td>
</tr>
<tr>
<td>GMT-1</td>
<td>WAT - West Africa Azores, Cape Verde Islands</td>
</tr>
<tr>
<td>GMT+1</td>
<td>CET - Central European Paris, France Berlin, Germany Amsterdam, The Netherlands Brussels, Belgium Vienna, Austria Madrid, Spain Rome, Italy Bern, Switzerland Stockholm, Sweden Oslo, Norway</td>
</tr>
</tbody>
</table>
11. **User Type**—Select the user access level from the drop-down list to assign to this user. Valid values are

- Super User
- Account Admin
- Tenant Admin
- Tenant User
- Remote Archiver User
Available selections in the “User Type” field are dependent on the permission level of the current user. The following table identifies the available values available for each level of access.

<table>
<thead>
<tr>
<th>User Type</th>
<th>Available User Type Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Superuser</td>
<td>Superuser</td>
</tr>
<tr>
<td></td>
<td>Account Admin</td>
</tr>
<tr>
<td></td>
<td>Tenant Admin</td>
</tr>
<tr>
<td></td>
<td>Tenant User</td>
</tr>
<tr>
<td>Account Administrator</td>
<td>Account Admin</td>
</tr>
<tr>
<td></td>
<td>Tenant Admin</td>
</tr>
<tr>
<td></td>
<td>Tenant User</td>
</tr>
<tr>
<td>Tenant Administrator</td>
<td>Tenant Admin</td>
</tr>
<tr>
<td></td>
<td>Tenant User</td>
</tr>
<tr>
<td>Tenant User</td>
<td>N/A</td>
</tr>
<tr>
<td>Remote Archiver User</td>
<td>N/A</td>
</tr>
</tbody>
</table>

12. **Permissions and Privileges**—Left-click and hold your mouse button on an item in the Available column, and drag it to the Granted column. The items in the Available column (red boxes) indicate what permissions and privileges are available to the user you specified in Step 11. The items in the Granted column (green boxes) enable those permission and privileges for the user. The box colors change as you move from one column to the other.

**Note:** To disable permissions and privileges, drag the items from the Granted column to the Available column.

Available selections for Permissions and Privileges are dependent on the permission level of the user. The following table identifies the available values available for each level of access.

<table>
<thead>
<tr>
<th>User Type</th>
<th>Available Permission and Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Superuser</td>
<td>A Superuser can assign these permissions to an Account Admin, Tenant Admin, and Tenant User:</td>
</tr>
<tr>
<td></td>
<td>• Delete Recordings Permission</td>
</tr>
<tr>
<td></td>
<td>• Edit Recordings Permission</td>
</tr>
<tr>
<td></td>
<td>• Notes and Scoring Permission</td>
</tr>
<tr>
<td></td>
<td>• Access to all Routes in Accounts Permission (Only applies to Tenant Users)</td>
</tr>
<tr>
<td>Account Administrator</td>
<td>An Account Admin can assign these permissions to a Tenant Admin and a Tenant User:</td>
</tr>
<tr>
<td></td>
<td>• Delete Recordings Permission</td>
</tr>
<tr>
<td></td>
<td>• Edit Recordings Permission</td>
</tr>
<tr>
<td></td>
<td>• Notes and Scoring Permission</td>
</tr>
<tr>
<td></td>
<td>• Access to all Routes in Accounts Permission (Only applies to Tenant Users)</td>
</tr>
<tr>
<td>Tenant Administrator</td>
<td>An Tenant Admin can assign these permissions to a Tenant User:</td>
</tr>
<tr>
<td></td>
<td>• Delete Recordings Permission</td>
</tr>
<tr>
<td></td>
<td>• Edit Recordings Permission</td>
</tr>
<tr>
<td></td>
<td>• Notes and Scoring Permission</td>
</tr>
<tr>
<td></td>
<td>• Access to all Routes in Accounts Permission (Only applies to Tenant Users)</td>
</tr>
</tbody>
</table>
13. Click Create to add the new User to the Users page.

Editing a User Profile

You can edit a User’s profile as required. Access to a User profile is dependant on your access privileges.

To edit a User profile:

1. Click Admin in the main menu (or Edit System Configurations on the Home page).
2. Click Manage Users. The Users page displays.

3. Choose a User and click the Details icon for that User. The User profile displays.
4. Edit the parameters for the User as applicable using the procedures defined in Adding a User, starting at Step 4.
5. When you are finished editing the User profile, click Update. The changes are saved to the ISR database for this User. The following message displays: “Successfully saved”.

Showing User Details

The ISR keeps track of a user’s activities while logged into the ISR Dashboard. It logs the following information into a User Audit Trail log:

- Date and time (based on time zone) that the User performed an action.
- Specific action that the User performed.
- Object (User email ID) of the User that was logged in when the action was performed.
- IP address of where the action was performed by the User.

You can view the contents of the User Audit Log by clicking the View User Audit Trail icon for a User on the Users page.

To display the User Audit Trail:

1. Click Admin in the main menu (or Edit System Configurations on the Home page).
2. Click **Manage Users**. The Users page displays.

![ ISR Dashboard Users Page ](image)

3. Choose a User from the Users page and click the View User Audit Trail icon for that User. The User Audit Trail for that User displays.

![ ISR User Audit Trail ](image)

The following table describes the columns in this User Audit Trail log.

<table>
<thead>
<tr>
<th>Column Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time (GMT)</td>
<td>Date and time (based on time zone) when the user performed an action.</td>
</tr>
<tr>
<td>Action</td>
<td>Specific action that the user performed.</td>
</tr>
<tr>
<td>Object</td>
<td>Object (User email ID) of the User that was logged in when the action was performed.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of where the action was performed by the User.</td>
</tr>
</tbody>
</table>

If more than 14 entries appear in the User Audit Trail log, you can use the scroll bar on the right side of the window to scroll through the list of entries.

4. To close the User Audit Trail, click the X in the upper-right corner of the window. The Users page displays.

**Deleting a User**

You can delete users from the ISR database as required.

**To delete a User:**

1. Click **Admin** in the main menu (or **Edit System Configurations** on the Home page).
2. Click **Manage Users**. The Users page displays.

3. Choose a User from the Users page and click the Delete icon for that User. The following prompt displays:

   “Are you sure you want to delete this user?”

4. Click **Continue** to delete the User from the ISR database. Or click the **X** in the upper-right corner of the box to cancel the delete function.

**Managing User Dashboard Security Settings**

The Admin Manage Security Settings link allows you to configure dashboard security settings. Using this link you are able to configure password expirations, user lockout durations, maximum failed login attempts before lockout, and whether or not a user can view a forgotten password page.

**To Configure Dashboard Security Settings:**

1. After logging into the ISR Dashboard, click **Edit System Configurations** or click **Admin** in the top menu bar.

2. Click **Manage Security Settings**.

3. **Users Password Expires in**—Specify the number of days after which users’ passwords expire. The default value is **90**.

4. **User Lockout Duration**—Specify the number of minutes a user must wait before attempting to log in again after reaching the User Max Failed Logins Before Lockout value. The default value is **30**.

5. **User Max Failed Logins Before Lockout**—Specify the number of failed login attempts allowed before the ISR locks a user out.

6. **Show Forgotten Password Page?**—Specify whether or not a user can view a Forgotten Password Page. The default value is **no**.

7. Click **Update**.
You can create user profiles and assign an account to these users using a CSV file. You can then import the data from the file into the ISR database.

To import a user profile from a CSV file:

1. Using any application that can save to a CSV file, create a file that contains the parameters required for creating a user profile.

   **Notes:**
   - Boolean (yes/no) values must be entered using 0 (yes or enabled) and/or 1 (false or disabled).
   - All parameters must be entered with no spaces (use underscores instead of spaces).

   The following table provides the parameters you must enter in the CSV file. Parameters must be entered in the same order presented below.

<table>
<thead>
<tr>
<th>Parameter Heading</th>
<th>Valid Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_name</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>user_email</td>
<td>Usually a domain name in the format <code>&lt;username&gt;:@&lt;host server&gt;..&lt;domain name system (.com, .org, .net, .edu, etc)&gt;</code>. For example: <a href="mailto:sample_email@abc.com">sample_email@abc.com</a></td>
</tr>
<tr>
<td>description</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>password</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>user_type</td>
<td>Superuser, Account Admin, Tenant Admin, Tenant User</td>
</tr>
<tr>
<td>account_name</td>
<td>alpha-numeric characters</td>
</tr>
<tr>
<td>login_disabled</td>
<td>0</td>
</tr>
<tr>
<td>timezone_offset</td>
<td>0</td>
</tr>
<tr>
<td>audit_view_permission</td>
<td>0</td>
</tr>
<tr>
<td>call_control_permission</td>
<td>0</td>
</tr>
<tr>
<td>edit_recording_data_permission</td>
<td>0</td>
</tr>
<tr>
<td>notes_and_scoring_permission</td>
<td>0</td>
</tr>
<tr>
<td>access_to_all_routes_in_account</td>
<td>0</td>
</tr>
</tbody>
</table>

**Example File with Parameters and Values**
2. Save the file as a `<filename>.csv` file (for example, `RouteB.csv`).
3. Login to the ISR Dashboard.
4. Click Admin in the main menu (or Edit System Configurations on the Home page).
5. Click Manage Users. The Users page displays.

6. Click Import. The following dialog box displays.

7. **CSV File to Upload**—Enter the name of the User Profile CSV file you want to import into the ISR database. Valid values are alpha-numeric characters. For example, `User1.csv`.

   **Note:** To find the file stored on your PC, click `<Browse>`, navigate to the file you want to upload, and click on the file to automatically populate the text field with the name of the file.

8. Click Upload to upload the User Profile CSV file to the ISR database.

   **Note:** The new user is added to your Users page and displays the values that correspond to the values you specified in the CSV file.

The dashboard also provides guidelines for creating your file and a working sample. Click Guidelines to display the parameter names you can use in a CSV file when creating a route.
Click on **Sample File**, then click **users.csv** to download an example of a route CSV file you can use as a guideline.
Managing Sites

Introduction

This chapter describes how to configure, manage, and monitor the components of a ISR Site. Site components can include the RSS (recording server), RSS locations, Archivers, Session Agents, and Web Appliances. Each of these components can be accessed from the “Manage Sites” page under the Administrator menu.

Manage Sites

Use the Manage Sites on the Admin Menu of the ISR Dashboard to manage ISR sites in your network. A site is a physical location, a group of recording servers, or a single ISR. Managing sites includes adding, editing, and deleting sites that contain configurations for the following components:

<table>
<thead>
<tr>
<th>Site Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSS</td>
<td>Allows you to view RSS (recording server) information, delete an RSS, modify an RSS, or add a new RSS associated with a site. The RSS configuration parameters include the RSS name, IP Address, XML-RPC port number, and utilization of available ports for each RSS.</td>
</tr>
<tr>
<td>Location</td>
<td>Allows you to edit or delete information about the current Location of the RSS, or add a new Location for the RSS associated with a site. The configuration parameters include Location name, the source directory path on the RSS (where recordings are stored), the HTTP URL path to the recordings, and the amount of free space on the RSS in Kilobytes and Percentage.</td>
</tr>
<tr>
<td>Archiver</td>
<td>Allows you to edit or delete information about an Archiver(s), or add a new Archiver to a site. An Archiver can move recording files from a single location to one location only. However, you can configure multiple archivers to each move files to corresponding destination locations. The configuration parameters include the Archiver’s IP address, the source from which to get the recordings, the destination for which to send the recordings, Archiver threads, number of move attempts, the mode of the archiver (primary or failover), and the state of the archiver (active or paused).</td>
</tr>
<tr>
<td>Session Agent</td>
<td>Allows you to edit or delete information about the current telephony Session Agent(s), or add a new Session Agent associated with a site. A Session Agent connects to the IP PBX and is used to transfer calls to agents or to the PSTN. The Session Agent configuration displays the Session Agent name, IP Address, type of Session Agent (primary or failover), and the status of Session Agent (active or disabled). It also displays information about the last event that occurred on the Session Agent.</td>
</tr>
<tr>
<td>Web Appliance</td>
<td>Allows you to edit or delete information about an Appliance, or add a new Appliance associated with all current sites configured for the ISR. An Appliance allows the ISR to connect to a Web Service to push call recording data to a remote storage area. The Web Appliance configuration displays the route(s) for which the Appliance is associated, the URL that connects the ISR to the Web Service, the maximum connections allowed by the ISR for connecting to the Web Service, the maximum failures allowed per call data record (CDR) by the ISR, whether or not the recording is deleted after the push (enabled or disabled), and the state of the Appliance (active or paused).</td>
</tr>
</tbody>
</table>
**Note:** Only Super Users have access to managing sites. Account Administrators can view the site configurations but do not have access to managing the information.

The following table describes the columns on the Sites page.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the managed Site. Displays configuration details of the RSSs, Locations, Archivers, Session Agents, and Web Appliances, in the ISR network, and allows you to edit the details. Deletes the managed Site.</td>
</tr>
</tbody>
</table>

**Adding a Site**

Superusers can add a Site to the ISR using the **New Site** link on the Manage Sites page. Once the Site is created and saved to the ISR database, you must configure the following applicable components for the Site:

- RSS (required)
- RSS Location (required)
To add a site:

1. After logging into the ISR Dashboard, click Admin in the main menu (or Edit System Configurations on the Home page).
2. Click Manage Sites. The Manage Sites page displays.
3. Click the New Site link in the upper right corner of the page. The following dialog box displays.
4. Name—Enter a name for the Site. Valid values are alpha-numeric characters.
5. Click Create. The Site name displays on the Sites page.

Once you add the Site, you must configure the RSS and the RSS Location. You can also configure an Archiver, Session Agent, and Web Appliance if required. The following paragraphs describe how to configure each of these elements.

Managing an RSS

After adding a Site to the ISR database, you must add an RSS to the Site configuration. The RSS configuration is the recording server information required for the Site’s ISR. You can add, edit, and delete RSSs from the ISR database.

**Important:** It is recommended that you contact your Technical Support representative before adding or changing an RSS configuration.

Adding an RSS

After adding a Site to the ISR, you must add an RSS to the Site’s configuration.

To add an RSS to a Site:
1. From the Sites page, choose a Site and click the Details icon.

The following page displays.

This page shows the current configuration information for all the components configured for the Site (RSS, Locations, Archivers, Session Agents, and Web Appliances). You can click on any of the components to display the main page for that component.

The following table describes the information that displays in the RSS component box.

<table>
<thead>
<tr>
<th>RSS Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running</td>
<td>Total number of RSSs currently running on this Site.</td>
</tr>
<tr>
<td>Offline</td>
<td>Total number or RSSs currently offline on this Site.</td>
</tr>
<tr>
<td>Running with errors</td>
<td>Total number of RSSs running with errors on this Site.</td>
</tr>
<tr>
<td>Current Sessions</td>
<td>Total number of ports currently being used on the RSSs on this Site.</td>
</tr>
<tr>
<td>Total Sessions Capacity</td>
<td>Total number of licensed ports on the RSSs on this Site.</td>
</tr>
</tbody>
</table>
2. Click on the **RSS** component. The following page displays.

3. Click **New RSS**. The following dialog box displays.

4. **Name**—Enter a name that describes the RSS you are adding. Valid values are alphanumeric characters.

5. **IP Address**—Enter the IP address (in dotted decimal format) for which the RSS is listening for traffic.

   **Note:** A new location is created for the RSS using this IP Address under the Location component, with a default path value of `/cxc_common/ISR/Recordings`. You can edit the location if you’ve installed the RSS on a different filesystem path. For more information, see Configuring Location.

6. **RSS XMLRPC Port**—Enter the Port number of the RSS XMLRPC service. This service accepts and queues remote call and recording commands. Default is **8888**.

   **Note:** This value should not be changed unless directed by Oracle Technical Support. Contact Technical Support for more information.

7. Click **Create**. The new RSS displays on the RSS page.

The following table identifies each column on the RSS page.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSS</td>
<td>Name of the RSS.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP Address of the RSS in dotted decimal format (0.0.0.0).</td>
</tr>
<tr>
<td>SIP Traffic Port</td>
<td>SIP Port number on the RSS that is currently accepting SIP traffic.</td>
</tr>
</tbody>
</table>
Editing an RSS

Once you’ve added an RSS, you can edit the RSS parameters if required.

**To configure the RSS:**

1. On the Sites page, choose a Site with an RSS configured and click the Details icon. The Viewing Site page displays.

2. Click on the RSS component. The following page displays.
3. Choose an RSS to edit and click the Details icon. The following dialog box displays.

4. Edit the parameters for the RSS as applicable using the procedures defined in Adding an RSS, starting at Step 4.

5. When you are finished editing the RSS configuration, click **Update**. The changes are saved to the ISR database. The RSS page displays.

### Deleting an RSS

You can delete an RSS from a Site if required.

**To delete an RSS:**

1. On the Sites page, choose a Site with an RSS and click the Details icon. The Viewing Site page displays.

2. Click on the RSS component. The following page displays.

3. Choose an RSS to delete and click the Delete icon. The following prompt displays: “Are you sure you want to delete this RSS?”

4. Click **Continue** to delete the RSS from the ISR database or click the X in the upper-right corner of the box to cancel the delete function.
Warning: Once you delete an RSS, it cannot be recovered.

RSS Handling of a 302 Response via the ISR

A status code of “302 Moved Temporarily” (redirect message) tells a client that the resource they asked for has temporarily moved to a new location. The response includes the new location. It tells the client that it should carry on using the same URL to access this resource.

In addition to handling the 302 locally, the RSS now has the ability to pass through the 302 message to pass through the RSS, letting the Caller determine how it should be handled. This feature is a configurable option via XML.

Managing an RSS Location

After adding an RSS to the ISR, the Location is automatically assigned (see Adding an RSS). The Location indicates the specific location on the RSS where the recordings are stored by the Archiver. You can add a new Location or change an existing Location if required. You can also delete the location if necessary.

Adding a Location

You can add a new Location for an RSS if required.

Note: A single configured Archiver (on the RSS) can move recordings to only one destination location. If you need recordings to go to other destination locations, you must configure an Archiver for each of those locations. For more information about configuring an Archiver, see Managing Archivers.

To add a new RSS Location:

1. From the Sites page, choose a Site and click the Details icon.
The following page displays.

![Location Component](image)

The following table describes the information that displays in the Location component box.

<table>
<thead>
<tr>
<th>Location Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Usage- All Locations</td>
<td>Indicates the percentage of storage disk used by the RSSs in all locations. Valid values are 0% to 100%.</td>
</tr>
</tbody>
</table>

2. Click on the **Location** component. The following page displays.

![Location Page](image)

The following table identifies each column on the Location page.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the RSS Location.</td>
</tr>
<tr>
<td>Recordings Directory</td>
<td>Specifies the directory path on the RSS where the recordings are stored before they are forwarded to the database on the Control and Index Server (CIS).</td>
</tr>
<tr>
<td>Access URL</td>
<td>Specifies the Web URL path for accessing the recordings via a browser.</td>
</tr>
<tr>
<td>Disk Usage</td>
<td>Indicates the percentage of storage disk used for recordings in the source directory/location. Valid values are 0% to 100%.</td>
</tr>
<tr>
<td></td>
<td>Displays details of the RSS Location and allows you to edit the details.</td>
</tr>
<tr>
<td></td>
<td>Deletes the RSS Location from the ISR database.</td>
</tr>
</tbody>
</table>
3. Click **New Location**. The following dialog box displays.

![New Location dialog box]

4. **Name**—Enter a name that describes the Location you are adding. Valid values are alpha-numeric characters. For example, RSS1 (1.1.1.1) Primary.

5. **Recordings Directory**—Enter the directory path to where the Archiver stores the recordings on the RSS (destination directory). Valid values are alpha-numeric characters. For example, /cxc_common/ISR/Recordings.

6. **URL**—Enter the URL that identifies the Web location for accessing the recordings via a browser. For example, http://location1.foo.com/Recordings.

7. **Global**—Select whether or not this Location may be used in Archival configurations on all Sites. Valid values are:
   - Yes - This Location may be used in all Sites.
   - No (default) - This Location configuration may apply to this Site only.

**Recording Converter**

8. **IP Address**—Enter the IP address (in dotted decimal format) of the G.729 media converter (RMC). The RMC media converter converts incoming G.729 recordings from “.rpdd” formatted files to “.wav” formatted files, for playback by the ISR Dashboard. It allows the ISR to accept calls using a G.729 codec. For example, 172.453.45.6.

9. **Port**—Enter the port number of the RMC media converter that receives the G.729 media. Default is 8890.

10. Click **Create**. The new RSS Location displays on the Location page.

---

**Editing a Location**

You can edit the location of an existing RSS if required.

**To edit the Location of an RSS:**

![Location page]

---

112 Oracle Communications Interactive Session Recorder Administrator Guide Release 5.1
1. On the Sites page, choose a Site with an RSS and click the Details icon. The Viewing Site page displays.

2. Click on the Location component. The following page displays.

3. Choose a Location to edit and click the Details icon. The following dialog box displays.

4. Edit the parameters for the RSS Location as applicable using the procedures defined in Adding a Location, starting at Step 4.

5. When you are finished editing the RSS Location, click Update. The changes are saved to the ISR database and display on the Location page.

**Deleting a Location**

You can delete an RSS Location if required.

**To delete an RSS Location:**
1. On the Sites page, choose a Site with an RSS and click the Details icon. The Viewing Site page displays.

2. Click on the Location component. The following page displays.

3. Choose an Location to delete and click the Delete icon. The following prompt displays:

   “Are you sure you want to delete this Location?”

4. Click Continue to delete the Location from the ISR database or click the X in the upper-right corner of the box to cancel the delete function.

---

**Warning:** Once you delete a Location, it cannot be recovered.

---

**Managing Archivers**

You configure an Archiver(s) to store recordings. The Archiver(s) move recording files from a local disk to a Network Attached Storage (NAS) or a Storage Area Network (SAN). It is important to consider your archival requirements before assigning servers to sites, as archivers are ISR-specific.

When you first install the ISR, you specify a Primary location for where the Archiver actively writes the recordings in real time. This can be a partition on the ISR server (RSS) or on another drive or server on the network. (The primary source location in the illustration below is `E:\Recordings on the RSS`).
You can also specify a secondary (failover) source location for the recordings. In the event that the primary location is inaccessible (i.e., it is full, or it can’t be reached on the network, etc.), the ISR begins writing the recordings to the secondary location in real time. (The secondary source location in the illustration below is D:\Recordings).

The following illustration shows an example of the primary and secondary storage locations on the ISR server.

![Diagram showing primary and secondary storage locations](image)

**Note:** Oracle recommends that you specify a secondary location for your recordings in the event the primary is inaccessible for any reason. For more information about setting up your secondary (failover) location, see the *Interactive Session Recorder Installation Guide*.

For ISR installations that do not require large capacity storage spaces for recordings, the primary and secondary locations may provide sufficient space to store the recordings. However, for installations that may have a very large quantity of recordings, additional storage devices such as a Network-Attached Storage (NAS) or a Storage Area Network (SAN), may be required to off-load the recordings from the ISR, to a more permanent location on the NAS or SAN.

On the ISR, you can configure a Primary and Secondary (Failover) Archiver to move recordings from the primary and secondary locations, to more permanent storage devices as required. The Primary Archiver moves recordings from the primary location (source location) to the NAS or (destination location). The Secondary or Failover Archiver moves recordings from the secondary location (source location) to the NAS or (destination location). Since the recordings in the secondary location are flagged as being stored in this location, the Failover Archiver looks for these flagged recordings and moves them to the more permanent storage location.
The following illustration shows the use of the Primary and Failover Archiver in a network.

Note: A single configured Archiver can move recordings to only one destination location. If you need recordings to go to other destination locations, you must configure an Archiver for each of those locations.
The **Archivers** box on the Viewing Sites page displays the current status of the Archiver.

The following table describes the information that displays in the Archivers component box.

<table>
<thead>
<tr>
<th>Archivers Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Total number of Archivers enabled on this Site.</td>
</tr>
<tr>
<td>Disabled</td>
<td>Total number of Archivers disabled on this Site.</td>
</tr>
</tbody>
</table>

Clicking on the **Archiver** box on the Viewing Sites page allows you to add a new Archiver to the site, edit the configuration of an existing Archiver, or delete an Archiver if required.

**Adding an Archiver**

You can add an Archiver to a Site if required.

**To add an Archiver:**

1. From the Sites page, choose a Site and click the Details icon.
2. Click on the Archivers component. The following page displays.

The following table identifies each column on the Archivers page.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
</table>
| IP Address | IP Address of the current Archiver.  
**Note:** Archiver resides on the RSS. |
| Source    | Specifies the location where the source recordings reside. This is the location from where the Archiver gets the recordings. For a Primary Archiver, the value for this field should be the Primary Source Location. For a Failover Archiver, the value should be the Secondary Source Location. |
| Destination | Specifies the location of the storage devices (NAS, SAN, etc.) for which the Archiver moves the recordings for storage. This is the Universal Naming Convention (UNC) path of the destination location. When the Archiver moves the recording files to the destination location, it creates the appropriate subdirectories in this path to sort by machine, date, and time. |
| Status    | Identifies whether the Archiver is enabled (active) for moving recording files, or temporarily disabled (paused). Status can be:  
- Enabled  
- Disabled |
3. Click **New Archiver**. The following dialog box displays.

4. **IP Address**—Enter the IP address of the Archiver you are adding to this site. Valid values are IPv4 addresses entered in the format 0.0.0.0. (for example, 134.345.43.56).

5. **Source Location**—Select the location where the source recordings reside. This is the location from where the Archiver gets the recordings. For a Primary Archiver, the value for this field should be the Primary Source Location. For a Failover Archiver, the value should be the Secondary Source Location. By default, this field displays the source location installed in your ISR network during the installation of the Archiver.

   **Note:** The Primary Source Location and Secondary Source Location were configured during the ISR installation. For more information, see the *Interactive Session Recorder Installation Guide*.

6. **Destination Location**—Select the location of the storage devices (NAS, SAN, etc.) for which the Archiver moves the recordings for storage. This is the Universal
Naming Convention (UNC) path of the destination location. When the Archiver moves the recording files to the destination location, it creates the appropriate subdirectories in this path to sort by machine, date, and time. By default, this field displays the destination location installed in your ISR network during the installation of the Archiver.

7. **Number of Threads**—Select the number of simultaneous recordings that an Archiver can move at one time. Valid values are 1 through 90. Default is 3.

8. **Move Attempts**—Select the number of attempts that the Archiver makes when moving recordings from the local disk to the storage device(s). If the Archiver fails to move the recording files from the source location to the destination location the first time, it repeats the attempts to move the files the number of times you set for this field. When all attempts are exhausted, and the Archiver still cannot move the recordings, a message displays stating that the Archiver has failed. If the Archiver is successful in moving the files, a message displays stating that the Archiver was successful. Valid values for this field are 1 through 10. Default is 1.

9. **Mode**—Select whether this Archiver is the Primary or the Failover Archiver. The Primary Archiver moves all recordings from the Primary Source Location to the destination location. The Failover Archiver moves all recordings from the Secondary Source Location to the destination location. Valid values are:
   - **Primary** (default) - This Archiver moves files from Primary Source Location.
   - **Failover** - This Archiver moves files from Secondary Source Location.

10. **Status**—Select whether the Archiver is enabled (active) for moving recording files, or temporarily disabled (paused). Valid values are:
    - **Enabled** (default) - Archiver is active and monitors when recording files are ready to be archived.
    - **Disabled** - Archiver is temporarily disabled and does not move recording files.

11. **Able to Delete Recordings**—Select whether or not this Archiver has permission to delete recordings and metadata stored longer than specified in Route/Account configurations. Valid values are:
    - **Yes** (default) - Archiver deletes files older than specified in Route/Account configurations.
    - **No** - Archiver does not delete files, regardless of the date specified in Route/Account configurations.

12. **Store in Date Directory**—Select whether or not the Archiver stores the recording files in a folder identified by the current date. Valid values are:
    - **Yes** (default) - Archiver stores recordings in a folder by date.
    - **No** - Archiver does not store recordings in a folder by date.

13. **Store in Account Directory**—Select whether or not the Archiver stores the recording files in a folder identified by the associated account on the local disk. Valid values are:
    - **Yes** - Archiver stores recordings in a folder by account.
    - **No** (default) - Archiver does not store recordings in a folder by account.

14. **Purge Index of Missing Recordings**—Select whether or not the Archiver attempts to remove recording files with no audio, from the main recording table, and send them to a “problem” table that can be reviewed at a later time. Enabling this feature prevents a user from viewing recording files with no audio, when they perform a search. However, an Administrator can view the “problem” table if required, for troubleshooting purposes. If this feature is disabled, the Archiver keeps the recording
file with no audio in the main recording table and moves on to the next record in the table. Valid values are:

- **Yes** - Archiver moves recordings with no audio from the main recording table to a “problem” table. Users cannot view these recordings. Administrators can view the “problem” table.

- **No** (default) - Archiver keeps recordings with no audio in the main recording table. Users can view these recordings.

**Conversion Configurations**

15. **Mode**—Select whether all G.729 recordings are converted, a percentage of recordings are converted, or no recordings are converted. Valid values are:

- **Disabled** (default) - The RMC media converter does not convert incoming G.729 recordings from .rpdd format to .wav format.

- **Convert All** - The RMC media converter converts all incoming G.729 recordings from .rpdd format to .wav format.

- **Convert by Percentage** - The RMC media converter converts only a percentage of all incoming G.729 recordings from .rpdd format to .wav format, based on the value entered for the “Percent of Recordings to Convert” parameter.

16. **Percent of Recordings to Convert**—Select a number to indicate the percentage of incoming recordings to be converted by the RMC media converter. The “Mode” field must be set to “Convert by Percentage” in order to set the percentage value. Valid values are 0 to **100**. Default is **100** percent.

17. **Convert All Recordings in Last Archiver Destination**—Select whether or not the RMC media converter converts all of the last G.729 recordings stored in the Archiver from .rpdd format to .wav format. Valid values are:

- **Yes** (default) - The RMC media converter converts all of the last G.729 recordings stored in the Archiver from .rpdd format to .wav format.

- **No** - The RMC media converter DOES NOT convert all of the last G.729 recordings stored in the Archiver from .rpdd format to .wav format.

18. Click <Create>. The new Archiver displays on the Archivers page.

**Editing an Archiver**

You can edit an Archiver configuration if required.

**To edit an Archiver:**
1. From the Sites page, choose a Site with an Archiver and click the Details icon. The Viewing Site page displays.

![Viewing Site page](image1)

2. Click on the **Archiver** component. The following page displays.

![Archiver page](image2)

3. Choose an Archiver to edit and click the Details icon. The following dialog box displays.

![Archiver dialog box](image3)
4. Edit the parameters for the Archiver as applicable using the procedures defined in Adding an Archiver, starting at Step 4.

5. When you are finished editing the Archiver, click Update. The changes are saved to the ISR database and display on the Archivers page.

**Deleting an Archiver**

You can delete an Archiver if required.

**To delete an Archiver:**

1. On the Sites page, choose a Site with an Archiver and click the Details icon. The Viewing Site page displays.

2. Click on the Archiver component. The following page displays.

3. Choose an Archiver to delete and click the Delete icon. The following prompt displays:

   “Are you sure you want to delete this Archiver?”

4. Click Continue to delete the Archiver from the ISR database or click the X in the upper-right corner of the box to cancel the delete function.
Warning: Once you delete an Archiver, it cannot be recovered.

Managing Session Agents

A Session Agent connects to the IP PBX and is used to transfer calls to other agents or to the PSTN. The Session Agents configuration allows you to add a new Session Agent to a Site, edit an existing Session Agent, or delete a Session Agent associated with a Site.

Adding a Session Agent

To add a Session Agent:

1. From the Sites page, choose a Site and click the Details icon.

The following page displays.

The following table describes the information that displays in the Session Agents component box.

<table>
<thead>
<tr>
<th>Archivers Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Total number of Session Agents enabled on this Site.</td>
</tr>
<tr>
<td>Failed</td>
<td>Total number of failed Session Agents on this Site.</td>
</tr>
</tbody>
</table>
2. Click on the **Session Agents** component. The following page displays.

![Session Agents page](image)

The following table identifies each column on the Session Agent page.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Session Agent.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP Address of the Session Agent in dotted decimal format (0.0.0.0).</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies whether the Session Agent is acting as a Primary or Secondary (failover) device.</td>
</tr>
<tr>
<td>Status</td>
<td>Identifies whether the Session Agent is:</td>
</tr>
<tr>
<td></td>
<td>- Enabled for this Site (default)</td>
</tr>
<tr>
<td></td>
<td>- Disabled for this Site</td>
</tr>
<tr>
<td>Last Event</td>
<td>Specifies the last event that occurred on the Session Agent. The event displays as the date, time, time zone, and User of the last event on the Session Agent. “None” indicates that no events have occurred.</td>
</tr>
<tr>
<td></td>
<td>- Displays details of the Session Agent and allows you to edit the details.</td>
</tr>
<tr>
<td></td>
<td>- Displays specific events that occurred on the Session Agent. Events display the date, time, time zone, and event description for each event.</td>
</tr>
<tr>
<td></td>
<td>- Deletes the Session Agent from the ISR database.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Archivers Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Total number of Session Agents disabled on this Site.</td>
</tr>
<tr>
<td>Max Failure Count</td>
<td>Total number of failures endured by all Session Agents for this Site before they are disabled.</td>
</tr>
<tr>
<td>Max Failure Seconds</td>
<td>Length of time, in seconds, for which the Session Agents for this Site can have failures before they are disabled.</td>
</tr>
<tr>
<td>Seconds Before Retry</td>
<td>Length of time, in seconds, that the Session Agents for this Site wait to retry a connection after a failed attempt has occurred.</td>
</tr>
</tbody>
</table>
3. Click **New Session Agent**. The following dialog box displays.

4. **Name**—Enter a name for the new Session Agent. Valid values are alpha-numeric characters. For example, SA2.

5. **IP Address**—Enter the IP address (in dotted decimal format), for the new Session Agent. Value must be entered in the format 0.0.0.0. For example, 123.243.3.5.

6. **Type**—Select the type to associated with this Session Agent you are adding. Valid values are:
   - **Primary** - The site uses this Session Agent as the Primary Session Agent to transfer calls to an agent or to the PSTN. By default, the Primary Session Agent is disabled if there are more than 5 failures in 30 seconds. If this occurs, the Session Agent is disabled for 5 minutes.
   - **Failover** - The site uses this Session Agent as the secondary (or failover) Session Agent to transfer calls to an agent or to the PSTN. The site uses this Session Agent ONLY if the primary Session Agent is inactive or has failed.

   **Note:** You can define multiple Primary Session Agents. The ISR load balances calls across all Primary Session Agents.

7. Click **Create**. The new Session Agent displays on the Session Agent page.

---

**Editing a Session Agent**

You can edit an existing Session Agent configuration if required.

**To edit a Session Agent:**

1. From the Sites page, choose a Site with a Session Agent and click the Details icon. The Viewing Site page displays.
2. Click on the **Session Agent** component. The following page displays.

![Session Agent Component](image1)

3. Choose a Session Agent to edit and click the Details icon. The following dialog box displays.

![Session Agent Details](image2)

4. Edit the parameters for the Session Agent as applicable using the procedures defined in Adding a Session Agent, starting at Step 4.

5. **Status**—Select whether or not to enable the Session Agent for the current Site. Valid values are:
   - **Enabled** - Enable this Session Agent for the current Site.
   - **Disabled** - Disable this Session Agent for the current Site.

6. When you are finished editing the Session Agent, click `<Update>`. The changes are saved to the ISR database and display on the Session Agents page.

### Deleting a Session Agent

You can delete a Session Agent if required.

**To delete a Session Agent:**
1. On the Sites page, choose a Site with a Session Agent and click the Details icon. The Viewing Site page displays.

![Viewing Site page](image1.png)

2. Click on the **Session Agents** component. The following page displays.

![Session Agents page](image2.png)

3. Choose a Session Agent to delete and click the Delete icon. The following prompt displays:

   "Are you sure you want to delete this Session Agent?"

4. Click Continue to delete the Session Agent from the ISR database or click the X in the upper-right corner of the box to cancel the delete function.

   **Warning:** Once you delete a Session Agent, it cannot be recovered.

---

**Display Events for a Session Agent**

You can display the events that occur for each Session Agent by clicking the Events icon. Events include information on the date, time, time zone, and User of the event. If no events have occurred for the Session Agent, a message, "There are no Events for this Session Agent" displays.

**To display events for a Session Agent:**
1. From the Sites page, choose a Site with a Session Agent and click the Details icon. The Viewing Site page displays.

![Viewing Site page](image)

2. Click on the **Session Agent** component. The following page displays.

![Session Agent page](image)

3. Choose a Session Agent and click **i**. The following Event box displays.

![Event box](image)

The Event list is read-only.

4. Click X in the upper-right corner to close the Events box.

**Advanced Configuration for Session Agents (Site-wide)**

You can configure specific advanced configuration parameters that apply to all Session Agents for a single Site.

**To configure advanced parameters for Session Agents:**
1. From the Sites page, choose a Site with a Session Agent and click the Details icon. The Viewing Site page displays.

2. Click on the **Session Agent** component. The following page displays.

3. Click **Advanced Configuration**. The following dialog box displays.

4. **Max Failure Count**—Select the number of failures that the Session Agent endures before it is disabled. Valid values are 1 through 100. Default is 5.

5. **Max Failure Seconds**—Specify the length of time, in seconds, for which the Session Agent can have failures before it is disabled. Valid values are 1 through 300 seconds (5 minutes). Default is 30 seconds.

6. **Seconds Before Retry**—Specify the length of time, in seconds, that the Session Agent waits to retry a connection after a failed attempt has occurred. Valid values are 0 through 300 seconds (5 minutes). Default is 0 seconds.

7. Click **Update**. The settings apply to all the Session Agents for the current Site. The following message displays in the dialog box:

   “Updated successfully”.
Managing Web Appliances

A Web Appliance allows the ISR to connect to a Web Service to push call recording data to a remote storage area. The Web Appliances page allows you to edit or delete information about an Appliance, or add a new Appliance associated with a Site configured for the ISR. This page displays the route(s) for which the Appliance is associated, the URL that connects the ISR to the Web Service, the maximum connections allowed by the ISR for connecting to the Web Service, the maximum failures allowed per call data record (CDR) by the ISR, whether or not the recording is deleted after the push, and the state of the Appliance (enabled or disabled).

Note: For additional information about configuring a Web Service, contact Technical Support.

Adding a Web Appliance

To add a Web Appliance:

1. From the Sites page, choose a Site and click the Details icon.

The following page displays.
The following table describes the information that displays in the Web Appliances component box.

<table>
<thead>
<tr>
<th>Archivers Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Total number of Web Appliances enabled on this Site.</td>
</tr>
<tr>
<td>Disabled</td>
<td>Total number of Web Appliances disabled on this Site.</td>
</tr>
</tbody>
</table>

2. Click on the **Web Appliance** component. The following page displays.

The following table identifies each column on the Web Appliances page.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route</td>
<td>Specifies the Route pattern of the route configured with a Web Service.</td>
</tr>
<tr>
<td>URLs</td>
<td>Specifies the URL(s) that connects the ISR to the Web Service.</td>
</tr>
<tr>
<td>Status</td>
<td>Identifies whether the Web Service is:</td>
</tr>
<tr>
<td></td>
<td>✔ Enabled for this Route pattern.</td>
</tr>
<tr>
<td></td>
<td>✗ Disabled for this Route pattern.</td>
</tr>
<tr>
<td>Max Concurrent Connections</td>
<td>Specifies the maximum concurrent connection attempts allowed from the ISR to the Web Service for this route.</td>
</tr>
<tr>
<td>Max Failures per CDR</td>
<td>Specifies the number of maximum failures allowed by the ISR during the push of data from the Web Service for a call detail record (CDR). When this threshold is reached, the information is not stored and is lost.</td>
</tr>
<tr>
<td>Delete after Push</td>
<td>Specifies whether or not the ISR deletes the call recording detail record after the Web Service has completed pushing the data to the ISR. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>• Yes</td>
</tr>
<tr>
<td></td>
<td>• No</td>
</tr>
<tr>
<td></td>
<td>Displays details of the Web Service associated with this route, and allows you to edit the details.</td>
</tr>
<tr>
<td></td>
<td>Deletes the Web Service association with this route. After performing this delete function, the Web Service information still exists in the database but is no longer associated with the current route.</td>
</tr>
</tbody>
</table>
3. Click **New Web Appliance**. The following dialog box displays.

![New Web Appliance Dialog Box](image)

4. **Route**—Select the route pattern to which you are applying this new Web Appliance. Valid values are dependant on the route patterns currently configured on the ISR.

5. **URL 1**—Enter the Uniform Resource Locator (URL) of the first Web Service for which the ISR connects. Valid values can be an IP address in the format 0.0.0.0 (for example, 132.32.45.6), or a domain name in the format http://www.<domain name>.<applicable suffix> (for example, www.acmepacket.com).

   **Note:** A domain name may have a secure connection using “https” as well.

6. **URL 2**—(optional) Enter the second Web Service URL for which the ISR connects. This URL is used by the ISR if it fails to connect to the first Web Service URL (Web Service URL 1). Valid values can be an IP address in the format 0.0.0.0 (for example, 132.32.45.6), or a domain name in the format http://www.<domain name>.<applicable suffix> (for example, www.acmepacket.com).

7. **URL 3**—(optional) Enter the third Web Service URL for which the ISR connects. This URL is used by the ISR if it fails to connect to the second Web Service URL (Web Service URL 2). Valid values can be an IP address in the format 0.0.0.0 (for example, 132.32.45.6), or a domain name in the format http://www.<domain name>.<applicable suffix> (for example, www.acmepacket.com).

   **Note:** The ISR attempts to connect to URL 1. If connection fails, it attempts to connect to URL 2. If this fails, it attempts to connect to URL 3. Each time the attempt is made to connect, it must reach the value specified for the “Max Concurrent Connections” field before dropping the connection and trying the next configured URL. If all attempts fail, no further attempts are made to connect to a Web Service.

   Likewise, if URL 2 and URL 3 are blank (no specified value), and the attempt to connect to URL 1 fails, after the value specified for “Max Concurrent Connections” is reached, no further attempts are made to connect to a Web Service and the call is dropped.

8. **Max Concurrent Connections**—Select the number of maximum connection attempts allowed from the ISR to the Web Service for this route. Valid values are 1 through 90. Default is 1.

9. **Max Failures per CDR**—Select the number of maximum failures allowed by the ISR during the push of data from the Web Service for a call recording detail record. Valid values are 1 through 10. Default is 1.

   When this threshold is reached the information is not stored and is lost.

10. **Delete CDR after Push**—Select whether or not the ISR deletes the call recording detail record after the Web Service has completed pushing the data to the ISR.
• Yes - Indicates the ISR deletes all call recording detail records after the recording sessions are complete with the Web Service.

• No (default) - Indicates the ISR stores all call recording detail records after the recording sessions are complete with the Web Service.

11. Initial Status—Select whether or not the Web Appliance is available to connect to the ISR. Valid values are:

• Enabled (default) - Indicates the Web Service is available to the ISR for connection.

• Disabled - Indicates the Web Service availability is not currently available to the ISR for connection.


**Editing a Web Appliance**

You can edit an existing Web Appliance configuration if required.

**To edit a Web Appliance:**

1. From the Sites page, choose a Site with a Web Appliance and click the Details icon. The Viewing Site page displays.

2. Click on the Web Appliance component. The following page displays.
3. Choose a Web Appliance to edit and click the Details icon. The following dialog box displays.

4. Edit the parameters for the Web Appliance as applicable using the procedures defined in Adding a Web Appliance, starting at Step 4.

5. **Current Status**—Select whether or not to enable the Web Appliance for the current Site. Valid values are:
   - **Enabled** - Enable this Web Appliance for the current Site.
   - **Disabled** - Disable this Web Appliance for the current Site.

6. When you are finished editing the Web appliance, click **Update**. The changes are saved to the ISR database and display on the Web Appliances page.

**Deleting a Web Appliance**

You can delete a Web Appliance if required.

**To delete a Web Appliance:**

1. On the Sites page, choose a Site with a Web Appliance and click the Details icon. The Viewing Site page displays.
2. Click on the Web Appliances component. The following page displays.

![Web Appliances component](image)

3. Choose a Web Appliance to delete and click the Delete icon. The following prompt displays:

   "Are you sure you want to delete this Web Appliance?"

4. Click Continue to delete the Web Appliance from the ISR database or click the X in the upper-right corner of the box to cancel the delete function.

**Warning:** Once you delete a Web Appliance it cannot be recovered.
Introduction

This chapter describes how to view active call sessions on the ISR, and whether or not the RSS is recording those sessions.

Manage Live Sessions

You can view live call sessions currently occurring on the ISR using the Live Sessions link on the Admin page.

Note: Only Super Users and Account Administrators can view live call sessions currently being received by an RSS.
## Lives Sessions Page

The following table describes each column on the Live Sessions page.

<table>
<thead>
<tr>
<th>Column Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>Specifies the From SIP URI. This is the URI from where the call session is coming.</td>
</tr>
<tr>
<td>To</td>
<td>Specifies the To SIP URI. This is the URI to where the call session is destined.</td>
</tr>
<tr>
<td>Session Start</td>
<td>Specifies the date and GMT time when the active session began.</td>
</tr>
<tr>
<td>Status</td>
<td>Identifies whether the session is:</td>
</tr>
<tr>
<td></td>
<td><strong>Recording</strong> - Call session is in progress and the RSS is recording the session.</td>
</tr>
<tr>
<td></td>
<td><strong>Idle</strong> - Call session is in progress but the RSS is not currently recording the session.</td>
</tr>
<tr>
<td>RSS</td>
<td>Specifies the name of the RSS receiving the live call session.</td>
</tr>
</tbody>
</table>

The Live Sessions page allows you to view all active call sessions currently coming into the RSS, and whether or not the call session is being recorded by the RSS.

If a session is recording, a Recording status displays in the Status column. If the RSS is not currently recording the session, the status displays as Idle.

Up to 15 active call sessions display on a single page. The total number of active call sessions display at the bottom of each page.

If more than 15 calls display on a single page, click the **Next** and **Previous** links to navigate between pages of the Live Sessions list.
Viewing Live Sessions

You can view live call sessions currently coming into an RSS.

To view the Live Sessions:

1. After logging into the ISR Dashboard, click Admin in the main menu (or Edit System Configurations on the Home page).

2. Click Live Sessions. The Live Sessions page displays.

This page lists all of the active call sessions currently being received by an RSS, and the recording status of each session (recording or idle).

3. If more than 15 sessions display on the page, click Next and Previous to navigate between pages, or click the page number you want to display.
9 Managing Recordings

Introduction

This chapter provides information about managing account recordings on the ISR. You can play, view, edit, and delete recordings as required.

Manage Recordings

All user levels can view, edit, delete, and/or play recordings stored on the ISR’s Archiver (or other configured storage facility). However, a Tenant Administrator and Tenant User can edit, play, and delete their own recordings only.

Note: Recordings that display are dependant on the level of user currently logged into the ISR Dashboard.

In addition to viewing, editing, playing, and deleting recordings, a user with “Notes and Scoring” permission can also specify notes for a recording, and specify a rate or score for a recording. A recording can be rated or scored on a chart from 1 star to 10 stars, with 10 stars being the best. For more information about assigning a score to a recording see Recording Details.

You can access the Recordings from the Home page by clicking “Find Recordings” (or by clicking “Recordings” on the top menu bar).

Each recording displays on the Recordings page with information about that recording.
Recordings Page

The following table describes each column on the Recordings page.

<table>
<thead>
<tr>
<th>Column Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Specifies the start date and time of the recording. This column is based on the User's GMT offset.</td>
</tr>
<tr>
<td>From</td>
<td>Specifies the From SIP URI. This is the URI from where the session that was recorded came from.</td>
</tr>
<tr>
<td>Duration</td>
<td>Specifies the length of time, in seconds, of the recording.</td>
</tr>
<tr>
<td>File Name</td>
<td>Specifies the name of the recording file, assigned by the system or by the device that invoked the recording.</td>
</tr>
<tr>
<td>Session ID</td>
<td>Specifies the unique XISR-UCID for this recording.</td>
</tr>
<tr>
<td></td>
<td>Plays the selected recording.</td>
</tr>
<tr>
<td></td>
<td>Downloads the selected recording to a file on your PC.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> All users can download recordings from the Archiver to a “.csv” file if required. However, only 10,000 recordings at a time can be downloaded to a single file. For more information, see Downloading a Recording List to a CSV.</td>
</tr>
<tr>
<td></td>
<td>Displays details of the Recording and allows you to edit the details.</td>
</tr>
<tr>
<td></td>
<td>Deletes the Recording from the Archiver.</td>
</tr>
</tbody>
</table>
Playing a Recording

After a recording occurs on the ISR, it is saved to the Archiver as an audio file so a user can review the details of the recording and listen to the audio. You can choose a recording from the Recordings page, and play the audio file for that recording by clicking the Play icon.

**Note:** The recording’s metadata is saved in the ISR database.

The Recordings page displays all up-to-date recordings. Depending on the size of your storage device (Network Attached Storage (NAS), Storage Area Network (SAN)), older recordings may not be stored locally. However, this is transparent to the user viewing the recordings. Regardless of where the recordings are stored, all recordings display on the Recordings page.

**Note:** Before playing recordings, make sure you have a media application that plays audio files with a “.wav” format. For more information about the software requirements and recommendations for playing recordings, see Requirements/Recommendations.

To play a recording:

1. After logging into the ISR Dashboard, click **Find Recordings** on the Home Page (or **Recordings** on the main menu bar). The Recordings page displays.

2. Choose a recording and click the Play icon. The following message displays.

**Note:** To find a specific recording, perform a search using the **Advanced Search** link in the upper-right corner of the page. For more information, see Search Tools.
The Recordings page refreshes depending on the value set at *Settings*->*Refresh Rate (seconds)*. Default is every 30 seconds. For more information about setting the Refresh rate, see Dashboard Settings.

When the recording is retrieved, the audio file automatically opens and plays using the applicable media application installed on your computer. For media applications you can use, see Requirements/Recommendations.

**Viewing and Editing Details of a Recording**

The ISR Dashboard allows you to view and edit specific details and metadata of a recording if required. From a Recording’s Details page, you can:

- Play a recording.
- Assign custom data fields to a recording.
- Specify whether or not the recording is completed.
- Assign a length of time, in hours/minutes that the reviewer spent reviewing/transcribing the recording.
- Specify notes pertaining to the recording.
- Assign a rating to the recording.
- Create a category for which to place the recording.
- Transcribe the conversation that took place on the recording.

To play a recording from the details page:

1. After logging into the ISR Dashboard, click **Find Recordings** on the Home Page (or **Recordings** on the main menu bar). The Recordings page displays.
2. Choose a recording and click the Details icon. The following dialog box displays.

The following table describes each field on the Recording Details page.

<table>
<thead>
<tr>
<th>Column Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recording</td>
<td>Specifies the file name of the recording assigned by the system or by the device that invoked the recording. You can click this field to play the recording.</td>
</tr>
<tr>
<td>Account Name</td>
<td>Specifies the Account name associated with the recording.</td>
</tr>
<tr>
<td>Session ID</td>
<td>Specifies the unique X-ISR-UCID for this recording.</td>
</tr>
<tr>
<td>From</td>
<td>Specifies the From SIP URI. This is the URI from where the call session was coming.</td>
</tr>
<tr>
<td>To</td>
<td>Specifies the To SIP URI. This is the URI to where the call session was destined.</td>
</tr>
<tr>
<td>Duration</td>
<td>Specifies the length of time, in seconds, of the recording.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Specifies the date and GMT time when the active session began.</td>
</tr>
</tbody>
</table>

To play the recording, click the recording file name.

When the recording is retrieved, the audio file automatically opens and plays using the applicable media application installed on your computer. For media applications you can use, see Requirements/Recommendations.

You can display additional recording details, session metadata, and session participant metadata if required. Refer to the following paragraphs for information about session metadata.

**Recording Details**

The ISR allows you to assign specific information to each recording that can be used to identify and analyze calls. You can save this information to be reviewed at a later time. You can display the additional details and add specific information about a recording by clicking **Details** on the Recording Details page.

For each recording stored in the Recording list, you can perform the following:

- Specify Custom Data Fields for the recording
- Apply a score to the call session (a rating on a scale from 1 to 10 stars, with 1 being the worst session and 10 being the best session). The score is at the discretion of the Administrator or User that is scoring the recording.
- Specify whether or not the call session completed.
- Specify the number of hours spent on the call session.
• Write notes about the call session.
• Transcribe the conversation that took place in the call session.

After specifying and saving this information, the data is attached to the applicable recording and stays with the recording even when the recording is archived. Administrators and users can create reports against the call scoring information in the database.

**Note:** To add or change detailed information about a recording, the user must have permission privileges for the Account’s route associated with the recording. To provide permission to add Custom Data Fields, see Custom Data. To provide permission to set “Complete Transaction”, “Notes/Transcription”, and “Rating”, see Recording, Editing Permissions.

**To display and specify details:**

1. On the Recordings page, choose a recording and click the Details icon. The following Recording Details page displays.

![Recording Details](image)

2. Click Details. The following information displays.

![Details](image)

The **RSS** field indicates the RSS that received the call session for the recording.

The **RSS Ingress Call ID** field indicates the call-id received in the header of the initial SIP INVITE.

3. **Custom Data Field 1** through **Custom Data Field 4**—Specify a custom data value to associate with this recording. This is information that should be specific to this recording. Valid values are alpha-numeric characters.

**Note:** The Custom Data Fields 1 through 4 must be enabled for editing. For more information about entering values and enabling the Custom Data Fields, see Custom Data.
4. **Complete Transaction**—Select whether or not the call session is completed for this recording. For example, if a caller calls into a Technical Support Center for problems with his PC, the call is recorded. If the problem was not resolved on the initial call session, the reviewer can select “No” for the Complete Transaction field, indicating that the problem was not resolved on this call. Valid values are:

- No (default) - Call session and this recording are not yet complete.
- Yes - Call session and recording are complete.

**Note:** The Complete Transaction field must be enabled for editing. For more information about enabling this field for editing, see Recording, Editing Permissions.

5. **Hours**—Enter the length of time, in hours/minutes that the reviewer spent reviewing/transcribing the recording. Valid values are in decimal format using numeric characters. For example, 6.15, where 6 indicates the hours and 15 indicates 1/4 hour.

6. **Rating**—Click on a star to rate the recording. This is a score that you can assign to this recording based on a level from 1 star to 5 stars, with 1 being the worst call session, and 5 being the best call session. When all stars are blank, no rating is assigned to the recording.

**Note:** The Rating field must be enabled for editing. For more information about enabling this field for editing, see Recording, Editing Permissions.

7. **Category**—Enter a category name to associate with the recording, and press <Tab>. Valid values are alpha-numeric characters.

   A category bubble displays in the Category field. This feature provides easy recording searches based on category rather than individual recordings.

   To create additional categories to associate with the current recording, repeat Step 7.

8. **Notes**—Enter notes pertaining to the call session for the current recording. Adding more than 135 characters in this box displays scroll bars in the window that allow you to scroll through multiple screens of the note. Valid values are alpha-numeric characters.

**Note:** The Notes field must be enabled for editing. For more information about enabling this field for editing, see Recording, Editing Permissions. Enabling the Notes field automatically enables the Transcription field.

9. **Transcription**—Enter the conversation that took place on the call session that pertains to the current recording. Adding more than 135 characters in this box displays scroll bars in the window that allow you to scroll through multiple screens of the transcription. Valid values are alpha-numeric characters.

10. Click **Save Changes** to save the details for the recording.

### Archiving Recordings Permanently

You can view whether or not a recording is archived by clicking **File Location** on the Recordings Details page.

You can also flag a recording to remain archived permanently.

**To flag a recording to never expire:**

1. After logging into the ISR Dashboard, click **Find Recordings** or click **Recordings** in the top menu bar.

2. Choose the recording you want to flag and click the Details icon.
The Recording’s detail page displays.

3. Click the **File Location** link.

4. **Store Indefinitely**—Check the box to ensure this recording is never deleted due to expiration.

5. Click **Save Changes**.

### Recording Session Metadata

You can view specific metadata information about a recording by clicking **Session Metadata** on the Recording Details page.

The ISR supports a value in the SIP INVITE header called X-ISR-UCID, which is used to identify incoming calls. X-ISR-UCID uses Unique Caller ID (UCID) and assigns a unique number to a call when it enters the network to provide uniform data-tracking of all ingress calls on that network. This unique ID is also used in egress SIP calls that are passed through the network or stored as session data on the CIS.

The value of this unique ID is stored in the lookup tables with the session data on the CIS for recording control, and can be viewed in the meta-data details of a recording and used as a means of searching for a recording.

The fields in the SIP Header for this feature are:

- **ingress_callid** - RSS uses the call-id in the SIP Header of the initial INVITE to populate this field.
- **egress_callid** - RSS initiates a second call leg (egress) for pass-through (or Record & Save) configurations and uses the new call leg’s call-id to populate this field. (When the RSS is acting as a B2BUA).
- **isr_ucid** - RSS matches the X-ISR-UCID to the SIP Header, then populates this field.

**Note:** The ingress_callid is always populated. The egress_callid may not be populated for calls with only one participant. The isr_ucid is only populated for calls where the X-ISR-UCID SIP header is present in the ingress INVITE.

The following illustration shows the call flow using the call control unique ID on the NN-ISR.

1. The ISR receives a SIP INVITE with optional X-ISR-UCID header.
2. The VMG_CHANNEL_LOOKUP table is updated with the ingress_callid and isr_ucid.
3. The ISR sends an INVITE to the Session Agent and updates the egress_ucid if applicable.

4. Recording control is now possible from a third-party application using either the isr_ucid, ingress_ucid, or the egress_ucid.

You can configure the X-ISR-UCID header field using the standard RSS configuration file, vmgConfig.xml. This allows you to customize the SIP header field without having to make changes to your application. For more information on configuring X-ISR-UCID in the vmgConfig.xml file, see the Interactive Session Recorder Installation Guide.

To view Session Metadata:

1. On the Recordings page, choose a recording and click the Details icon. The following Recording Details page displays.

2. Click Session Metadata. The following information displays.

The SIPREC Session ID field displays the SIP Recording Session ID assigned to the call recording session at the time the call was received by the RSS.

The Start Time field displays the date and GMT time the call recording session began. The date and time are based on the time zone configured for the Account.

The Session Extension Metadata displays the Unique Caller ID (ucid) assigned by the ISR and indicates the ID of the incoming call.

Recording Session Participant Metadata

You can view specific participant metadata information about a recording by clicking “Session Participant Metadata” on the Recording Details page.

To view Session Participant Metadata:
1. On the Recordings page, choose a recording and click the Details icon. The following Recording Details page displays.

![Recording Details](image)

2. Click **Session Participant Metadata**. The following information displays.

![Session Participant Metadata](image)

The following table describes each field on the Session Participant Metadata page.

<table>
<thead>
<tr>
<th>Column Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIPREC Participant ID</td>
<td>Specifies the ID of the incoming caller who is the SIPREC participant on the recording.</td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the From SIP URI name. This is the URI from where the call session was coming.</td>
</tr>
<tr>
<td>AOR</td>
<td>Specifies the address of record (AOR) associated with the call that was recorded.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Specifies the date and GMT time when the active session recording began.</td>
</tr>
<tr>
<td>End Time</td>
<td>Specifies the date and GMT time when the active session recording ended.</td>
</tr>
<tr>
<td></td>
<td>Displays additional metadata information about the participant if it exists.</td>
</tr>
</tbody>
</table>
3. Choose a SIPREC Participant ID and click the Details icon to display additional metadata information about the participant. The following box displays.

![Participant Extension Metadata](image)

Information in this box can include metadata for:

- `apkt:ucid`
- `callingPartyNumber`
- `extTrackingID`
- `calledPartyNumber`
- `ServiceProviderID`
- `newExtTrackingID`
- `userID`
- `apkt:in-realm`
- `groupID`
- `apkt:P-Asserted-Identity`
- `callID`
- `apkt:Diversion`
- `apkt:request-uri`

For more information about these parameters, see Recording Search by Session.

### Displaying DTMF Data in Recording’s Details

You can configure the ISR to display DTMF details within a call’s recording details for digits transmitted via RFC 2833 and SIP INFO. The DTMF Logging parameter has been created which allows you to specify whether or not to display DTMF details on either a per-route or per-account basis.

**To enable the ISR to display DTMF details for a particular route:**

1. After logging into the ISR Dashboard, click Edit System Configurations or click Admin in the top menu bar.
2. Click Manage Routes.
   - A list of all routes configured on the ISR displays.
3. Click the route on which you are enabling DTMF details.
4. Click Route Advanced Configuration.
5. **Record DTMF**—Select whether or not to display DTMF details. Valid values are:
   - Use account or system default—This route defaults to its account’s behavior. This is the default value.
   - No—No DTMF details appear in the recording details.
   - Yes—DTMF details appear in the recording details.

6. Click **Update**.

**To enable the ISR to display DTMF details for a particular account:**

1. After logging into the ISR Dashboard, click **Edit System Configurations** or click **Admin** in the top menu bar.
2. Click **Manage Accounts**.
   A list of all accounts configured on the ISR displays.
3. Click the account on which you are enabling DTMF details.
4. Click **Account Route Defaults**.

![Account Route Defaults](image)

5. **Record DTMF**—Select whether or not to display DTMF details. Valid values are:
   - No—No DTMF details appear in the recording details. This is the default value.
   - Yes—DTMF details appear in the recording details.

6. Click **Update**.

**To view DTMF data in recording details:**

1. After logging into the ISR Dashboard, click **Find Recordings** or click **Recordings** in the top menu bar.
2. Choose the recording you want to view and click the Details icon.
   The Recording’s detail page displays.
3. Click **DTMF Events**. The DTMF data appears.

![DTMF Events Graph](image)

You can zoom in on a particular area of the DTMF Events graph by highlighting the section you want to view. To get back to the original graphical view, click **Reset zoom**.

**Deleting a Recording**

You can delete a recording from the ISR Dashboard as required.

**To delete a Recording:**

1. After logging into the ISR Dashboard, click **Find Recordings** on the Home Page (or **Recordings** on the main menu bar). The Recordings page displays.

![Recordings Page](image)

2. Choose a Recording from the Recordings page and click the Delete icon. The following prompt displays:

   “Are you sure you want to delete this recording?”
3. Click **OK** to delete the Recording from the ISR database or click **Cancel** to cancel the delete function.

**Warning:** Once a recording is deleted, it cannot be recovered. The file is deleted from disk and the metadata is removed from the database.
10 Managing Reports

Introduction

The ISR allows you to generate call usage and billing statistical reports using date and route filters. This chapter describes the type of reports you can generate and filters you can use to generate the reports.

Manage Reports

The ISR provides the following types of reports you can generate:

- **Usage Reports** - Generates a report that includes call recorder usage information by date range and/or by route.
- **Billing Reports** - Generates a report that includes billing information by date range and/or by route.

You can run these reports for the current month or the previous month, or specify a date range.

You can access the Reports from the Home page by clicking **Build A Report** (or by clicking **Reports** on the top menu bar).
The Reports page allows you to build Usage and/or Billing Reports based on the filters you set in the **Search Date** and **Select Route** fields.

The following paragraphs provide information about building Usage and Billing reports.

### Usage Reports

Usage Reports show information about calls that use routes configured on your ISR. Usage Reports include:

- Route used for calls
- Number of sessions provisioned on the route
- Number of provisioned burst sessions on the route
- Total number of calls initiated using the route
- Number of calls made during peak time on the route
- Number of calls that used burst sessions on the route
- Number of calls rejected on the route

You can filter the call data by month or by date range, and select a single or multiple routes to display in the report.

**To generate a Usage Report:**
1. After logging into the ISR Dashboard, click **Build a Report** on the Home Page (or **Reports** on the main menu bar). The Reports page displays.

2. **Search Date**—Select whether you want to generate a report by the month or by date range.

   **To generate a report by month:**

   3. Select **By Month**.

   4. In the drop-down box, select the month for which you want to generate the report. Valid values are dependant on the dates for calls stored in the ISR database.

   **To generate a report by range:**

   5. Select **By Range**. The “From Date” and “To Date” fields display.

   6. **From Date**—Click the cursor in the text box or click the Calendar icon to display the calendar.

   7. Click the date from where you want to begin to include the report data. Use the arrow keys in the calendar to change months.

   8. **To Date**—Click the cursor in the text box or click the Calendar icon to display the calendar.

   9. Click the date from where you want to end the inclusion of the report data. Use the arrow keys in the calendar to change months.

   **To select a route:**

   10. **Select Route**—Select a route or routes to include in the report. Valid values are dependant on the routes currently configured in the ISR database.

      **Note:** To select multiple routes, click on a route in the selection box, press and hold the <Ctrl> key, and select additional routes.

   11. Click **Usage Reports**. The **Generate Report** button displays.

   12. Click **Generate Report** to generate the Usage Report. The following report displays.
The Usage Report displays the information in bar graph format at the top of the page, and in data format at the bottom of the page.

The following table identifies the information in the bar graph section of the report.

### Usage Report Bar Graph Descriptions

<table>
<thead>
<tr>
<th>Graph Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routes (Policies)</td>
<td>Indicates the route selected for this report.</td>
</tr>
<tr>
<td>Calls</td>
<td>Indicates the number of calls on this route.</td>
</tr>
<tr>
<td>Recorded</td>
<td>Indicates total number of recorded calls during the reported period.</td>
</tr>
<tr>
<td>Rejected</td>
<td>Indicates total number of rejected calls during the reporting period.</td>
</tr>
<tr>
<td>Burst</td>
<td>Indicates total number of burst calls during the reporting period. Burst calls are calls handled by the Burst Ports.</td>
</tr>
<tr>
<td>Peak</td>
<td>Indicates maximum number of simultaneous calls during the reporting period.</td>
</tr>
<tr>
<td>Total Calls</td>
<td>Indicates total number of calls during the reporting period.</td>
</tr>
</tbody>
</table>

The following table describes each column in the data format section of the report.

### Usage Report Data Format Descriptions

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route</td>
<td>Route(s) included in this Usage Report.</td>
</tr>
<tr>
<td>Capacity</td>
<td>Total concurrent sessions allocated to the route.</td>
</tr>
<tr>
<td>Burst Capacity</td>
<td>Number of concurrent sessions available for call recording when the provisioned capacity has been depleted.</td>
</tr>
<tr>
<td>Total Sessions</td>
<td>The total number of sessions for this reporting period.</td>
</tr>
<tr>
<td>Peak Sessions</td>
<td>The maximum number of concurrent sessions that occurred during this reporting period.</td>
</tr>
<tr>
<td>Burst Sessions</td>
<td>The total number of sessions that occurred after the provisioned capacity had been depleted.</td>
</tr>
<tr>
<td>Rejected</td>
<td>Total number of rejected sessions on this route during this reporting period.</td>
</tr>
</tbody>
</table>
After you have generated a usage report, you can click on a specific route within the report to view a day by day breakdown of the statistics.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Rejected</td>
<td>The total number of rejected sessions by the ISR during this reporting period.</td>
</tr>
<tr>
<td>Account Rejected</td>
<td>The total number of rejected sessions by this account during this reporting period.</td>
</tr>
<tr>
<td>Route Rejected</td>
<td>The total number of rejected sessions by this route during this reporting period.</td>
</tr>
<tr>
<td>Recorded</td>
<td>Total number of recorded sessions on this route during this reporting period.</td>
</tr>
</tbody>
</table>

**Billing Reports**

Billing Reports show information about calls that use the routes configured on your ISR. Billing Reports include:

- Route used for calls
- Number of sessions provisioned on the route
- Number of provisioned burst sessions on the route
- Total number of calls initiated using the route
- Number of calls made during peak time on the route
- Number of calls that used burst sessions on the route
- Number of calls rejected on the route

You can filter the call data by month or by date range, and select a single or multiple routes to display in the report. You can use this information for billing purposes as required.

**To generate a Billing Report:**
1. After logging into the ISR Dashboard, click **Build a Report** on the Home Page (or **Reports** on the main menu bar). The Reports page displays.

![ISR Reports Page]

2. **Search Date**—Select whether you want to generate a report by the month or by date range.

   **To generate a report by month:**

3. Select **By Month**.

4. In the drop-down box, select the month for which you want to generate the report. Valid values are dependant on the dates for calls stored in the ISR database.

   **To generate a report by range:**

5. Select **By Range**. The “From Date” and “To Date” fields display.

6. **From Date**—Click the cursor in the text box or click the Calendar icon to display the calendar.

7. Click the date from where you want to begin to include the report data. Use the arrow keys in the calendar to change months.

8. **To Date**—Click the cursor in the text box or click the Calendar icon to display the calendar.

9. Click the date from where you want to end the inclusion of the report data. Use the arrow keys in the calendar to change months.

   **To select a route:**

10. **Select Route**—Select a route or routes to include in the report. Valid values are dependant on the routes currently configured in the ISR database.

    **Note:** To select multiple routes, click on a route in the selection box, press and hold the `<Ctrl>` key, and select additional routes.

11. Click **Billing Reports**. The **Generate Report** button displays.

12. Click **Generate Report** to generate the Billing Report. The following report displays.
The Billing Report displays the information in bar graph format at the top of the page, and in data format at the bottom of the page.

The following table identifies the information in the bar graph section of the report.

**Billing Report Bar Graph Descriptions**

<table>
<thead>
<tr>
<th>Graph Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routes (Policies)</td>
<td>Indicates the route selected for this report.</td>
</tr>
<tr>
<td>Calls</td>
<td>Indicates the number of calls on this route.</td>
</tr>
<tr>
<td>Recorded</td>
<td>Indicates total number of recorded calls during the reported period.</td>
</tr>
<tr>
<td>Rejected</td>
<td>Indicates total number of rejected calls during the reporting period.</td>
</tr>
<tr>
<td>Burst</td>
<td>Indicates total number of burst calls during the reporting period. Burst calls are calls handled by the Burst Ports.</td>
</tr>
<tr>
<td>Peak</td>
<td>Indicates maximum number of simultaneous calls during the reporting period.</td>
</tr>
<tr>
<td>Total Calls</td>
<td>Indicates total number of calls during the reporting period.</td>
</tr>
</tbody>
</table>

The following table describes each column in the data format section of the report.

**Billing Report Data Format Descriptions**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of route policy (i.e., To, From, or To/From).</td>
</tr>
<tr>
<td>Pattern</td>
<td>The route pattern that the RSS looks for when searching for a route policy.</td>
</tr>
<tr>
<td>Capacity</td>
<td>Total concurrent sessions allocated to the route.</td>
</tr>
<tr>
<td>Burst Capacity</td>
<td>Number of concurrent sessions available for call recording when the provisioned capacity has been depleted.</td>
</tr>
<tr>
<td>Total Sessions</td>
<td>The total number of sessions for this reporting period.</td>
</tr>
<tr>
<td>Peak Sessions</td>
<td>The maximum number of concurrent sessions that occurred during this reporting period.</td>
</tr>
<tr>
<td>Burst Sessions</td>
<td>The total number of sessions that occurred after the provisioned capacity had been depleted.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Rejected</td>
<td>Total number of rejected sessions on this route during this reporting period.</td>
</tr>
<tr>
<td>System Rejected</td>
<td>The total number of rejected sessions by the ISR during this reporting period.</td>
</tr>
<tr>
<td>Account Rejected</td>
<td>The total number of rejected sessions by this account during this reporting period.</td>
</tr>
<tr>
<td>Route Rejected</td>
<td>The total number of rejected sessions by this route during this reporting period.</td>
</tr>
<tr>
<td>Recorded</td>
<td>Total number of recorded sessions on this route during this reporting period.</td>
</tr>
</tbody>
</table>
11 Remote Archival Webservice

Introduction

Remote Archival allows customers of hosted call recording providers to pull their recordings to a premise location. Utilizing a secure connection between the premise and service provider applications, a Remote Archival client connects to the Remote Archival Webservice and retrieves all recordings for a single account configured on the host platform.

The Remote Archival process includes:

1. Moving recording files to a remote file system. The files may be optionally deleted from the source RSS/NAS/SAN after the client confirms a successful delivery.
2. Moving recording metadata for the configured account, including the standard recording data from the recordings table, SIPREC metadata, and ISR custom fields, to a remote store. The data may be optionally deleted from the source index after a successful push.

To enable the Remote Archival Webservice, you must configure at least one Remote Archival user and at least one account. This user’s username and password are required in the client requests.

Configuring Remote Archival Users

Remote Archival users are configured under the ISR Dashboard’s Manage Users link.

Note: A Remote Archival user is specific to the Remote Archival Webservice only and cannot log into the ISR Dashboard.

To configure a Remote Archival user:

1. After logging into the ISR Dashboard, click Admin in the main menu (or Edit System Configurations on the Home page).
2. Click Manage Users. The Users page displays.
3. Click **New User**. The New User page appears.

4. **Primary Account**—Select the primary account to assign to this Remote Archival user. Valid values are dependant on the accounts currently configured in the ISR. The default value is **System**.

5. **User Name**—Enter a name for this Remote Archival user. Valid values are alpha-numeric characters.

6. **Email**—Enter the user’s email address. This is the value the user enters in the **Email** field on the login page. Valid values are alpha-numeric characters and it is usually a domain name in the format:

   `<username>@<host server>.<DNS (.com, .org., .net., .edu)>`

   For example, jsmith@abc.com.

7. **Password**—Enter a password for the user to specify when logging into the Remote Archival Webservice. By default, the password must contain letters and numbers, have at least one uppercase letter, and be at least 8 characters long. Valid values are alpha-numeric and special characters.

8. **Confirm Password**—Re-enter the password to verify you entered the password correctly.

9. **Preferred Timezone**—Select the time zone associated with the location of the Remote Archival user. This value is an offset of Greenwich Mean Time (GMT). The following table provides the valid values and default for this field.

**Time Zone Table**

<table>
<thead>
<tr>
<th>Time Zone</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMT-12 (default)</td>
<td>IDLW - International Date Line West</td>
</tr>
<tr>
<td>GMT-11</td>
<td>NT - Nome</td>
</tr>
<tr>
<td>GMT-10</td>
<td>AHST - Alaska-Hawaii Standard</td>
</tr>
<tr>
<td></td>
<td>CAT - Central Alaska</td>
</tr>
<tr>
<td></td>
<td>HST - Hawaii Standard</td>
</tr>
<tr>
<td>GMT-9</td>
<td>YST - Yukon Standard</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Location</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| GMT-8     | PST - Pacific Standard  
 Los Angeles, CA, USA |
| GMT-7     | MST - Mountain Standard |
| GMT-6     | CST - Central Standard  
 Mexico City, Mexico  
 Saskatchewan, Canada |
| GMT-5     | EST - Eastern Standard  
 Bogota  
 Lima, Peru  
 New York, NY, USA |
| GMT-4     | AST - Atlantic Standard  
 Caracas  
 La Paz |
| GMT-3     | Brasilia, Brazil  
 Buenos Aires, Argentina  
 Georgetown, Guyana |
| GMT-2     | AT - Azores |
| GMT-1     | WAT - West Africa  
 Azores, Cape Verde Islands |
| GMT       | London, England  
 Dublin, Ireland  
 Edinburgh, Scotland  
 Lisbon, Portugal  
 Reykjavik, Iceland  
 Casablanca, Morocco |
| GMT+1     | CET - Central European  
 Paris, France  
 Berlin, Germany  
 Amsterdam, The Netherlands  
 Brussels, Belgium  
 Vienna, Austria  
 Madrid, Spain  
 Rome, Italy  
 Bern, Switzerland  
 Stockholm, Sweden  
 Oslo, Norway |
| GMT+2     | EET - Eastern European  
 Athens, Greece  
 Helsinki, Finland  
 Istanbul, Turkey  
 Jerusalem, Israel  
 Harare, Zimbabwe |
| GMT+3     | BT - Baghdad  
 Kuwait  
 Nairobi, Kenya  
 Riyadh, Saudi Arabia  
 Moscow, Russia |
<p>| GMT+4     | Abu Dhabi, UAE |</p>
<table>
<thead>
<tr>
<th>Time Zone</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMT+5</td>
<td>Kazakhstan (western-Aqtau)</td>
</tr>
<tr>
<td></td>
<td>Maldives (Male)</td>
</tr>
<tr>
<td></td>
<td>Pakistan (Islamabad, Karachi)</td>
</tr>
<tr>
<td></td>
<td>Russia</td>
</tr>
<tr>
<td></td>
<td>Tajikistan (Dushanbe)</td>
</tr>
<tr>
<td></td>
<td>Turkmenistan (Ashkhabat)</td>
</tr>
<tr>
<td></td>
<td>Uzbekistan (Tashkent)</td>
</tr>
<tr>
<td></td>
<td>India (New Delhi, Calcutta)</td>
</tr>
<tr>
<td></td>
<td>Sri Lanka (Colombo)</td>
</tr>
<tr>
<td></td>
<td>Nepal (Katmandu)</td>
</tr>
<tr>
<td>GMT+6</td>
<td>Bangladesh</td>
</tr>
<tr>
<td></td>
<td>Bhutan</td>
</tr>
<tr>
<td></td>
<td>Kazakhstan</td>
</tr>
<tr>
<td></td>
<td>Kyrgyzstan</td>
</tr>
<tr>
<td></td>
<td>Sri Lanka (formerly Ceylon)</td>
</tr>
<tr>
<td>GMT+7</td>
<td>Cambodia</td>
</tr>
<tr>
<td></td>
<td>Christmas Island</td>
</tr>
<tr>
<td></td>
<td>Indonesia</td>
</tr>
<tr>
<td></td>
<td>Lao</td>
</tr>
<tr>
<td></td>
<td>Thailand</td>
</tr>
<tr>
<td></td>
<td>Vietnam</td>
</tr>
<tr>
<td>GMT+8</td>
<td>CCT - China Coast</td>
</tr>
<tr>
<td>GMT+9</td>
<td>JST - Japan Standard</td>
</tr>
<tr>
<td>GMT+10</td>
<td>GST - Guam Standard</td>
</tr>
<tr>
<td>GMT+11</td>
<td>Solomon Islands</td>
</tr>
<tr>
<td>GMT+12</td>
<td>IDLE - International Date Line East</td>
</tr>
<tr>
<td></td>
<td>NZST - New Zealand Standard</td>
</tr>
<tr>
<td></td>
<td>Wellington, New Zealand</td>
</tr>
<tr>
<td></td>
<td>Fiji</td>
</tr>
<tr>
<td></td>
<td>Marshall Islands</td>
</tr>
</tbody>
</table>

10. **User Type**—Select **Remote Archiver User** from the drop-down list.
11. Click **Create**.

### Configuring Remote Archival Accounts

In addition to creating a Remote Archival-specific user to enable the Remote Archival Webservice, you must also configure it within the user’s associated account.

**To enable Remote Archival on an account:**

1. After logging into the ISR Dashboard, click **Admin** in the main menu (or **Edit System Configurations** on the Home page).
2. Click **Manage Accounts**. The Accounts page displays.
3. Either select an existing account on which to enable Remote Archival or click **New Account**.

   **Note:** If you are creating a new account, configure it as you would any account. For more information on configuring accounts, see Chapter 3, Managing Realms/Accounts.

4. Click **Account Remote Archiver Server**.

5. **Client IP Address**—Enter the Remote Archival client’s IP address.

6. **Remove Recordings**—When set to **On**, the associated metadata is deleted from the Index after the client confirms a successful delivery. Valid values are **On** and **Off**. The default setting is **Off**.

7. **Max Allowed Attempts**—The maximum number of unsuccessful downloads of an ISR recording until the recording is marked as failed and ignored in future Remote Archival “getList” requests. The default setting is 3.

8. Click **Update**.

   **Note:** Remote Archival Webservice logging information can be found on the rWebservice host’s /cxc_common/ISR/RemoteArchival/RemoteArchivalWebservice.log file.

---

**Running the Remote Archival Client**

The Remote Archival client is an application created specifically for developer testing purposes.

**To run the Remote Archival client in a Windows environment:**

1. Verify Java Version 5 or greater is installed on the Remote Archival client host.
2. Unzip the file “Remote Archival Client Development-Only Version <number>.zip to the install directory.
3. From a command line, change to the install directory and, depending on the operating system, execute **run.bat** or **run.sh** and hit <Enter>.
4. Follow the usage information provided in the response.
12

Securing the ISR

Introduction

This chapter describes how to configure security on the ISR.

SSL-Enabling the ISR Dashboard

You can enable serving pages with SSL to force SSL cookies. In the ISR, by default cookies are not forced through the Secure Sockets Layer (SSL).

To force the SSL cookies, you may need to generate a certificate and you must enable serving of pages in SSL.

To enable serving pages with SSL to force SSL cookies:

1. Enable SSL in nginx by editing the nginx configuration file (/opt/nginx/conf/nginx.conf) and edit the following SSL config lines to the following (edit paths and remove the ‘#’ sign).

   # listen 443;
   # ssl on;
   # ssl_certificate /opt/nginx/conf/<pem_keystore_file>;
   # ssl_certificate_key /opt/nginx/conf/<pem_keystore_file>;
   # keepalive_timeout 60;

2. Add the following line below keepalive_timeout 60:.

   ssl_protocols TLSv1 TLSv1.1 TLSv1.2;

3. Confirm the location of the SSL certificate and key currently being used.

4. Save the changes in the editor:

5. Enable secure cookies in the ISR Dashboard:

   • Edit /var/www/dashboard/current/config/initializers/session_store.rb
   • Inside of “actionController::Base.session = {.....}”, add the new line
     :secure => true
   
   Note: You must add a comma to the end of the line for this to work properly.

   • Restart nginx by entering the command:
     service nginx restart

6. Edit the following line in the iptables configuration file (/etc/sysconfig/iptables) to open port 443:

   Change From:  
   -A INPUT -m state --state NEW -m tcp --dport 80 -j ACCEPT
   Change To:
   -A INPUT -m state --state NEW -m tcp --dport 443 -j ACCEPT

7. Restart the iptables service by executing the following command:

   service iptables restart

8. After the restart, confirm access of the application using HTTPS in a browser.
Generating a PEM Format Keystore

Generate a PEM format keystore if needed.

**Note:** Oracle recommends creating the keystore using Java 7.

1. The following is an example command.

   ```bash
   >C:\Program Files\java\jre7\bin\keytool\keytool -genkeypair -alias alias_of_choice -keyalg RSA -ext san=ip:dashboard_ip -keystore <keystore_path>
   ```

   2. Using the keystore created by keytool, create the PKCS12 file with the following command:

   ```bash
   keytool -v -importkeystore -srckeystore <keystore_path> -srcalias alias_of_choice -destkeystore <pkcs12_keystore_path> -deststoretype PKCS12
   ```

   Once the PKCS12-formatted keystore has been successfully created, copy the PKCS12 keystore file to the ISR Dashboard host. From the Dashboard host, execute the following:

   3. Using openssl, create the PEM format keystore by following this example command:

   ```bash
   # openssl pkcs12 -in <pkcs12_keystore_file> -out <keystore_filename>.pem
   ```

   4. Once the .pem keystore is available, copy the file to the /opt/nginx/conf directory.

SSL-Enabling the Remote Archival Webservice

You can configure the Remote Archival Webservice to handle HTTP requests over SSL.

**To enable SSL on the Remote Archival Webservice:**

1. Create a key on server. To do this, on the rWebservice host, generate the keystore by executing the following command (and follow the instructions).

   ```bash
   /opt/jdk 1.6.0 24/bin/keytool -genkey -alias alias_of_choice -keyalg RSA -keystore /cxc_common/ISR/RemoteArchival/server.keystore
   ```

2. Import the certificate into the client’s truststore. To do this, on the Remote Archival Webservice host export the certificate by executing the following command (and follow the instructions).

   ```bash
   /opt/jdk 1.6.0 24/bin/keytool -export -keystore /cxc_common/ISR/RemoteArchival/server.keystore -alias alias chosen -file /cxc_common/ISR/RemoteArchival/raws.crt
   ```

   Transfer the newly-created file, raws.crt, from the rWebservice host to the Remote Archival Client host.

   If the Remote Archival Client is a Java-based application, execute the following command (and follow the instructions).

   ```bash
   /opt/jdk 1.6.0 24/bin/keytool -import -alias alias chosen -file /cxc_common/ISR/raws2.crt -keystore /opt/jdk 1.6.0 24/jre/lib/security/cacerts
   ```

   Note: The password for the keystore is required and, by default, is “changeit”. To change the password, execute the following command:

   ```bash
   keytool -storepass -new <new_storepass> -keystore <JAVA_HOME>/jre/lib/security/cacert
   ```

3. Edit and verify the RA Client’s run.sh or run.bat files so that the -k parameter matches the keystore path.

   **Note:** Some troubleshooting tips on the keystores:

   - Your client keystore path is not valid.
4. Configure the Remote Archival Webservice for SSL-only requests. To do this edit
/opt/jboss/standalone/configuration/standalone.xml.

Within the section marked by the following tag:

```xml
<subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-server="default-host" native="false">
  <connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https" secure="true">
    <ssl name="ssl" key-alias="alias chosen" password="key password" certificate-key-file="/cxc_common/ISR/RemoteArchival/server.keystore" protocol="TLSv1,TLSv1.1,TLSv1.2"/>
  </connector>
</subsystem>
```

Note: `<key_password>` refers to the password provided during the instructions to
generate, export, and import the key.

For JBoss to stop listening on port 8080, remove (or comment) the following lines in
standalone.xml:

```xml
<connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="http"/>
```

5. Modify the Linux firewall to allow port 8443 instead of 8080 by editing:

   `/etc/sysconfig/iptables`

   Change the following line:

   ```
   -A INPUT -m state --state NEW -m tcp --dport 8080 -j ACCEPT
   ```

   To:

   ```
   -A INPUT -m state --state NEW -m tcp --dport 8443 -j ACCEPT
   ```

   Restart the iptables service with the following command:

   `service iptables restart`

   Restart Jboss with the following command:

   `service jboss restart`

6. Modify the ISR API connection parameter for the RAWS to use HTTPS. To do this edit
   `/opt/jboss/standalone/deployments/RemoteArchival.war/WEB-INF/web.xml`. Find the
   section for baseApiUrl and change the param-value.

   Change the following line:

   ```
   http://<localhost>:8080/IsrApi/rest/
   ```

   To:

   ```
   https://<localhost>:8443/IsrApi/rest/
   ```

   It should now look like the following:

   ```xml
   <context-param>
     <param-name>baseApiUrl</param-name>
     <param-value>https://localhost:8443/IsrApi/rest/</param-value>
   </context-param>
   ```
7. To confirm the new configuration, point a web browser to the Remote Archival Webservice JBoss root URL at:

   https://<RA Webservice IP>:8443/IsrApi/

   and confirm that it is accessible.

Adding User Accounts on the RSS

After the RSS has been installed, by default it has no configured users or authorization at the login. Once you have at least one user configured, authorization is limited to configured users only.

To configure users and authorization you must create a permissions group, create a user, and then assign the user to the appropriate permissions group.

The following is an example of configuring users and authorization via the CLI.

```
NN-ISR>config access
  config access>config permissions basic
  Creating 'permissions basic'
  config permissions basic>exit
  Do you want to commit your changes before you exit (y or n)? y
  Do you want to update the startup configuration (y or n)? y

NN-ISR>config access
  config access>config users
  Creating 'users'
  config users>config user testuser
  Creating 'user testuser'
  config user testuser>set password
  password: ******************
  confirm: ******************
  config user testuser>set permissions access\permissions basic
  config user testuser>exit
  Do you want to update the startup configuration (y or n)? y

NN-ISR>
```

SSL-Enabling the RSS ISR API

You can configure the RSS ISR API to handle HTTP requests over SSL.

To enable SSL on the RSS ISR API:

1. Create a key on the RSS. To do this, on the RSS host, generate the keystore by executing the following commands (and follow the instructions).

   mkdir /home/jboss
   keytool -genkey -alias <alias of choice> -keyalg RSA -keystore /home/jboss/.keystore

2. Configure the RSS for SSL (or to allow SSL-only requests), edit /usr/local/jboss-7.1.1/standalone/configuration/standalone.xml.

   Within the section marked by the following tab:

   <subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-server="default-host" native="false">
   Add:

   <connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https" secure="true">
   <ssl name="ssl" key-alias="<alias chosen>" password="<keystore password>" certificate-key-file="/home/jboss/.keystore" protocol="TLSv1,TLSv1.1,TLSv1.2"/>

```

Note: The <keystore_password> and <alias_chosen> values refer to the password provided and alias chosen in the instructions to generate the key in step 1.

3. Remove (or comment) the following lines in standalone xml for JBoss to stop listening on port 9000.

```xml
<connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="http"/>
```

4. Restart JBoss with the following command from the Linux CLI:

```
/etc/init.d/jboss restart
```

5. Confirm the configuration by pointing a browser to the RSS JBoss root URL:

```
https://<RSS IP>:8443/IsrApi/
```
A ISR Software Diagrams and Call Setup Sequence

Overview

This appendix contains a high-level, software architecture diagram of the ISR platform along with a set of ladder diagrams describing interaction of the software components. This is for informational purposes only.

ISR Software Architecture Diagram

The following is a diagram of the ISR software architecture.
Description of Components

The components of the ISR consist of the following:

- **RSS - Record Store Server**
- **CIS - Control Index Server**

Each of these components are described in the following paragraphs.

**Record Store Server (RSS)**

The RSS consists of the following components:

- **Call Manager** - Using call state, channel and route information, Call Manager handles account and platform-related call decisions.
- **SIP Agent** - Processor for SIP-related events.
- **Channel Map** - State storage and reference for active call information and available channels.
- **Local Route Cache** - Binary tree store of route-based information for call and recording decisions. Initializes reflecting the dashboard-driven route_config database table with periodic (configurable) updates mirroring changes in the table.
- **Call Stats Updater** - Processes call metrics and refreshes call and recording tables with call statistics.
- **XML-RPC Server** - Accepts and queues remote call and recording commands.
- **XML-RPC Agent** - Manages API requests and responses via XML-RPC.
- **RTP Port Manager** - Returns available RTP ports and maintains port status for SIP Agent.
- **Event Queue** - Prioritizes and stores call and other events.
- **Cache Manager** - Local audio store which makes available audio content such as busy messages and beeps during recording.
- **Mixer Channel** - RTP support for sending, receiving, buffering, transcoding and mixing audio which contains the following:
  - **RTP I/O** - RTP input and output stream handling.
  - **Audio Mixer** - Audio stream processing for injecting platform or route-specific audio.
  - **Recorder Thread** - Manages audio and file stream processing.
- **RSS API** - Offers ISR remote call and recording services along with resources for route and channel references in ISR database.
- **VoiceXML API** - VoiceXML resource for ISR API commands.
- **RSS API Servlet** - Service handles ISR XML-RPC API requests.
- **REST API** - REST resource for ISR API commands.
- **Archiver**
- **SIPREC** - Used to interact between a Session Recording Client (SRC) and a Session Recording Server (SRS).
  - **SIP Proxy** - SIP user agent. SIP Proxy acts as B2BUA if configured in pass-thru mode and acts as SIP Endpoint for conference mode and call parking mode. The proxy handles SIP signaling and keeps track of call states. It also maps two legs to a call session when acting as B2BUA. Once it receives a new call, the SIP Proxy gets routing and recording decisions from the Call Manager, then submits...
an event to Event Queue to be distributed to a Mixer that corresponds to the call channel.

- Codec Negotiator - Responsible for generating supported Codec list for SDP offers and answers to offers.

- SIPREC Processor - This component is responsible for processing SIPREC requests. When the SIP Proxy receives a SIPREC call, judging by multipart bodies, it passes call context and SIPREC Metadata to SIPREC process. The SIPREC Processor then parses the Metadata of the Recording Session (RS) into a structured data object. The SIPREC Processor, in turn, passes the call context back to SIP Proxy with flag set for detailed instructions on SIP signaling. Note: Final SIP action for SIPREC from SIP Proxy, afterward, is also affected by Call Manager.

Control Index Server (CIS)

The CIS consists of the following components:

ISR Database
ISR User Dashboard
ISR Administrator Dashboard

Sequence Diagrams

This section provides details about the ISR call setup for a single successful call. This is for informational purposes only.

Non-SIPREC Call

The following sequence diagram applies to the ISR configuration in non-SIPREC, pass-through, interactive voice response (IVR) skip mode. The call applies to a percentage-based recording route.

The simple call flow below reflects a single successful call which applies to a route configured for pass-through mode and recording of 100% of calls. The diagram highlights some of the features in the ISR, such as IVR-skip mode. Previously, the ISR architecture required a VoiceXML platform to make routing, recording and availability decisions. This information now resides locally in the Local Route Cache or is referenced in the database through API commands.
SIPREC Call

The following sequence diagram applies to the ISR configuration in SIPREC environment.
This appendix provides an overview of the ISR Media Converter (RMC) and provides procedures for editing locations that contain raw RTP files that require conversion for playback. It also includes a procedure for installing the RMC license.

About the ISR RMC

The ISR records sessions in several RTP codecs and handles the conversion and playback of most codecs using the RMC. This RMC is automatically installed as part of the RSS installation and runs on its own license. Contact your Oracle sales representative for more information about obtaining the RMC license.

The ISR RMC is a media converter that converts recordings from RTP packet data (".rpdd" formatted files) to Pulse Code Modulation (PCM) wave files (".wav" formatted files), for playback by the ISR Dashboard. It allows the ISR to record calls from multiple codecs, including G.729 and G.722. Consult the ISR Release Notes for a complete list of RTP codecs currently supported on the ISR.

In previous releases, the location configurations through the ISR Dashboard were associated only with archiving - the moving of recorded files and updating of the recording information in the database. Now each location also has a G.729 converter, or RMC, configuration to define which RMC has access to the files at that location. When a user plays a recording that is in raw RTP format (.rpdd formatted file), the dashboard makes a request to the RMC converter set for that file's location. Once the RMC converter is finished transcoding (to .wav format), the browser's media player plays the file.

ISR RMC License

This RMC is automatically installed when performing the RSS installations.

When you have obtained an RMC license for the ISR, you can install the license key to enable the RMC to work in your network.

Obtaining the RMC License Key

Use the following procedure to obtain and install the license key and enable RMC in your network.

To obtain the RMC license key:

1. SSH to your RSS.
2. At the “Login as” prompt, enter “root” and press <Enter>.
   
   Login as: root
   The password prompt displays.
3. At the “Password” prompt, enter “sips” and press <Enter>.
root@<hostname>'s password> sips
The following prompt and message display.
Net-Net ISR
Copyright (c) 2004-2012 Acme Packet Inc.
Username:
4. No username is required so press <Enter>.
Username: (leave blank)
The password prompt displays.
5. No password is required so press <Enter>.
Password: (leave blank)
The following message displays followed by the NN-ISR hostname prompt.
"Access granted since there are no configured users."
NN-ISR>
6. Enter ifconfig and press <Enter> to list the current configuration on the ISR.
NN-ISR> ifconfig
eth0 Link encap:Ethernet HWaddr 3C:4A:92:F5:9B:C4
inet addr:172.30.58.141 Bcast:172.30.255.255 Mask:255.255.0.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:184074 errors:0 dropped:0 overruns:0 frame:0
TX packets:34402 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:20765532 (19.8 Mb) TX bytes:3099950 (2.9 Mb)
Interrupt:30 Memory:f4000000-f4012800
7. Make a note of the MAC Address (HWaddr) for the license request.
8. Contact your Oracle sales representative and provide the following SBC information to request an RMC license key:
   • System name
   • Number of ports
   • Production or development license
   • License expiration (Development licenses only)
   • Product name (converter with G.729 for standard ISR RSS hosts)
   • MAC address (from Step 4 and 5)

**Installing the RMC License Key**

After receiving the RMC license key, you must transfer it to the RSS host's filesystem.

**To install the RMC license:**

1. Open an FTP client.
2. In the "Host" field, enter the RSS management IP address. For example, Host: 172.30.58.16
3. In the "Port" field, enter 22. For example, Port: 22
4. In the “Username” and “Password” fields, enter root and sips, respectively. For example,

**Username:** root  
**Password:** sips  

The license file is stored in the /cxc directory of the RSS. When you connect via FTP (or SSH) you are in the /cxc directory.

5. Copy the license file from your local machine to the RSS using the FTP application.

6. Using an SSH Client, login to the ISR by entering “root” at the “Login as” prompt, and press <Enter>.

**Login as:** root  
The password prompt displays.

7. At the “Password” prompt, enter “sips” and press <Enter>.

root@<hostname>’s password> sips  
The following prompt and message display.

Net-Net OS-E  
Copyright (c) 2004-2012 Acme Packet Inc.

8. No username is required so press <Enter>.

**Username:** (leave blank)  
The password prompt displays.

9. No password is required so press <Enter>.

**Password:** (leave blank)  
The following message displays followed by the NN-ISR hostname prompt.

“Access granted since there are no configured users.”

NN-ISR>

10. At the “<Hostname>” prompt, enter “restart process isr” and press <Enter>.

<NN-ISR> # restart process isr  

**Note:** The “restart process isr” restarts the ISR and allows the RSS to read the new license information immediately.

---

**Testing the RMC Converter**

When the RMC license is enabled on the ISR, you can test that it is working properly by playing a G.729 recording through the ISR Dashboard.

**To test the RMC converter:**

1. Open your Internet Web browser.

2. Enter the IP address of the ISR. For example:

   http://172.54.66.7  

   The Login page displays.
3. Enter your email and password, respectively, in the “Email” and “Password” fields. The default user name and password are:
   - **User name**: isradmin@acmepacket.com
   - **Password**: admin123
   The following page displays.

4. From the Main Menu, click **Recordings**. The following page displays.
5. Select a recording that has a file name in the format “.rpdd” and then click the `play` button.

The following message displays:

If the RMC conversion process was successful (message is converted from a “.rpdd” file to a “.wav” file), the recording opens and an audible playback of the recording is heard.

If the RMC conversion process was unsuccessful, the following message displays:

Converter logs can be found on the RSS host `/cxc_common/ISR/converter` for troubleshooting.
Assigning RMC Conversion to Specific Locations

The ISR recordings are stored at locations you specified during the installation process of the CIS and RSS. If you enable the RMC license on your ISR, each location containing files that could require conversion must have an RMC set to handle conversion of the files for playback.

By default, a converter is configured on every location that is created. Some locations, like SANs, do not have a converter installed and should be configured to use an existing converter.

**To specify RMC conversion to a specific location:**

1. Open your Internet Web browser.
2. Enter the IP address of the ISR. For example:
   
   ```
   http://172.54.66.7
   ```
   
   The Login page displays.
3. Enter your email and password, respectively, in the “Email” and “Password” fields.
   The default user name and password are:
   
   **User name:** isradmin@acmepacket.com
   **Password:** admin123
   
   The following page displays.
4. From the Main Menu, click **Admin**. The following page displays.

5. Click **Manage Sites**. The following page displays.
6. Click the associated with a site that you want to edit. The following pages displays.

7. Click on the “Locations” tab. The following page displays.
8. Click the to edit the configuration of that location. The following dialog box displays.

9. In the “Recording Converter” section, in the “Converter IP Address” field, specify the RMC IP address.

10. If the RMC is listening to XML-RPC requests on a port other than the default (Port 8890), specify the correct converter port number in the “Converter Port” field.

11. Click Update to update the location with the RMC information.
Remote Archival Webservice WSDL

The Remote Archival Webservice WSDL may also be found on a deployed Webservice host by pointing a browser to the following URL:


Note: The Remote Archival Webservice WSDL file is password protected. Remote Archival users must provide valid usernames and passwords when accessing this file.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<definitions

targetNamespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
xmns="http://schemas.xmlsoap.org/wsdl/">
  xmlns:tns1="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
  xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/
  xmlns:impl="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
  xmlns:apachesoap="http://xml.apache.org/xml-soap"
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:intf="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
  xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
>
  <types>
    <schema
      targetNamespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
xmns="http://www.w3.org/2001/XMLSchema"
      xmlns="http://www.w3.org/2001/XMLSchema"
>
```

Release 5.1  Oracle Communications Interactive Session Recorder Administrator Guide 191
<complexType name="account">
  <xs:sequence>
    <xs:element name="action" type="xs:int"/>
    <xs:element name="accountId" type="xs:int"/>
    <xs:element name="accountName" type="xs:string"/>
    <xs:element name="accountDescription" type="xs:string"/>
    <xs:element name="accountMisc" type="xs:string"/>
    <xs:element name="percentToRecord" type="xs:int"/>
    <xs:element name="recordingEnabled" type="xs:int"/>
    <xs:element name="callMetaDataSrc" type="xs:int"/>
    <xs:element name="announceEnabled" type="xs:boolean" nillable="true"/>
    <xs:element name="defaultAnnounceAudioFile" type="xs:string" nillable="true"/>
    <xs:element name="defaultAnnounceAudioText" type="xs:string" nillable="true"/>
    <xs:element name="defaultOptOutVxmlFile" type="xs:string" nillable="true"/>
    <xs:element name="optOutEnabled" type="xs:boolean"/>
    <xs:element name="recorderState" type="xs:int"/>
    <xs:element name="defaultRecordingType" type="xs:int"/>
    <xs:element name="customDataLabelsSource" type="xs:int"/>
    <xs:element name="agentIdEditableFlag" type="xs:boolean"/>
    <xs:element name="ratingEditableFlag" type="xs:boolean"/>
    <xs:element name="completedEditableFlag" type="xs:boolean"/>
    <xs:element name="notesEditableFlag" type="xs:boolean"/>
    <xs:element name="customData1Name" nillable="true" type="xs:string"/>
    <xs:element name="customData1FriendlyName" type="xs:string"/>
    <xs:element name="customData1EditableFlag" type="xs:boolean"/>
    <xs:element name="customData2Name" nillable="true" type="xs:string"/>
    <xs:element name="customData2FriendlyName" type="xs:string"/>
    <xs:element name="customData2EditableFlag" type="xs:boolean"/>
    <xs:element name="customData3Name" nillable="true" type="xs:string"/>
    <xs:element name="customData3FriendlyName" type="xs:string"/>
    <xs:element name="customData3EditableFlag" type="xs:boolean"/>
    <xs:element name="customData4Name" nillable="true" type="xs:string"/>
    <xs:element name="customData4FriendlyName" type="xs:string"/>
    <xs:element name="customData4EditableFlag" type="xs:boolean"/>
    <xs:element name="application" type="xs:string" nillable="true"/>
    <xs:element name="playBeepBeforeRecord" type="xs:boolean"/>
  </xs:sequence>
</complexType>
<xs:element name="terminateOnDtmf" type="xs:boolean"/>
<xs:element name="terminateOnEos" type="xs:int"/>
<xs:element name="recurringBeepEnabled" type="xs:boolean"/>
<xs:element name="recurringBeepInterval" type="xs:int"/>
<xs:element name="recurringBeepFile" nillable="true" type="xs:string"/>
<xs:element name="recordSaveDtmf" type="xs:string"/>
<xs:element name="maximumNumberOfPorts" type="xs:int"/>
<xs:element name="numberOfBurstPorts" type="xs:int"/>
<xs:element name="acctPortLimit" type="xs:int"/>
<xs:element name="showApplianceTabInRouteView" type="xs:boolean"/>
<xs:element name="storeDtmfSetting" type="xs:int"/>
</xs:sequence>
</complexType>
<complexType name="route">
<xs:sequence>
<xs:element name="action" type="xs:int"/>
<xs:element name="routeId" type="xs:int"/>
<xs:element minOccurs="0" name="routeType" type="xs:int"/>
<xs:element minOccurs="0" name="routePattern" type="xs:string"/>
<xs:element minOccurs="0" name="label" type="xs:string"/>
<xs:element minOccurs="0" name="accountId" type="xs:int"/>
<xs:element minOccurs="0" name="percentToRecord" type="xs:int"/>
<xs:element minOccurs="0" name="recordingEnabled" type="xs:int"/>
<xs:element minOccurs="0" name="defaultRecordingType" type="xs:int"/>
<xs:element minOccurs="0" name="virtualRoutePattern" type="xs:string" nillable="true"/>
<xs:element minOccurs="0" name="announceAudioFile" nillable="true" type="xs:string"/>
<xs:element minOccurs="0" name="announceAudioText" nillable="true" type="xs:string"/>
<xs:element minOccurs="0" name="optOutVxmlFile" nillable="true" type="xs:string"/>
<xs:element minOccurs="0" name="optOutEnabled" type="xs:boolean"/>
<xs:element minOccurs="0" name="announceEnabled" type="xs:boolean"/>
<xs:element minOccurs="0" name="customData1Name" nillable="true" type="xs:string"/>
<xs:element minOccurs="0" name="customData1FriendlyName" type="xs:string"/>
<xs:element minOccurs="0" name="customData1EditableFlag" type="xs:boolean" nillable="true"/>
<xs:element minOccurs="0" name="customData2Name" nillable="true" type="xs:string"/>
<xs:element minOccurs="0" name="customData2FriendlyName" type="xs:string"/>
<xs:element minOccurs="0" name="customData2EditableFlag" type="xs:boolean" nillable="true"/>
</xs:sequence>
</complexType>
<xs:element minOccurs="0" name="customData2FriendlyName" type="xs:string"/>
<xs:element minOccurs="0" name="customData2EditableFlag" type="xs:boolean"/>
<xs:element minOccurs="0" name="customData3Name" nillable="true" type="xs:string"/>
<xs:element minOccurs="0" name="customData3FriendlyName" type="xs:string"/>
<xs:element minOccurs="0" name="customData3EditableFlag" type="xs:boolean"/>
<xs:element minOccurs="0" name="customData4Name" nillable="true" type="xs:string"/>
<xs:element minOccurs="0" name="customData4FriendlyName" type="xs:string"/>
<xs:element minOccurs="0" name="customData4EditableFlag" type="xs:boolean"/>
<xs:element minOccurs="0" name="application" type="xs:string"/>
<xs:element minOccurs="0" name="playBeepBeforeRecord" type="xs:boolean"/>
<xs:element minOccurs="0" name="terminateOnDtmf" type="xs:boolean"/>
<xs:element minOccurs="0" name="terminateOnEos" type="xs:int"/>
<xs:element minOccurs="0" name="priority" type="xs:float"/>
<xs:element minOccurs="0" name="maximumNumberOfPorts" type="xs:int"/>
<xs:element minOccurs="0" name="minimumStorageDays" type="xs:int"/>
<xs:element minOccurs="0" name="numberOfBurstPorts" type="xs:int"/>
<xs:element minOccurs="0" name="storageGracePeriod" type="xs:int"/>
<xs:element minOccurs="0" name="recurringBeepEnabled" type="xs:boolean"/>
<xs:element minOccurs="0" name="recurringBeepInterval" type="xs:int" nillable="true" type="xs:string"/>
<xs:element minOccurs="0" name="recurringBeepFile" type="xs:string"/>
<xs:element minOccurs="0" name="recordSaveDtmf" type="xs:string"/>
<xs:element minOccurs="0" name="callMetaDataSrc" type="xs:int"/>
<xs:element minOccurs="0" name="agentIdEditableFlag" type="xs:boolean"/>
<xs:element minOccurs="0" name="ratingEditableFlag" type="xs:boolean"/>
<xs:element minOccurs="0" name="completedEditableFlag" type="xs:boolean"/>
<xs:element minOccurs="0" name="notesEditableFlag" type="xs:boolean"/>
<xs:element minOccurs="0" name="storeDtmfSetting" type="xs:int"/>
</xs:sequence>
</complexType>
<complexType name="memberRoute">
<xs:sequence>
<xs:element name="action" type="xs:int"/>
<xs:element name="routeGroupMemberId" type="xs:int"/>
</xs:sequence>
</complexType>
<xs:element minOccurs="0" name="routeGroupMasterId" type="xs:int"/>
<xs:element minOccurs="0" name="routePattern" type="xs:string"/>
<xs:element minOccurs="0" name="virtualRoutePattern" type="xs:string"/>
</xs:sequence>
</complexType>
<complexType name="metadataType">
<xs:sequence>
<xs:element name="action" type="xs:int"/>
<xs:element name="metadataTypeId" type="xs:int"/>
<xs:element minOccurs="0" name="name" type="xs:string"/>
<xs:element minOccurs="0" name="sessionCorrelationNumber" nillable="true" type="xs:int"/>
<xs:element minOccurs="0" name="nodeType" nillable="true" type="xs:string"/>
<xs:element minOccurs="0" name="srcTypeId" type="xs:int"/>
<xs:element minOccurs="0" name="searchable" nillable="true" type="xs:boolean"/>
<xs:element minOccurs="0" name="isDisplayed" nillable="true" type="xs:boolean"/>
</xs:sequence>
</complexType>
<complexType name="getNewAdministrativeDataReqObject">
<xs:sequence>
<xs:element minOccurs="0" name="lastRunTime" nillable="true" type="xs:dateTime"/>
</xs:sequence>
</complexType>
<complexType name="getNewAdministrativeDataRespObject">
<xs:sequence>
<xs:element name="returnCode" type="xs:int"/>
<xs:element name="returnString" nillable="true" type="xs:string"/>
<xs:element minOccurs="0" name="currentRunTime" type="xs:dateTime"/>
<xs:element maxOccurs="unbounded" minOccurs="0" name="accounts" type="tns1:account"/>
<xs:element maxOccurs="unbounded" minOccurs="0" name="routes" type="tns1:route"/>
<xs:element maxOccurs="unbounded" minOccurs="0" name="memberRoutes" type="tns1:memberRoute"/>
<xs:element maxOccurs="unbounded" minOccurs="0" name="metadataTypes" type="tns1:metadataType"/>
</xs:sequence>
</complexType>
<complexType name="sessionStats">
<xs:sequence>
<xs:element name="routeId" type="xs:int"/>
<xs:element name="sessionDate" type="xs:dateTime"/>
<xs:element name="totalNumberOfSessions" type="xs:int"/>
</xs:sequence>
</complexType>
<complexType name="sessionStats">
  <xs:sequence>
    <xs:element name="peakNumberOfSessions" type="xs:int"/>
    <xs:element name="numberOfSessionsRejected" type="xs:int"/>
    <xs:element name="numberOfBurstSessions" type="xs:int"/>
    <xs:element name="recordingLengthMs" type="xs:long"/>
    <xs:element name="numberOfSessionsRecorded" type="xs:int"/>
    <xs:element name="systemCapacity Reached" type="xs:int"/>
    <xs:element name="routeCapacity Reached" type="xs:int"/>
    <xs:element name="accountCapacity Reached" type="xs:int"/>
  </xs:sequence>
</complexType>

<complexType name="getSessionStatsReqObject">
  <xs:sequence>
    <xs:element name="date" nillable="true" type="xs:dateTime"/>
  </xs:sequence>
</complexType>

<complexType name="getSessionStatsRespObject">
  <xs:sequence>
    <xs:element name="returnCode" type="xs:int"/>
    <xs:element name="returnString" nillable="true" type="xs:string" maxOccurs="unbounded" minOccurs="0"/>
    <xs:element name="sessionStatsArray" nillable="true" type="tns1:sessionStats" maxOccurs="unbounded" minOccurs="0"/>
  </xs:sequence>
</complexType>

<complexType name="reqObject">
  <xs:sequence>
    <xs:element name="recordingId" type="xs:long"/>
    <xs:element name="fileName" nillable="true" type="xs:string"/>
  </xs:sequence>
</complexType>

<complexType name="respObject">
  <xs:sequence>
    <xs:element minOccurs="0" name="cdrId" type="xs:long"/>
    <xs:element name="recordingId" type="xs:long"/>
    <xs:element name="fileName" type="xs:string"/>
    <xs:element minOccurs="0" name="fileStatus" type="xs:int" nillable="true"/>
    <xs:element minOccurs="0" name="ani" nillable="true" type="xs:string"/>
    <xs:element minOccurs="0" name="dnis" nillable="true" type="xs:string"/>
    <xs:element minOccurs="0" name="accountId" type="xs:int"/>
    <xs:element minOccurs="0" name="duration" type="xs:long"/>
    <xs:element minOccurs="0" name="timestamp" type="xs:dateTime"/>
    <xs:element minOccurs="0" name="directory" nillable="true" type="xs:string"/>
  </xs:sequence>
</complexType>
<xs:element minOccurs="0" name="vmgId" type="xs:int"/>
<xs:element minOccurs="0" name="custom1" nillable="true" type="xs:string"/>
<xs:element minOccurs="0" name="custom2" nillable="true" type="xs:string"/>
<xs:element minOccurs="0" name="custom3" nillable="true" type="xs:string"/>
<xs:element minOccurs="0" name="custom4" nillable="true" type="xs:string"/>
<xs:element minOccurs="0" name="archived" type="xs:int"/>
<xs:element minOccurs="0" name="routeId" type="xs:long"/>
<xs:element minOccurs="0" name="archivalRemarks" nillable="true" type="xs:string"/>
<xs:element minOccurs="0" name="archivalFailCount" type="xs:int"/>
<xs:element minOccurs="0" name="agentId" nillable="true" type="xs:string"/>
<xs:element minOccurs="0" name="agentTerminal" nillable="true" type="xs:string"/>
<xs:element minOccurs="0" name="archiverMode" type="xs:string"/>
<xs:element minOccurs="0" name="sensitive" type="xs:int"/>
<xs:element minOccurs="0" name="lastPauseTime" nillable="true" type="xs:dateTime"/>
<xs:element minOccurs="0" name="pauseLength" type="xs:int"/>
<xs:element minOccurs="0" name="deleteFlag" type="xs:boolean"/>
<xs:element minOccurs="0" name="previousFileName" nillable="true" type="xs:string"/>
<xs:element minOccurs="0" name="archiverAction" type="xs:int"/>
<xs:element minOccurs="0" name="conversionStatus" type="xs:int"/>
<xs:element minOccurs="0" name="isrUcid" nillable="true" type="xs:string"/>
<xs:element minOccurs="0" name="ingressCallId" nillable="true" type="xs:string"/>
<xs:element minOccurs="0" name="egressCallId" nillable="true" type="xs:string"/>
<xs:element maxOccurs="unbounded" minOccurs="0" name="siprecDataSets" type="tns1:siprecData"/>
<xs:element maxOccurs="unbounded" minOccurs="0" name="dtmfEntries" type="tns1:dtmfEntry"/>
<xs:element name="returnCode" type="xs:int"/>
<xs:element name="returnString" nillable="true" type="xs:string"/>
<xs:element minOccurs="0" name="downloadable" type="xs:boolean"/>
<xs:element minOccurs="0" name="fileNotFound" type="xs:boolean"/>
<xs:element minOccurs="0" name="splitFile" nillable="true" type="xs:boolean"/>
<complexType name="metadataCorrelationSet">
  <xs:sequence>
    <xs:element name="mcsId" type="xs:long"/>
    <xs:element name="metadataTypeId1" type="xs:int"/>
    <xs:element name="metadataValue1" type="xs:string"/>
    <xs:element name="metadataTypeId2" type="xs:int"/>
    <xs:element name="metadataValue2" type="xs:string"/>
  </xs:sequence>
</complexType>

<complexType name="extensionData">
  <xs:sequence>
    <xs:element name="extensionDataId" type="xs:long"/>
    <xs:element name="nodeId" type="xs:long"/>
    <xs:element name="metadataTypeId" type="xs:int"/>
    <xs:element minOccurs="0" name="value" nillable="true" type="xs:string"/>
    <xs:element minOccurs="0" name="indexedValue" nillable="true" type="xs:string"/>
    <xs:element minOccurs="0" name="mcs" nillable="true" type="impl:metadataCorrelationSet"/>
  </xs:sequence>
</complexType>

<complexType name="siprecParticipant">
  <xs:sequence>
    <xs:element name="participantId" type="xsd:long"/>
    <xs:element name="siprecParticipantId" nillable="true" type="xsd:string"/>
    <xs:element name="participantAor" nillable="true" type="xsd:string"/>
    <xs:element name="participantName" nillable="true" type="xsd:string"/>
    <xs:element name="participantStart" nillable="true" type="xsd:dateTime"/>
    <xs:element name="participantEnd" nillable="true" type="xsd:dateTime"/>
    <xs:element maxOccurs="unbounded" minOccurs="0" name="participantExtensionData" type="impl:extensionData"/>
  </xs:sequence>
</complexType>

<complexType name="siprecSession">
  <xs:sequence>
    <xs:element name="sessionId" type="xsd:long"/>
    <xs:element name="siprecSessionId" nillable="true" type="xsd:string"/>
    <xs:element name="sessionStart" nillable="true" type="xsd:dateTime"/>
    <xs:element name="sessionEnd" nillable="true" type="xsd:dateTime"/>
    <xs:element maxOccurs="unbounded" minOccurs="0" name="sessionExtensionData" type="impl:extensionData"/>
  </xs:sequence>
</complexType>
<complexType name="siprecStream">
  <xs:sequence>
    <xs:element name="streamId" type="xsd:long"/>
    <xs:element name="siprecStreamId" nillable="true" type="xsd:string"/>
    <xs:element name="streamLabel" nillable="true" type="xsd:string"/>
    <xs:element name="streamMode" nillable="true" type="xsd:string"/>
    <xs:element name="participantId" nillable="true" type="xsd:long"/>
    <xs:element name="streamStart" nillable="true" type="xsd:dateTime"/>
    <xs:element name="streamEnd" nillable="true" type="xsd:dateTime"/>
    <xs:element maxOccurs="unbounded" minOccurs="0" name="streamExtensionData" type="impl:extensionData"/>
  </xs:sequence>
</complexType>

<complexType name="siprecData">
  <xs:sequence>
    <xs:element maxOccurs="unbounded" minOccurs="0" name="siprecParticipants" nillable="true" type="impl:siprecParticipant"/>
    <xs:element name="siprecSession" nillable="true" type="impl:siprecSession"/>
    <xs:element maxOccurs="unbounded" minOccurs="0" name="siprecStreams" nillable="true" type="impl:siprecStream"/>
  </xs:sequence>
</complexType>

<complexType name="dtmfEntry">
  <xs:sequence>
    <xs:element minOccurs="0" name="msOffset" type="xs:long"/>
    <xs:element minOccurs="0" name="originSource" type="xs:int"/>
    <xs:element minOccurs="0" name="dtmfDigit" type="xs:int"/>
  </xs:sequence>
</complexType>

<complexType name="reqObject_Array">
  <xs:sequence>
    <xs:element maxOccurs="unbounded" minOccurs="0" name="gfRequest" nillable="true" type="tns1:reqObject"/>
  </xs:sequence>
</complexType>

<complexType name="respObject_Array">
  <xs:sequence>
    <xs:element maxOccurs="unbounded" minOccurs="0" name="gfResponse" nillable="true" type="tns1:respObject"/>
  </xs:sequence>
</complexType>

<complexType name="getListReqObj">
  <xs:sequence/>
</complexType>
<xsd:element name="statusUpdate">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element form="unqualified" name="parameters" type="ns2:statusUpdateReqObj"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>

<xsd:element name="getNewAdministrativeData">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element form="unqualified" name="parameters" type="ns3:getNewAdministrativeDataReqObject"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>

<xsd:element name="getFile">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element form="unqualified" name="parameters" type="ns4:reqObject_Array"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>

<xsd:element name="getSessionStatsResponse">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element form="unqualified" name="parameters" type="ns5:getSessionStatsRespObject"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>

<xsd:element name="getListResponse">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element form="unqualified" name="parameters" type="ns6:getListRespObj"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>

<xsd:element name="statusUpdateResponse">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element form="unqualified" name="parameters" type="ns7:statusUpdateRespObj"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>

<xsd:element name="getNewAdministrativeDataResponse">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element form="unqualified" name="parameters" type="ns3:getNewAdministrativeDataRespObject"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
<xsd:element form="unqualified" name="parameters" type="ns8:getNewAdministrativeDataRespObject"/>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:complexType>
</xsd:element>
</xsd:complexType>
</xsd:element>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:element>
</xsd:complexType>
</xsd:element>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
<operation name="getSessionStats">
  <wsdlsoap:operation soapAction=""/>
  <input name="getSessionStatsRequest">
    <wsdlsoap:body use="literal"
      namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
      encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
  </input>
  <output name="getSessionStatsResponse">
    <wsdlsoap:body use="literal"
      namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
      encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
  </output>
</operation>

<operation name="getFile">
  <wsdlsoap:operation soapAction=""/>
  <input name="getFileRequest">
    <wsdlsoap:body use="literal"
      namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
      encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
  </input>
  <output name="getFileResponse">
    <wsdlsoap:body use="literal"
      namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
      encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
  </output>
</operation>

<operation name="getList">
  <wsdlsoap:operation soapAction=""/>
  <input name="getListRequest">
    <wsdlsoap:body use="literal"
      namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
      encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
  </input>
  <output name="getListResponse">
    <wsdlsoap:body use="literal"
      namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
      encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
  </output>
</operation>

<operation name="statusUpdate">
  <wsdlsoap:operation soapAction=""/>
  <input name="statusUpdateRequest">
    <wsdlsoap:body use="literal"
      namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
      encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
  </input>
  <output name="statusUpdateResponse">
    <wsdlsoap:body use="literal"
      namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
      encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
  </output>
</operation>
<wsdl:body use="literal"
namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <input>
    <wsdl:body use="literal"
namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
      <output name="getFileResponse">
        <wsdl:body use="literal"
namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
      </output>
    </input>
    <operation name="getList">
      <wsdl:operation soapAction=""/>
      <input name="getListRequest">
        <wsdl:body use="literal"
namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
      </input>
      <output name="getListResponse">
        <wsdl:body use="literal"
namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
      </output>
    </operation>
    <operation name="statusUpdate">
      <wsdl:operation soapAction=""/>
      <input name="statusUpdateRequest">
        <wsdl:body use="literal"
namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
      </input>
      <output name="statusUpdateResponse">
        <wsdl:body use="literal"
namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
      </output>
    </operation>
  </input>
</wsdl:body>
</definitions>

<wsdl:binding name="RemoteArchiverWS">
  <wsdl:service name="RemoteArchiverWS">
    <wsdl:port name="RemoteArchiverWSService" binding="tns1:RemoteArchiverWSSoapBinding">
    </wsdl:port>
  </wsdl:service>
</wsdl:binding>
Introduction

This appendix provides the Database Schema Definitions and Descriptions for the ISR Administrator Dashboard. It lists, in table format, the parameters contained in the Administrator Dashboard and provides the schema and descriptions of each parameter.

The following tables are included in the ISR Administrator Database Schema Descriptions:

- accounts
- archivers
- audit
- call_stats
- categories
- cdr_receive
- cdr_transmit
- dash_config
- db_slaves
- failover_db_status
- heartbeats
- locations
- log
- outbound_gateway_events
- outbound_gateways
- peak_stats
- playback_problems
- rec_notes_and_scoring
- recording_categories
- recordings
- remote_archivers
- route_groups
- route_map_tracking_events
- saved_searches
- security_settings
- sites
- tokens
- user_accounts
- user_display_preferences
- user_routes
- user_type
- users
- vmg_channel_lookup
- vmgs
## ISR Administrator Database Schema Descriptions

**Table Name: Accounts**  
**Purpose:** Configuration and setup of accounts (tenants)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>account_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td>auto_increment</td>
<td>PRIMARY KEY</td>
<td>Primary key</td>
</tr>
<tr>
<td>account_name</td>
<td>varchar(40)</td>
<td>NOT NULL</td>
<td>Text</td>
<td></td>
<td>Name of the account</td>
</tr>
<tr>
<td>account_description</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td>Text</td>
<td></td>
<td>Description of the account</td>
</tr>
<tr>
<td>account_name</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td>Text</td>
<td></td>
<td>Description of the account</td>
</tr>
<tr>
<td>percent_decay</td>
<td>smallint(4)</td>
<td>NOT NULL</td>
<td>5-100</td>
<td>25</td>
<td>Default recording percentage for routes created under this account</td>
</tr>
<tr>
<td>recording_enabled</td>
<td>tinyint(1)</td>
<td>NOT NULL</td>
<td>Overrecording disabled</td>
<td>1</td>
<td>Whether recording is enabled by default for routes created under this account</td>
</tr>
<tr>
<td>cell_meta_data_src</td>
<td>tinyint(1)</td>
<td>NOT NULL</td>
<td>0 = RFC 1, 1 = TAPI</td>
<td>0</td>
<td>For future use</td>
</tr>
<tr>
<td>announce_enabled</td>
<td>tinyint(1)</td>
<td>NOT NULL</td>
<td>0 = announce disabled, 1 = announce enabled</td>
<td>0</td>
<td>Whether announcements are enabled by default for routes created under this account</td>
</tr>
<tr>
<td>default addslashes</td>
<td>varchar(100)</td>
<td>NOT NULL</td>
<td>Text</td>
<td></td>
<td>Default announcement audio file for routes created under this account</td>
</tr>
<tr>
<td>default_last_audio</td>
<td>varchar(200)</td>
<td>NOT NULL</td>
<td>Text</td>
<td></td>
<td>Default last audio file for routes created under this account</td>
</tr>
<tr>
<td>opt_out_enabled</td>
<td>tinyint(1)</td>
<td>NOT NULL</td>
<td>0 = disabled, 1 = enabled</td>
<td>0</td>
<td>Whether opt out is enabled by default for routes created under this account</td>
</tr>
<tr>
<td>recorder_type</td>
<td>tinyint(1)</td>
<td>NOT NULL</td>
<td>0 = disabled, 1 = enabled</td>
<td>0</td>
<td>Whether calls can currently be recorded for calls on routes under this account</td>
</tr>
<tr>
<td>custom_data_labels</td>
<td>tinyint(2)</td>
<td>NOT NULL</td>
<td>DiRoute</td>
<td>0</td>
<td>If the custom field labels defined at route will be shown, if 1, labels defined at account will be</td>
</tr>
<tr>
<td>agent_ideditable_flag</td>
<td>tinyint(1)</td>
<td>NOT NULL</td>
<td>0 = not editable, 1 = editable</td>
<td>0</td>
<td>Can users edit the data in the recordings’ agent_id field</td>
</tr>
<tr>
<td>ratingeditable_flag</td>
<td>tinyint(1)</td>
<td>NOT NULL</td>
<td>0 = not editable, 1 = editable</td>
<td>0</td>
<td>Can users edit the data in the scoring rating? (rsc_notes_and_scoring.user_rating)</td>
</tr>
<tr>
<td>completededitable_flag</td>
<td>tinyint(1)</td>
<td>NOT NULL</td>
<td>0 = not editable, 1 = editable</td>
<td>0</td>
<td>Can users edit the data in the complete transaction flag? (rsc_notes_and_scoring.complete_status)</td>
</tr>
<tr>
<td>noteseditable_flag</td>
<td>tinyint(1)</td>
<td>NOT NULL</td>
<td>0 = not editable, 1 = editable</td>
<td>0</td>
<td>Can users edit the scoring notes? (rsc_notes_and_scoring.notes)</td>
</tr>
<tr>
<td>custom_data_1_name</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td>Text</td>
<td>NULL</td>
<td>Name of Custom Data 1 Field (must match API calls)</td>
</tr>
<tr>
<td>custom_data_1_friendly name</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td>Text</td>
<td></td>
<td>Displayed name of Custom Data 1 Field</td>
</tr>
<tr>
<td>custom_data_2_name</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td>Text</td>
<td>NULL</td>
<td>Name of Custom Data 2 Field (must match API calls)</td>
</tr>
<tr>
<td>custom_data_2_friendly name</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td>Text</td>
<td></td>
<td>Displayed name of Custom Data 2 Field</td>
</tr>
<tr>
<td>custom_data_2editable_flag</td>
<td>tinyint(1)</td>
<td>NOT NULL</td>
<td>0 = not editable, 1 = editable</td>
<td>0</td>
<td>Can users edit Custom Data 2 Field?</td>
</tr>
<tr>
<td>custom_data_3_name</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td>Text</td>
<td>NULL</td>
<td>Name of Custom Data 3 Field (must match API calls)</td>
</tr>
<tr>
<td>custom_data_3_friendly name</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td>Text</td>
<td></td>
<td>Displayed name of Custom Data 3 Field</td>
</tr>
<tr>
<td>custom_data_3editable_flag</td>
<td>tinyint(1)</td>
<td>NOT NULL</td>
<td>0 = not editable, 1 = editable</td>
<td>0</td>
<td>Can users edit Custom Data 3 Field?</td>
</tr>
<tr>
<td>custom_data_4_name</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td>Text</td>
<td>NULL</td>
<td>Name of Custom Data 4 Field (must match API calls)</td>
</tr>
<tr>
<td>custom_data_4_friendly name</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td>Text</td>
<td></td>
<td>Displayed name of Custom Data 4 Field</td>
</tr>
<tr>
<td>custom_data_4editable_flag</td>
<td>tinyint(1)</td>
<td>NOT NULL</td>
<td>0 = not editable, 1 = editable</td>
<td>0</td>
<td>Can users edit Custom Data 4 Field?</td>
</tr>
<tr>
<td>application</td>
<td>type</td>
<td>nullability</td>
<td>default</td>
<td>description</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------</td>
<td>-------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>play_beep_before_record</td>
<td>tinyint(3)</td>
<td>NOT NULL</td>
<td>0</td>
<td>Should this beep tone be played by default on a conference route under this account?</td>
<td></td>
</tr>
<tr>
<td>terminate_on_dtmf</td>
<td>tinyint(3)</td>
<td>NOT NULL</td>
<td>0</td>
<td>Should a conference mode recording terminate on DTMF entry</td>
<td></td>
</tr>
<tr>
<td>terminate_on_eos</td>
<td>tinyint(4)</td>
<td>NOT NULL</td>
<td>-1</td>
<td>Should a conference mode recording terminate on End of Speech</td>
<td></td>
</tr>
<tr>
<td>recurring_beep_enabled</td>
<td>tinyint(5)</td>
<td>NOT NULL</td>
<td>0</td>
<td>Enable/Disable recurring beep played during recording</td>
<td></td>
</tr>
<tr>
<td>recurring_beep_interval</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td>50</td>
<td>If enabled, how often should the beep be played</td>
<td></td>
</tr>
<tr>
<td>recurring_beep_file</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td>beep.wav</td>
<td>Name of file, stored in .css file, that should be played</td>
<td></td>
</tr>
<tr>
<td>record_save_dtmf</td>
<td>varchar(4)</td>
<td>NOT NULL</td>
<td>#</td>
<td>Single DTMF digit that will save a recording made on a Record &amp; Save route.</td>
<td></td>
</tr>
<tr>
<td>maximum_number_of_ports</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td>24</td>
<td>Default maximum number of simultaneous sessions a route created on this account will be able to support.</td>
<td></td>
</tr>
<tr>
<td>number_of_burst_ports</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td>0</td>
<td>Default number of ports over maximum that the route will be able to use. These ports are reported separately.</td>
<td></td>
</tr>
<tr>
<td>acct_port1_limit</td>
<td>int(11)</td>
<td>NOT NULL</td>
<td>-2</td>
<td>-1 for unlimited. The maximum number of sessions all routes on this account will be able to use.</td>
<td></td>
</tr>
<tr>
<td>show_appliance_tab_in_route_view</td>
<td>tinyint(5)</td>
<td>NOT NULL</td>
<td>0</td>
<td>Whether account's routes should be allowed to see and use the Appliance Tab</td>
<td></td>
</tr>
</tbody>
</table>

* deprecated
### Table Name: archivers
Purpose: Definition and configuration of archivers

<table>
<thead>
<tr>
<th>Field name</th>
<th>Field type</th>
<th>Null?</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>archiver_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>auto_increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>archiver_ip</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td>ip addresses</td>
<td>&quot;&quot;</td>
<td>Archiver’s IP Address</td>
</tr>
<tr>
<td>site_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>State the site this archiver is associated with</td>
</tr>
<tr>
<td>source_directory</td>
<td>varchar(200)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Directory where archiver should move files from — replaced with locations table, left for backwards compatibility</td>
</tr>
<tr>
<td>destination_directory</td>
<td>varchar(200)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Directory where archiver should move files to — replaced with locations table, left for backwards compatibility</td>
</tr>
<tr>
<td>archiver_thread_number</td>
<td>smallint(4) unsigned</td>
<td>NOT NULL</td>
<td></td>
<td>1</td>
<td>Number of threads the archiver should attempt to move a file before permanently marking it full (f)</td>
</tr>
<tr>
<td>max_file_count</td>
<td>smallint(6)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Amount of free space remaining on the source_directory</td>
</tr>
<tr>
<td>source_free_space_kb</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Amount of free space remaining on the destination directory</td>
</tr>
<tr>
<td>dest_free_space_kb</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Amount of free space remaining on the destination directory</td>
</tr>
<tr>
<td>Older_than_enabled</td>
<td>smallint(2)</td>
<td>NOT NULL</td>
<td>0 = disabled, 1 = enabled</td>
<td>0</td>
<td>Should the archiver delete files from the destination_directory after route_config.minimum_storage_days</td>
</tr>
<tr>
<td>archiver_state</td>
<td>smallint(2)</td>
<td>NOT NULL</td>
<td>0 = paused, 1 = active</td>
<td>1</td>
<td>Is the archiver active?</td>
</tr>
<tr>
<td>archiver_mode</td>
<td>varchar(10)</td>
<td>NOT NULL</td>
<td></td>
<td>NULL</td>
<td>Primary: Failed: followed</td>
</tr>
<tr>
<td>source_location</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td>-1</td>
<td>locations.location_id of the source location for this archiver</td>
</tr>
<tr>
<td>dest_location</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td>-1</td>
<td>locations.location_id of the destination location for this archiver</td>
</tr>
<tr>
<td>dir_date_structure</td>
<td>tinyint(1)</td>
<td>NOT NULL</td>
<td>0 = do not archive with date structure, 1 = archive with date structure</td>
<td>2</td>
<td>Should recordings be archived by date</td>
</tr>
<tr>
<td>move_non_existent_record</td>
<td>tinyint(1)</td>
<td>NOT NULL</td>
<td>0 = do not move non-existing files, 1 = move non-existing files</td>
<td>0</td>
<td>If recording is not found, should record be removed from recordings db and added to recordings_missing table for tracking.</td>
</tr>
</tbody>
</table>
## ISR Database Schema Definitions and Descriptions

### Table Name: audit

**Purpose:** Log user activity within the Admin Dashboard

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullble</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>audit_id</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td>auto_increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>audit_time</td>
<td>datetime</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Date entry added to table</td>
</tr>
<tr>
<td>user_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>users.user_id performing the action</td>
</tr>
<tr>
<td>user_email</td>
<td>varchar(100)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>users.email performing the action</td>
</tr>
<tr>
<td>session_id</td>
<td>varchar(50)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>User's session ID</td>
</tr>
<tr>
<td>requesting_ip</td>
<td>varchar(15)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>IP address the request originated from</td>
</tr>
<tr>
<td>action_type</td>
<td>varchar(15)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Action the user performed</td>
</tr>
<tr>
<td>object_name</td>
<td>varchar(100)</td>
<td>NOT NULL</td>
<td>VIEW_xxx, modify_xxx, Create_xxx, Delete_xxx, where xxxx=Account, Route, Site, User, Recording</td>
<td>NULL</td>
<td>Object the action was performed on</td>
</tr>
<tr>
<td>prev_value</td>
<td>varchar(128)</td>
<td>NULL</td>
<td></td>
<td></td>
<td>Value of the field before the edit</td>
</tr>
<tr>
<td>new_value</td>
<td>varchar(128)</td>
<td>NULL</td>
<td></td>
<td></td>
<td>Value of the field after the edit</td>
</tr>
<tr>
<td>result_flag</td>
<td>tinyint(4)</td>
<td>NOT NULL</td>
<td>0 = failed, 1 = success</td>
<td></td>
<td>Was the action successful</td>
</tr>
</tbody>
</table>

### Table Name: call_stats

**Purpose:** Track various system statistics to be used for reports

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullble</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>route_config.route_id that is being tracked</td>
</tr>
<tr>
<td>call_date</td>
<td>datetime</td>
<td>NOT NULL</td>
<td></td>
<td>0000-00-00 00:00:00</td>
<td>Date of statistical information</td>
</tr>
<tr>
<td>total_number_of_calls</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Total number of INVITES received by the RSS</td>
</tr>
<tr>
<td>peak_number_of_calls</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Maximum number of simultaneous sessions for the call date</td>
</tr>
<tr>
<td>number_of_calls_rejected</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Total number of sessions RSS did not accept because session exceeds</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>accountsacct_port_limit or route_config.maximum_number_of_ports + route_config.number_of_burst_ports or RSS total licensed session capacity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>number_of_burst_calls</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Number of sessions handled on a burst port, if configured</td>
</tr>
<tr>
<td>recording_length_ms</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Total length of all recordings on route_id for call_data</td>
</tr>
<tr>
<td>number_of_calls_recorded</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Total number of RECORD START commands received by RSS</td>
</tr>
</tbody>
</table>
### Table Name: categories

**Purpose:** Track various system statistics to be used for reports

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>INT(11)</td>
<td>NOT NULL</td>
<td></td>
<td>auto_increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>account_id</td>
<td>INT(11)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>accounts.account_id category pertains to</td>
</tr>
<tr>
<td>name</td>
<td>varchar(255)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>name of category</td>
</tr>
<tr>
<td>active</td>
<td>tinyint(1)</td>
<td>NOT NULL</td>
<td>0 = inactive 1 = active</td>
<td>0</td>
<td>Is category still used?</td>
</tr>
<tr>
<td>created_dt</td>
<td>datetime</td>
<td>NULL</td>
<td></td>
<td>NULL</td>
<td>Date category was created</td>
</tr>
<tr>
<td>updated_dt</td>
<td>datetime</td>
<td>NULL</td>
<td></td>
<td>NULL</td>
<td>Date category last updated</td>
</tr>
</tbody>
</table>

### Table Name: cdrreceive

**Purpose:** Log of CDR records received on Remote Archiver Appliance

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdr_id</td>
<td>bigint(20) unsigned</td>
<td>NOT NULL</td>
<td></td>
<td>auto_increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>ANI</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>ANI</td>
</tr>
<tr>
<td>DNS</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
<tr>
<td>timestamp</td>
<td>datetime</td>
<td>NOT NULL</td>
<td></td>
<td>0000-00-00 00:00:00</td>
<td>Time of call</td>
</tr>
<tr>
<td>duration_ms</td>
<td>bigint(20) unsigned</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Duration of call</td>
</tr>
<tr>
<td>status</td>
<td>varchar(20)</td>
<td>NOT NULL</td>
<td></td>
<td>Complete</td>
<td>Status of receipt</td>
</tr>
<tr>
<td>status_code</td>
<td>integer</td>
<td>NOT NULL</td>
<td>0 = pending 1 = success 2 = fail 3 = unknown 4 = processing</td>
<td>0</td>
<td>Status code for remote archiving</td>
</tr>
<tr>
<td>archived_file_count</td>
<td>smallint(5) unsigned</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Number of failed attempts to archive</td>
</tr>
<tr>
<td>archived_remark</td>
<td>text</td>
<td>NULL</td>
<td></td>
<td></td>
<td>Comments about archival</td>
</tr>
<tr>
<td>file_name</td>
<td>varchar(255)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Recording file name</td>
</tr>
<tr>
<td>recording_id</td>
<td>bigint(20) unsigned</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>recordings.recording_id of the recording file</td>
</tr>
</tbody>
</table>
### Table Name: cdr_transmit

**Purpose:** Log of CDR records sent to Remote Archiver Appliance

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crid</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td>auto_increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>recording_id</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>recordings.recording_id value transmitted</td>
</tr>
<tr>
<td>webservice_id</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>webservice_destinations.webservice_id used</td>
</tr>
<tr>
<td>status</td>
<td>tinyint(2)</td>
<td>NOT NULL</td>
<td>0 = pending, 1 = attempted, 2 = sent, 3 = aborted</td>
<td>0</td>
<td>Status of CDR transmission</td>
</tr>
<tr>
<td>try_count</td>
<td>tinyint(2)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Number of transmission attempts currently made</td>
</tr>
</tbody>
</table>

### Table Name: dash_config

**Purpose:** Global dashboard settings

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config_id</td>
<td>tinyint(3)</td>
<td>NOT NULL</td>
<td></td>
<td>auto_increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>admin_help_url</td>
<td>varchar(255)</td>
<td>NOT NULL</td>
<td></td>
<td>adminhelp.jsp</td>
<td>Page to display when an Admin selects Help link</td>
</tr>
<tr>
<td>user_help_url</td>
<td>varchar(255)</td>
<td>NOT NULL</td>
<td></td>
<td>userhelp.jsp</td>
<td>Page to display when a user selects Help link</td>
</tr>
<tr>
<td>login_help_url</td>
<td>varchar(255)</td>
<td>NOT NULL</td>
<td></td>
<td>loginhelp.jsp</td>
<td>Page to display when a user selects Login help</td>
</tr>
<tr>
<td>max_csv_entries_per_download</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td>10000</td>
<td>Maximum number of records to allow for CSV download</td>
</tr>
<tr>
<td>banner_url</td>
<td>varchar(255)</td>
<td>NOT NULL</td>
<td></td>
<td>logo.png</td>
<td>URL of banner to be displayed in User Dashboard</td>
</tr>
<tr>
<td>base_url</td>
<td>varchar(255)</td>
<td>NOT NULL</td>
<td></td>
<td><a href="http://localhost:9000/3par_dash">http://localhost:9000/3par_dash</a></td>
<td>URL of base user dashboard application</td>
</tr>
<tr>
<td>header_foooo</td>
<td>varchar(255)</td>
<td>NOT NULL</td>
<td></td>
<td>#000D45</td>
<td>Color to be used for header/footer show on user dashboard</td>
</tr>
<tr>
<td>logo_url</td>
<td>varchar(255)</td>
<td>NOT NULL</td>
<td></td>
<td>comapocket_logo.png</td>
<td>URL of logo for User dashboard template</td>
</tr>
</tbody>
</table>
### Table Name: db_slaves
**Purpose:** Configure database slaves to be used for read only access for certain accounts

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td>auto_increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>url</td>
<td>varchar(255)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>URL of database slave to be used</td>
</tr>
<tr>
<td>user</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Database User</td>
</tr>
<tr>
<td>password</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Database password</td>
</tr>
<tr>
<td>account_id</td>
<td>bigint(20)</td>
<td>NULL</td>
<td></td>
<td></td>
<td>accounts.account_id for which this db will be used</td>
</tr>
</tbody>
</table>

### Table Name: failover_db_status
**Purpose:** Track the status of failover databases

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>min_before_retry_primary</td>
<td>smallint(6)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Minutes before db connection will be reattempted</td>
</tr>
<tr>
<td>last_primary_fail_time</td>
<td>timestamp</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Timestamp of last failure to connect to primary db</td>
</tr>
</tbody>
</table>

### Table Name: heartbeats
**Purpose:** Used by VAM SIP Test Route Type to track health of components

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>heartbeat_id</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td>auto_increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>component_type</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td>0 = unspecified</td>
<td></td>
<td>1 = extender</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 = Vsrkey</td>
<td></td>
<td>3 = Dashboard</td>
</tr>
<tr>
<td>component_id</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>The relevant foreign key</td>
</tr>
<tr>
<td>timestamp</td>
<td>datetime</td>
<td>NOT NULL</td>
<td></td>
<td>0000-00-00 00:00:00</td>
<td>Timestamp of last heartbeat</td>
</tr>
<tr>
<td>notes</td>
<td>varchar(100)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### ISR DATABASE SCHEMA DEFINITIONS AND DESCRIPTIONS

**Table Name: locations**

**Purpose:** Locations for recording storage and archival

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>location_id</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td>auto_increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>www_served_from</td>
<td>varchar(250)</td>
<td>NULL</td>
<td></td>
<td></td>
<td>URL where files stored in this location will be served from</td>
</tr>
<tr>
<td>destination_dir</td>
<td>varchar(220)</td>
<td>NULL</td>
<td></td>
<td></td>
<td>Directory files will be moved to</td>
</tr>
<tr>
<td>source_dir</td>
<td>varchar(250)</td>
<td>NULL</td>
<td></td>
<td></td>
<td>Directory files will be moved from</td>
</tr>
<tr>
<td>description</td>
<td>varchar(255)</td>
<td>NULL</td>
<td></td>
<td></td>
<td>Descriptive text about this location</td>
</tr>
<tr>
<td>source_free_space_KB</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Source directory free space</td>
</tr>
<tr>
<td>source_free_space_perc</td>
<td>tinyint(3)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Source directory percentage of free space</td>
</tr>
<tr>
<td>dest_free_space_KB</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Destination directory free space</td>
</tr>
<tr>
<td>dest_free_space_perc</td>
<td>tinyint(3)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Destination directory percentage of free space</td>
</tr>
</tbody>
</table>

**Table Name: log**

**Purpose:** Log entries for RSS / displayed in Dashboard -> Sites

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log_id</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td>auto_increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>time_of_occurrence</td>
<td>datetime</td>
<td>NOT NULL</td>
<td></td>
<td>0000-00-00 00:00:00</td>
<td>Date of log entry</td>
</tr>
<tr>
<td>priority</td>
<td>varchar(15)</td>
<td>NOT NULL</td>
<td></td>
<td>INFO</td>
<td>Log entry priority</td>
</tr>
<tr>
<td>description</td>
<td>text</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>componentType</td>
<td>smallint(2)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>componentId</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>The relevant foreign key</td>
</tr>
</tbody>
</table>
### Table Name: outbound_gateway_events

**Purpose:** Track events on the outbound session agents

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>outbound_gateway_event_id</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td>auto_increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>gateway_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>outbound_gateway.gateway_id the event occurred on</td>
</tr>
<tr>
<td>event_timestamp</td>
<td>timestamp</td>
<td>NOT NULL</td>
<td></td>
<td>CURRENT_TIMESTAMP</td>
<td>time of event</td>
</tr>
<tr>
<td>event_type</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td>0 = unavailable</td>
<td></td>
<td>Status of outbound gateway</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 = software</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 = disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 = inactive</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 = enabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table Name: outbound_gateways

**Purpose:** Configure gateways RSS will connect calls to after applying recording logic

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gateway_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>auto_increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>site_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>sites.site_id gateway is affiliated with</td>
</tr>
<tr>
<td>gateway_name</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Gateway name</td>
</tr>
<tr>
<td>gateway_ip</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>IP Address of gateway. Can also include port.</td>
</tr>
<tr>
<td>gateway_type</td>
<td>tinyint(5)</td>
<td>NOT NULL</td>
<td>0 = P. strick</td>
<td></td>
<td>Status of gateway</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 = temporarily disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 = disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 = temporarily disabled follower</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5 = disabled follower</td>
<td></td>
<td></td>
</tr>
<tr>
<td>last_call_sent</td>
<td>timestamp</td>
<td>NOT NULL</td>
<td></td>
<td>CURRENT_TIMESTAMP</td>
<td>Date/Time last call was delivered to this gateway</td>
</tr>
<tr>
<td>last_call_time</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## ISR Database Schema Definitions and Descriptions

### Table Name: peak_stats

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>route_config.route_id being tracked</td>
</tr>
<tr>
<td>site_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>site.site_id</td>
</tr>
<tr>
<td>count</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>number of sessions</td>
</tr>
</tbody>
</table>

**Purpose:** Track peak number of calls per route/site

### Table Name: playback_problems

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>playback_problems</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td>auto_increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>recording_id</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>recordings.recording_id with playback issue</td>
</tr>
<tr>
<td>reported_date</td>
<td>timestamp</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Date problem reported</td>
</tr>
<tr>
<td>problem_description</td>
<td>varchar(128)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Description of issue encountered</td>
</tr>
</tbody>
</table>

**Purpose:** Track recordings with playback issues

### Table Name: rec_notes_and_scoring

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>recording_id</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>recordings.recording_id</td>
</tr>
<tr>
<td>user_rating</td>
<td>tinyint(3)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Rating the user assigns to this recording</td>
</tr>
<tr>
<td>complete_status</td>
<td>tinyint(3)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Does the recording show a complete transaction</td>
</tr>
<tr>
<td>hours</td>
<td>float</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Hours spent on analysis</td>
</tr>
<tr>
<td>notes</td>
<td>text</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Users notes on the recording</td>
</tr>
<tr>
<td>transcription</td>
<td>text</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Transcription of the session recording</td>
</tr>
</tbody>
</table>

**Purpose:** Notes and transcription data for recordings
### ISR DATABASE SCHEMA DEFINITIONS AND DESCRIPTIONS

#### Table Name: recording_categories
#### Purpose: Link recordings to categories

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ts</td>
<td>int(11)</td>
<td>NOT NULL</td>
<td></td>
<td>auto_increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>recording_id</td>
<td>int(11)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>recordings recording_id category assigned to</td>
</tr>
<tr>
<td>category_id</td>
<td>int(11)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>categories category_id assigned</td>
</tr>
<tr>
<td>active</td>
<td>tinyint(1)</td>
<td></td>
<td>0 = inactive 1 = active</td>
<td>0</td>
<td>is category still used</td>
</tr>
<tr>
<td>created_at</td>
<td>datetime</td>
<td></td>
<td>NULL</td>
<td>NULL</td>
<td>Date category was assigned to recording</td>
</tr>
<tr>
<td>updated_at</td>
<td>datetime</td>
<td></td>
<td>NULL</td>
<td>NULL</td>
<td>Date affection last updated</td>
</tr>
</tbody>
</table>

#### Table Name: recordings
#### Purpose: Recording details and metadata

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>recording_id</td>
<td>bigint(20) unsigned</td>
<td>NOT NULL</td>
<td></td>
<td>auto_increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>file_name</td>
<td>varchar(255)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Recording file name</td>
</tr>
<tr>
<td>file_status</td>
<td>tinyint(3) unsigned</td>
<td>NOT NULL</td>
<td>0 = normal 1 = file not found 2 = file/backup problem reported</td>
<td>0</td>
<td>Recent file status</td>
</tr>
<tr>
<td>ANI</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td></td>
<td>NULL</td>
<td>ANI</td>
</tr>
<tr>
<td>DNS</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td></td>
<td>NULL</td>
<td>DNS</td>
</tr>
<tr>
<td>ACCOUNT_CODE</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>accounts.account_id</td>
</tr>
<tr>
<td>duration</td>
<td>mediumint(8) unsigned</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Duration of recording</td>
</tr>
<tr>
<td>start_time</td>
<td>datetime</td>
<td>NOT NULL</td>
<td></td>
<td>0000-00-00 00:00:00</td>
<td>Session start time</td>
</tr>
<tr>
<td>directory</td>
<td>varchar(255)</td>
<td>NOT NULL</td>
<td></td>
<td>NULL</td>
<td>Recording location</td>
</tr>
<tr>
<td>vmsg_id</td>
<td>mediumint(8) unsigned</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>vmsg.vmsg_id of the RSS the session was recorded on</td>
</tr>
<tr>
<td>custom_1</td>
<td>varchar(100)</td>
<td>NOT NULL</td>
<td></td>
<td>NULL</td>
<td>Account/Route specific session information</td>
</tr>
<tr>
<td>custom_2</td>
<td>varchar(100)</td>
<td>NOT NULL</td>
<td></td>
<td>NULL</td>
<td>Account/Route specific session information</td>
</tr>
<tr>
<td>custom_3</td>
<td>varchar(100)</td>
<td>NOT NULL</td>
<td></td>
<td>NULL</td>
<td>Account/Route specific session information</td>
</tr>
<tr>
<td>custom_4</td>
<td>varchar(100)</td>
<td>NOT NULL</td>
<td></td>
<td>NULL</td>
<td>Account/Route specific session information</td>
</tr>
<tr>
<td>archived</td>
<td>int(1)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Archived status</td>
</tr>
<tr>
<td>route_id</td>
<td>bigint(10) unsigned</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>route_config.route_id this session was recorded against</td>
</tr>
<tr>
<td>archival_remarks</td>
<td>text</td>
<td></td>
<td></td>
<td>comments about archived state</td>
<td></td>
</tr>
<tr>
<td>archival_fail_count</td>
<td>smallint(5) unsigned</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Number of failed attempts to archive this recording</td>
</tr>
<tr>
<td>agent_id</td>
<td>varchar(255)</td>
<td>NOT NULL</td>
<td></td>
<td>NULL</td>
<td>Agent ID</td>
</tr>
<tr>
<td>agent_extension</td>
<td>varchar(128)</td>
<td>NOT NULL</td>
<td></td>
<td>NULL</td>
<td>Agent extension</td>
</tr>
<tr>
<td>archiver_mode</td>
<td>varchar(10)</td>
<td>NOT NULL</td>
<td></td>
<td>Primary Follower</td>
<td>Whether file archival by primary or followers archiver</td>
</tr>
</tbody>
</table>
## Table Name: remote_archivers

### Purpose: Configure archival to remote locations

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>remote_archiver_id</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td>auto_increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>remote_archiver_ip</td>
<td>varchar(50)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Remote IP address</td>
</tr>
<tr>
<td>remote_archiver_state</td>
<td>varchar(50)</td>
<td>NOT NULL</td>
<td>0=pauze, 1=active</td>
<td></td>
<td>Status of remote archiver</td>
</tr>
<tr>
<td>max_file_count</td>
<td>smallint(5)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Number of times the archiver should attempt to move a file before permanently marking it failed</td>
</tr>
<tr>
<td>delete_enabled</td>
<td>smallint(5)</td>
<td>NOT NULL</td>
<td>0=disabled, 1=enabled</td>
<td></td>
<td>Should the archiver delete files from the destination directory after max_file_count?</td>
</tr>
<tr>
<td>www_served_from</td>
<td>varchar(255)</td>
<td>NULL</td>
<td></td>
<td></td>
<td>URL where recordings will be served from, location storage on remote archiver</td>
</tr>
<tr>
<td>cron_schedule</td>
<td>varchar(40)</td>
<td>NULL</td>
<td></td>
<td></td>
<td>Cron schedule of the remote archival job</td>
</tr>
<tr>
<td>web_service_uri</td>
<td>varchar(255)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Remote archival web service URI</td>
</tr>
<tr>
<td>web_service_url_token</td>
<td>varchar(255)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Remote archival web service URL token</td>
</tr>
</tbody>
</table>
Table Name: route_config  

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route_id</td>
<td>int(11) unsigned</td>
<td>NOT NULL</td>
<td>Auto increment</td>
<td></td>
<td>Primary key</td>
</tr>
<tr>
<td>route_type</td>
<td>tinyint(3) unsigned</td>
<td>NOT NULL</td>
<td>0 = DNS 1 = ANI 2 = ANI/DNI</td>
<td>0</td>
<td>Type of route</td>
</tr>
<tr>
<td>route_pattern</td>
<td>varchar(100)</td>
<td>NOT NULL</td>
<td>Value to be evaluated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>account_id</td>
<td>varchar(100)</td>
<td>NOT NULL</td>
<td>Value to be shown as DNS in recordings list</td>
<td></td>
<td></td>
</tr>
<tr>
<td>percent_to_record</td>
<td>smallint(5)</td>
<td>NOT NULL</td>
<td>1-100</td>
<td>-1</td>
<td>Percentage of sessions to record</td>
</tr>
<tr>
<td>recording_enabled</td>
<td>tinyint(3) unsigned</td>
<td>NOT NULL</td>
<td>0 = recording disabled 1 = recording enabled</td>
<td>-1</td>
<td>Is recording enabled for this route</td>
</tr>
<tr>
<td>call_meta_data_src</td>
<td>tinyint(4)</td>
<td>NOT NULL</td>
<td>0 = none 1 = TEAPU</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>defaul_recording_type</td>
<td>tinyint(3) unsigned</td>
<td>NOT NULL</td>
<td>See the admin guide for the supported recording formats</td>
<td>0</td>
<td>The default recording format used for this route</td>
</tr>
<tr>
<td>agent_id_editable_flag</td>
<td>tinyint(3) unsigned</td>
<td>NOT NULL</td>
<td>0 = not editable 1 = editable</td>
<td>0</td>
<td>Can users edit the data in the agent_id field</td>
</tr>
<tr>
<td>rating_editable_flag</td>
<td>tinyint(3) unsigned</td>
<td>NOT NULL</td>
<td>0 = not editable 1 = editable</td>
<td>0</td>
<td>Can users edit the data in the scoring rate information</td>
</tr>
<tr>
<td>completed_editable_flag</td>
<td>tinyint(3) unsigned</td>
<td>NOT NULL</td>
<td>0 = not editable 1 = editable</td>
<td>0</td>
<td>Can users edit the data in the complete transaction flag?</td>
</tr>
<tr>
<td>notes_editable_flag</td>
<td>tinyint(3) unsigned</td>
<td>NOT NULL</td>
<td>0 = not editable 1 = editable</td>
<td>0</td>
<td>Can users edit the scoring notes</td>
</tr>
<tr>
<td>virtual_route_pattern</td>
<td>varchar(100)</td>
<td>NOT NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>User value that will be set in the sipuri on call leg from R3S</td>
</tr>
<tr>
<td>announce_audio_file</td>
<td>varchar(100)</td>
<td>Text</td>
<td>NULL</td>
<td>NULL</td>
<td>Announcement to be played on this route</td>
</tr>
<tr>
<td>announce_audio_text</td>
<td>varchar(100)</td>
<td>Text</td>
<td>NULL</td>
<td>NULL</td>
<td>TTS fallback in the event the announcement file is not available</td>
</tr>
<tr>
<td>opt_out_xml_file</td>
<td>varchar(100)</td>
<td>Text</td>
<td>NULL</td>
<td>NULL</td>
<td>YAML file for implementing output on this route*</td>
</tr>
<tr>
<td>opt_out_xml</td>
<td>tinyint(1)</td>
<td>NOT NULL</td>
<td>0 = disabled 1 = enabled</td>
<td>0</td>
<td>Whether opt out is enabled</td>
</tr>
<tr>
<td>announce_enabled</td>
<td>tinyint(1)</td>
<td>NOT NULL</td>
<td>0 = announcement disabled 1 = announcement enabled</td>
<td>0</td>
<td>Whether announcements are enabled for this route</td>
</tr>
<tr>
<td>custom_data_1_name</td>
<td>varchar(45)</td>
<td>Text</td>
<td>NULL</td>
<td>Name of Custom Data 1 Field (must match API calls)</td>
<td></td>
</tr>
<tr>
<td>custom_data_1_friendly_name</td>
<td>varchar(45)</td>
<td>Text</td>
<td>Custom Data Field 1 Displayed name of Custom Data 1 Field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>custom_data_1_editable_flag</td>
<td>tinyint(3) unsigned</td>
<td>NOT NULL</td>
<td>0 = not editable 1 = editable</td>
<td>0</td>
<td>Can users edit Custom Data 1 Field</td>
</tr>
<tr>
<td>custom_data_2_name</td>
<td>varchar(45)</td>
<td>Text</td>
<td>NULL</td>
<td>Name of Custom Data 2 Field (must match API calls)</td>
<td></td>
</tr>
<tr>
<td>custom_data_2_friendly_name</td>
<td>varchar(45)</td>
<td>Text</td>
<td>Custom Data Field 2 Displayed name of Custom Data 2 Field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>custom_data_2_editable_flag</td>
<td>tinyint(3) unsigned</td>
<td>NOT NULL</td>
<td>0 = not editable 1 = editable</td>
<td>0</td>
<td>Can users edit Custom Data 2 Field</td>
</tr>
<tr>
<td>custom_data_3_name</td>
<td>varchar(45)</td>
<td>Text</td>
<td>NULL</td>
<td>Name of Custom Data 3 Field (must match API calls)</td>
<td></td>
</tr>
<tr>
<td>custom_data_3_friendly_name</td>
<td>varchar(45)</td>
<td>Text</td>
<td>Custom Data Field 3 Displayed name of Custom Data 3 Field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>custom_data_3_editable_flag</td>
<td>tinyint(3) unsigned</td>
<td>NOT NULL</td>
<td>0 = not editable 1 = editable</td>
<td>0</td>
<td>Can users edit Custom Data 3 Field</td>
</tr>
</tbody>
</table>
### ISR DATABASE SCHEMA DEFINITIONS AND DESCRIPTIONS

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>custom_data_4_name</td>
<td>varchar(45)</td>
<td>Text</td>
</tr>
<tr>
<td>custom_data_4_name</td>
<td>NULL</td>
<td>Name of Custom Data 4 Field (must match API calls)</td>
</tr>
<tr>
<td>custom_data_4_friendly_name</td>
<td>varchar(45)</td>
<td>Text</td>
</tr>
<tr>
<td>custom_data_4_visible_flag</td>
<td>tinyint(4)</td>
<td>NOT NULL</td>
</tr>
<tr>
<td>custom_data_4_visible_flag</td>
<td>0</td>
<td>Displayed name of Custom Data 4 Field</td>
</tr>
<tr>
<td>application</td>
<td>varchar(45)</td>
<td>Text</td>
</tr>
<tr>
<td>application</td>
<td>NULL</td>
<td>Route type used for this route</td>
</tr>
<tr>
<td>play_beep_before_record</td>
<td>tinyint(4)</td>
<td>NOT NULL</td>
</tr>
<tr>
<td>play_beep_before_record</td>
<td>0</td>
<td>Should the beep tone be played on route</td>
</tr>
<tr>
<td>terminate_on_drop</td>
<td>tinyint(4)</td>
<td>NOT NULL</td>
</tr>
<tr>
<td>terminate_on_drop</td>
<td>0</td>
<td>Should a conference mode recording terminate on DTMP entry</td>
</tr>
<tr>
<td>terminate_on_end</td>
<td>tinyint(4)</td>
<td>NOT NULL</td>
</tr>
<tr>
<td>terminate_on_end</td>
<td>-1</td>
<td>Should a conference mode recording terminate on end of speech</td>
</tr>
<tr>
<td>priority</td>
<td>float</td>
<td>NOT NULL</td>
</tr>
<tr>
<td>priority</td>
<td>0.8</td>
<td>Order in which routes will be evaluated</td>
</tr>
<tr>
<td>maximum_number_of_ports</td>
<td>int(11)</td>
<td>NOT NULL</td>
</tr>
<tr>
<td>maximum_number_of_ports</td>
<td>24</td>
<td>Maximum number of simultaneous sessions this route will be able to support.</td>
</tr>
<tr>
<td>number_of_burst_ports</td>
<td>int(10)</td>
<td>NOT NULL</td>
</tr>
<tr>
<td>number_of_burst_ports</td>
<td>0</td>
<td>Default number of ports over maximum that the route will be able to use. These ports are reported separately.</td>
</tr>
<tr>
<td>storage_size_period</td>
<td>int(10)</td>
<td>NOT NULL</td>
</tr>
<tr>
<td>storage_size_period</td>
<td>0</td>
<td>Number of days over minimum_storage_days that archiver should keep the recording before deleting.</td>
</tr>
<tr>
<td>recurring_beep_enabled</td>
<td>tinyint(4)</td>
<td>NOT NULL</td>
</tr>
<tr>
<td>recurring_beep_enabled</td>
<td>0</td>
<td>Enable/Disable recurring beep played during recording</td>
</tr>
<tr>
<td>recurring_beep_interval</td>
<td>int(10)</td>
<td>NOT NULL</td>
</tr>
<tr>
<td>recurring_beep_interval</td>
<td>0</td>
<td>If enabled, how often should the beep be played</td>
</tr>
<tr>
<td>recurring_beep_file</td>
<td>varchar(45)</td>
<td>Text</td>
</tr>
<tr>
<td>recurring_beep_file</td>
<td>beep.wav</td>
<td>Name of file, stored in RSA Cache, that should be played</td>
</tr>
<tr>
<td>record_save_disk</td>
<td>varchar(45)</td>
<td>Text</td>
</tr>
<tr>
<td>record_save_disk</td>
<td>#</td>
<td>single-digit, dlmn that will save a recording made on a record &amp; save route</td>
</tr>
</tbody>
</table>
### Table Name: route_groups

**Purpose:** Create and define a group of routes that should all have the same master requirements

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route_group_member_id</td>
<td>INT(11)</td>
<td>NOT NULL</td>
<td></td>
<td>auto_increment</td>
<td>primary key</td>
</tr>
<tr>
<td>route_group_master_id</td>
<td>INT(10)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>route_group_master_id in the master ID</td>
</tr>
<tr>
<td>route_pattern</td>
<td>VARCHAR(100)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>route pattern to be evaluated</td>
</tr>
<tr>
<td>virtual_route_pattern</td>
<td>VARCHAR(100)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>user value of end destination</td>
</tr>
</tbody>
</table>

### Table Name: route_map_tracking_events

**Purpose:** Track events related to the route map caching

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>INT(10)</td>
<td>NOT NULL</td>
<td></td>
<td>auto_increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>object_type</td>
<td>smallint(2) unsigned</td>
<td>NOT NULL</td>
<td>0 = SOURCE, 1 = route, 2 = destination</td>
<td></td>
<td>object event pertains to</td>
</tr>
<tr>
<td>action_type</td>
<td>smallint(2) unsigned</td>
<td>NOT NULL</td>
<td>0 = add, 1 = changed, 2 = delete</td>
<td></td>
<td>type of action</td>
</tr>
<tr>
<td>action_time</td>
<td>timestamp</td>
<td>NOT NULL</td>
<td></td>
<td>CURRENT_TIMESTAMP</td>
<td>time of event</td>
</tr>
<tr>
<td>src_id</td>
<td>INT(10)</td>
<td>NOT NULL</td>
<td></td>
<td>-1</td>
<td>sites src_id event pertains to</td>
</tr>
<tr>
<td>additional_info</td>
<td>VARCHAR(100)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>additional information</td>
</tr>
</tbody>
</table>
## Table Name: saved_searches

**Purpose:** Define searches saved in User Dashboard

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>int[11]</td>
<td>NOT NULL</td>
<td></td>
<td>auto_increment</td>
<td>primary key</td>
</tr>
<tr>
<td>user_id</td>
<td>int[11]</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>users.user_id which saved the search</td>
</tr>
<tr>
<td>name</td>
<td>varchar[255]</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>name of saved search</td>
</tr>
<tr>
<td>mode</td>
<td>int[11]</td>
<td></td>
<td>1</td>
<td></td>
<td>Type of saved search</td>
</tr>
<tr>
<td>ari</td>
<td>varchar[255]</td>
<td>NULL</td>
<td>NULL</td>
<td></td>
<td>ARi provided in search</td>
</tr>
<tr>
<td>dns</td>
<td>varchar[255]</td>
<td>NULL</td>
<td>NULL</td>
<td></td>
<td>DNS provided in search</td>
</tr>
<tr>
<td>filename</td>
<td>varchar[255]</td>
<td>NULL</td>
<td>NULL</td>
<td></td>
<td>Filename provided in search</td>
</tr>
<tr>
<td>agent_id</td>
<td>varchar[255]</td>
<td>NULL</td>
<td>NULL</td>
<td></td>
<td>Agent ID provided in search</td>
</tr>
<tr>
<td>duration</td>
<td>varchar[255]</td>
<td>NULL</td>
<td>NULL</td>
<td></td>
<td>Duration of recordings provided in search</td>
</tr>
<tr>
<td>custom1</td>
<td>varchar[255]</td>
<td>NULL</td>
<td>NULL</td>
<td></td>
<td>Value to search in custom data field 1</td>
</tr>
<tr>
<td>custom2</td>
<td>varchar[255]</td>
<td>NULL</td>
<td>NULL</td>
<td></td>
<td>Value to search in custom data field 2</td>
</tr>
<tr>
<td>custom3</td>
<td>varchar[255]</td>
<td>NULL</td>
<td>NULL</td>
<td></td>
<td>Value to search in custom data field 3</td>
</tr>
<tr>
<td>custom4</td>
<td>varchar[255]</td>
<td>NULL</td>
<td>NULL</td>
<td></td>
<td>Value to search in custom data field 4</td>
</tr>
<tr>
<td>vring</td>
<td>varchar[255]</td>
<td>NULL</td>
<td>NULL</td>
<td></td>
<td>Value to search in vring</td>
</tr>
<tr>
<td>duration_start</td>
<td>varchar[255]</td>
<td>NULL</td>
<td>NULL</td>
<td></td>
<td>Search duration minimum duration</td>
</tr>
<tr>
<td>duration_stop</td>
<td>varchar[255]</td>
<td>NULL</td>
<td>NULL</td>
<td></td>
<td>Search duration maximum duration</td>
</tr>
<tr>
<td>date_start</td>
<td>varchar[255]</td>
<td>NULL</td>
<td>NULL</td>
<td></td>
<td>Search calls after this date</td>
</tr>
<tr>
<td>date_stop</td>
<td>varchar[255]</td>
<td>NULL</td>
<td>NULL</td>
<td></td>
<td>Search calls before this date</td>
</tr>
<tr>
<td>allow_partial</td>
<td>tinyint[1]</td>
<td>0 = do not allow</td>
<td>1 = allow</td>
<td></td>
<td>Search for partial match of values within specified fields</td>
</tr>
<tr>
<td>active</td>
<td>tinyint[1]</td>
<td>0 = inactive</td>
<td>1 = active</td>
<td></td>
<td>Search is currently active</td>
</tr>
<tr>
<td>date_related</td>
<td>varchar[255]</td>
<td>NULL</td>
<td>NULL</td>
<td></td>
<td>Search related to which date</td>
</tr>
<tr>
<td>date_search_type</td>
<td>varchar[255]</td>
<td>NULL</td>
<td>range</td>
<td></td>
<td>Type of date search to perform</td>
</tr>
<tr>
<td>created_on</td>
<td>date-time</td>
<td>NULL</td>
<td>NULL</td>
<td></td>
<td>Date search initially saved</td>
</tr>
<tr>
<td>updated_on</td>
<td>date-time</td>
<td>NULL</td>
<td>NULL</td>
<td></td>
<td>Date of last update to search criteria</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Type</td>
<td>Nullability</td>
<td>Supported Values</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------</td>
<td>-------------</td>
<td>------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------</td>
</tr>
<tr>
<td>security_id</td>
<td>INT(10)</td>
<td>NOT NULL</td>
<td>AUTO_INCREMENT</td>
<td>PRIMARY KEY</td>
<td>Configure dashboard security settings</td>
</tr>
<tr>
<td>password_expires_days</td>
<td>INT(10)</td>
<td>NOT NULL</td>
<td>0, 1, 2</td>
<td>90</td>
<td>Number of days before a user password expires</td>
</tr>
<tr>
<td>password_strength_requirements</td>
<td>TINYINT(3)</td>
<td>NOT NULL</td>
<td>0, 1, 2</td>
<td>2</td>
<td>How strong does a user password need to be</td>
</tr>
<tr>
<td>lockout_time_seconds</td>
<td>INT(10)</td>
<td>NOT NULL</td>
<td>0, 1, 2</td>
<td>3000</td>
<td>Length of time a user will be locked out after max_failed_logins_before_lockout</td>
</tr>
<tr>
<td>max_failed_logins_before_lockout</td>
<td>TINYINT(3)</td>
<td>NOT NULL</td>
<td>0, 1, 2</td>
<td>5</td>
<td>Number of failed login attempts a user will be allowed before being locked out</td>
</tr>
<tr>
<td>maximum_password_history</td>
<td>TINYINT(3)</td>
<td>NOT NULL</td>
<td>0, 1, 2</td>
<td>4</td>
<td>Number of password changes before a user can reuse a password</td>
</tr>
<tr>
<td>show_forgotten_password_page</td>
<td>TINYINT(3)</td>
<td>NOT NULL</td>
<td>0, 1, 2</td>
<td>0</td>
<td>Should users see the link to be emailed a password</td>
</tr>
<tr>
<td>aes_cipher_key</td>
<td>VARCHAR(32)</td>
<td>NULL</td>
<td></td>
<td>Cypher key used for encryption of data</td>
<td></td>
</tr>
<tr>
<td>change_date</td>
<td>DATETIME</td>
<td>NOT NULL</td>
<td></td>
<td>Date of last security change</td>
<td></td>
</tr>
<tr>
<td>changed_by_user_id</td>
<td>INT(10)</td>
<td>NOT NULL</td>
<td></td>
<td>Users user_id who made last change</td>
<td></td>
</tr>
</tbody>
</table>
### Table Name: sites

**Purpose:** Configuration of site information

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>site_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>site_description</td>
<td>varchar(49)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Site name</td>
</tr>
<tr>
<td>site_level</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td>0 = Primary, 1 = Secondary</td>
<td></td>
<td>Site type</td>
</tr>
<tr>
<td>primary_site_db_ip</td>
<td>varchar(15)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Database IP to be used with this site</td>
</tr>
<tr>
<td>primary_site_db_link_status</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td>0 = Up, 1 = Down, 2 = Sync needed, 3 = Sync in Progress</td>
<td>0</td>
<td>DB status</td>
</tr>
<tr>
<td>gateway_max_failure_count</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>5</td>
<td>Sets the maximum number of outbound gateway failures allowed in max_fol_seconds before gateway is disabled</td>
</tr>
<tr>
<td>gateway_max_failure_secs</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>30</td>
<td>Number of seconds that number of failures can occur before gateway is disabled</td>
</tr>
<tr>
<td>gateway_min_secs_before_retry</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>300</td>
<td>once temp disabled, how long before the gateway will be reinitialized</td>
</tr>
</tbody>
</table>

### Table Name: tokens

**Purpose:** Assign tokens to sessions

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>token_id</td>
<td>int(20)</td>
<td>NOT NULL</td>
<td></td>
<td>auto increment</td>
<td>Primary key, zero fill</td>
</tr>
<tr>
<td>session_id</td>
<td>varchar(256)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Session ID token assigned to</td>
</tr>
<tr>
<td>timestamp</td>
<td>datetime</td>
<td>NOT NULL</td>
<td></td>
<td>0000-00-00 00:00:00</td>
<td>Session time</td>
</tr>
</tbody>
</table>

### Table Name: user_accounts

**Purpose:** Affiliate users with accounts

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>users.user_id</td>
<td>Users user_id</td>
</tr>
<tr>
<td>account_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>accounts.account_id</td>
<td>Accounts account_id</td>
</tr>
<tr>
<td>db_routes_in_account_access</td>
<td>int(3)</td>
<td>NOT NULL</td>
<td>0 = disabled, 1 = enabled</td>
<td></td>
<td>Does user have access to all routes in account</td>
</tr>
</tbody>
</table>
### Table Name: user_display_preferences

**Purpose:** Configure user preferences in User Dashboard

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>int(11)</td>
<td>NOT NULL</td>
<td></td>
<td>AUTO_INCREMENT</td>
<td>Primary key</td>
</tr>
<tr>
<td>user_id</td>
<td>int(11)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>users.user_id preferences parent to</td>
</tr>
<tr>
<td>name</td>
<td>varchar(255)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>priority</td>
<td>int(11)</td>
<td></td>
<td></td>
<td>0</td>
<td>Priority</td>
</tr>
<tr>
<td>created_at</td>
<td>datetime</td>
<td>NULL</td>
<td></td>
<td>NULL</td>
<td>Date preferences created</td>
</tr>
<tr>
<td>updated_at</td>
<td>datetime</td>
<td>NULL</td>
<td></td>
<td>NULL</td>
<td>Date preferences last updated</td>
</tr>
</tbody>
</table>

### Table Name: user_routes

**Purpose:** Affiliate users with routes

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route_id</td>
<td>int(10)</td>
<td>unsigned</td>
<td>NOT NULL</td>
<td></td>
<td>route_config.route_id</td>
</tr>
<tr>
<td>user_id</td>
<td>int(10)</td>
<td>unsigned</td>
<td>NOT NULL</td>
<td></td>
<td>users.user_id</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Type</td>
<td>Nullable</td>
<td>Supported Values</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>------------</td>
<td>----------</td>
<td>------------------</td>
<td>---------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>user_type_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>auto</td>
<td>Increment Primary key</td>
</tr>
<tr>
<td>user_type_name</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td></td>
<td>auto</td>
<td>Name of the user type</td>
</tr>
<tr>
<td>account_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>auto</td>
<td>Account ID this user is specifically tied to</td>
</tr>
<tr>
<td>priv_sys_create</td>
<td>tinyint(3)</td>
<td>NULL</td>
<td>0 = disabled</td>
<td>0</td>
<td>User can create system elements</td>
</tr>
<tr>
<td>priv_sys_modify</td>
<td>tinyint(3)</td>
<td>NULL</td>
<td>0 = disabled</td>
<td>0</td>
<td>User can modify system elements</td>
</tr>
<tr>
<td>priv_sys_view</td>
<td>tinyint(3)</td>
<td>NULL</td>
<td>0 = disabled</td>
<td>0</td>
<td>User can view system elements</td>
</tr>
<tr>
<td>priv_account_create</td>
<td>tinyint(3)</td>
<td>NULL</td>
<td>0 = disabled</td>
<td>0</td>
<td>User can create accounts</td>
</tr>
<tr>
<td>priv_account_modify</td>
<td>tinyint(3)</td>
<td>NULL</td>
<td>0 = disabled</td>
<td>0</td>
<td>User can modify accounts</td>
</tr>
<tr>
<td>priv_account_view</td>
<td>tinyint(3)</td>
<td>NULL</td>
<td>0 = disabled</td>
<td>0</td>
<td>User can view accounts</td>
</tr>
<tr>
<td>priv_route_create</td>
<td>tinyint(3)</td>
<td>NULL</td>
<td>0 = disabled</td>
<td>0</td>
<td>User can create routes</td>
</tr>
<tr>
<td>priv_route_modify</td>
<td>tinyint(3)</td>
<td>NULL</td>
<td>0 = disabled</td>
<td>0</td>
<td>User can modify routes</td>
</tr>
<tr>
<td>priv_route_view</td>
<td>tinyint(3)</td>
<td>NULL</td>
<td>0 = disabled</td>
<td>0</td>
<td>User can view routes</td>
</tr>
<tr>
<td>priv_user_create</td>
<td>tinyint(3)</td>
<td>NULL</td>
<td>0 = disabled</td>
<td>0</td>
<td>User can create users</td>
</tr>
<tr>
<td>priv_user_modify</td>
<td>tinyint(3)</td>
<td>NULL</td>
<td>0 = disabled</td>
<td>0</td>
<td>User can modify users</td>
</tr>
<tr>
<td>priv_user_view</td>
<td>tinyint(3)</td>
<td>NULL</td>
<td>0 = disabled</td>
<td>0</td>
<td>User can view users</td>
</tr>
<tr>
<td>priv_recording_create</td>
<td>tinyint(3)</td>
<td>NULL</td>
<td>0 = disabled</td>
<td>0</td>
<td>User can create recordings</td>
</tr>
<tr>
<td>priv_recording modify</td>
<td>tinyint(3)</td>
<td>NULL</td>
<td>0 = disabled</td>
<td>0</td>
<td>User can modify recording / data</td>
</tr>
<tr>
<td>priv_recording_view</td>
<td>tinyint(3)</td>
<td>NULL</td>
<td>0 = disabled</td>
<td>0</td>
<td>User can view recordings / data</td>
</tr>
</tbody>
</table>
**Table Name:** users  
**Purpose:** Define users, track login history and their dashboard preferences

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>auto_increment</td>
<td>primary key</td>
</tr>
<tr>
<td>user_name</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>User's name</td>
</tr>
<tr>
<td>user_email</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>User's login</td>
</tr>
<tr>
<td>description</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>User description</td>
</tr>
<tr>
<td>user_pass</td>
<td>varchar(42)</td>
<td>NULL</td>
<td></td>
<td></td>
<td>User's password</td>
</tr>
<tr>
<td>password_type</td>
<td>tinyint(3)</td>
<td>NOT NULL</td>
<td>0 = MD5, 1 = AES</td>
<td>0</td>
<td>What type of encryption was used on password</td>
</tr>
<tr>
<td>user_type_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>user_type.user_type_id</td>
</tr>
<tr>
<td>last_login</td>
<td>datetime</td>
<td>NULL</td>
<td></td>
<td></td>
<td>Date of last login</td>
</tr>
<tr>
<td>account_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Primary account user is affiliated with</td>
</tr>
<tr>
<td>delete_permission</td>
<td>tinyint(3)</td>
<td>NOT NULL</td>
<td>0 = disabled (can delete), 1 = enabled (can delete)</td>
<td>1</td>
<td>Can user delete recordings</td>
</tr>
<tr>
<td>last_pass_change</td>
<td>datetime</td>
<td>NULL</td>
<td></td>
<td></td>
<td>Date of last password change</td>
</tr>
<tr>
<td>login_check</td>
<td>tinyint(3)</td>
<td>NOT NULL</td>
<td>0 = enabled, 1 = disabled</td>
<td>0</td>
<td>Login active</td>
</tr>
<tr>
<td>failed_login_attempts</td>
<td>tinyint(3)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>Number of failed login attempts since last successful login</td>
</tr>
<tr>
<td>last_failed_login_attempt</td>
<td>datetime</td>
<td>NULL</td>
<td></td>
<td></td>
<td>Date and time of last failed login attempt</td>
</tr>
<tr>
<td>previous_password_0</td>
<td>varchar(42)</td>
<td>NULL</td>
<td></td>
<td></td>
<td>User's prior password</td>
</tr>
<tr>
<td>previous_password_1</td>
<td>varchar(42)</td>
<td>NULL</td>
<td></td>
<td></td>
<td>User's prior password</td>
</tr>
<tr>
<td>previous_password_2</td>
<td>varchar(42)</td>
<td>NULL</td>
<td></td>
<td></td>
<td>User's prior password</td>
</tr>
<tr>
<td>previous_password_3</td>
<td>varchar(42)</td>
<td>NULL</td>
<td></td>
<td></td>
<td>User's prior password</td>
</tr>
<tr>
<td>audit_view_permission</td>
<td>tinyint(3)</td>
<td>NOT NULL</td>
<td>0 = cannot view audit logs, 1 = can view audit logs</td>
<td>0</td>
<td>Can user view audit logs</td>
</tr>
<tr>
<td>timezone_offset</td>
<td>tinyint(4)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>User's timezone in relation to GMT</td>
</tr>
<tr>
<td>call_control_permission</td>
<td>tinyint(3)</td>
<td>NOT NULL</td>
<td>0 = cannot view, 1 = can view</td>
<td>0</td>
<td>Can user see call control option</td>
</tr>
<tr>
<td>edit_recording_data_permission</td>
<td>tinyint(3)</td>
<td>NOT NULL</td>
<td>0 = cannot edit, 1 = can edit</td>
<td>0</td>
<td>Can user edit recording metadata</td>
</tr>
<tr>
<td>view_and_inserting_permission</td>
<td>tinyint(3)</td>
<td>NOT NULL</td>
<td>0 = cannot view, 1 = can view</td>
<td>0</td>
<td>Can user view and insert into call data</td>
</tr>
<tr>
<td>dash_refresh_rate</td>
<td>tinyint(3)</td>
<td>NOT NULL</td>
<td></td>
<td>10</td>
<td>Rate at which dashboard refreshes</td>
</tr>
<tr>
<td>dash_start_page</td>
<td>varchar(20)</td>
<td>NOT NULL</td>
<td></td>
<td>recordings</td>
<td>Page displayed when user logs in</td>
</tr>
<tr>
<td>dash_max_logs</td>
<td>tinyint(5)</td>
<td>NOT NULL</td>
<td></td>
<td>40</td>
<td>Number of pages of logs to show</td>
</tr>
<tr>
<td>dash_max_logs_per_page</td>
<td>tinyint(3)</td>
<td>NOT NULL</td>
<td></td>
<td>10</td>
<td>Number of logs to show per page</td>
</tr>
<tr>
<td>dash_max_display_items_per_page</td>
<td>tinyint(3)</td>
<td>NOT NULL</td>
<td></td>
<td>10</td>
<td>Number of items (not logs) to show per page</td>
</tr>
<tr>
<td>dash_use_all_account_access</td>
<td>tinyint(3)</td>
<td>NOT NULL</td>
<td>0 = not by default, 1 = by default</td>
<td>0</td>
<td>Does user have access to all routes under their assigned account (only implemented in User Dashboard)</td>
</tr>
<tr>
<td>user_configuration</td>
<td>varchar(255)</td>
<td>NULL</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table Name: vmg_channel_lookup

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmg_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>vmg_id, RSS handling session</td>
</tr>
<tr>
<td>channel_no</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>channel number handling session</td>
</tr>
<tr>
<td>ANI</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>ANI of active session</td>
</tr>
<tr>
<td>DNS</td>
<td>varchar(45)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>DNS of active session</td>
</tr>
<tr>
<td>start_of_call</td>
<td>datetime</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>session start time</td>
</tr>
<tr>
<td>recording_file_name</td>
<td>varchar(100)</td>
<td>NULL</td>
<td></td>
<td>NULL</td>
<td>name of file being recorded for this session</td>
</tr>
<tr>
<td>virtual_dial</td>
<td>varchar(45)</td>
<td>NULL</td>
<td></td>
<td>NULL</td>
<td>virtual route pattern invoked on this session</td>
</tr>
<tr>
<td>route_id</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>route ID invoked on this session</td>
</tr>
<tr>
<td>account_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>1</td>
<td>account ID for this session</td>
</tr>
<tr>
<td>cell_state</td>
<td>tinyint(2)</td>
<td>NOT NULL</td>
<td></td>
<td>0 = unknown, 1 = observed</td>
<td></td>
</tr>
</tbody>
</table>

**Purpose:** Mapping of sessions to channels on the RSS

### Table Name: vmgs

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmg_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>vmg_ip</td>
<td>varchar(64)</td>
<td>NULL</td>
<td></td>
<td>NULL</td>
<td>RSS IP address - SIP signaling</td>
</tr>
<tr>
<td>vmg_description</td>
<td>varchar(64)</td>
<td>NULL</td>
<td></td>
<td>NULL</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>www_served_from</td>
<td>varchar(255)</td>
<td>NULL</td>
<td></td>
<td>NULL</td>
<td>URL where recordings stored on this RSS will be served from</td>
</tr>
<tr>
<td>site_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td>0</td>
<td>Site this RSS is affiliated with</td>
</tr>
<tr>
<td>location</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td>-1</td>
<td>Locations location_id for primary recording storage</td>
</tr>
<tr>
<td>follower_location</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td>-1</td>
<td>Locations location_id for follower recording storage</td>
</tr>
<tr>
<td>xmllrppe_port</td>
<td>varchar(7)</td>
<td>NOT NULL</td>
<td></td>
<td>9999</td>
<td>Xmllrppe port this RSS is listening on</td>
</tr>
</tbody>
</table>

**Purpose:** RSS configuration
**Table Name: webservice_destinations**  
**Purpose:** Configure webservices (through appliances tab)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Nullable</th>
<th>Supported Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>webservice_id</td>
<td>bigint(20)</td>
<td>NOT NULL</td>
<td></td>
<td>auto-increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>account_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>accounts.account_id info that will be sent to this webservice</td>
</tr>
<tr>
<td>route_id</td>
<td>int(10)</td>
<td>NOT NULL</td>
<td></td>
<td></td>
<td>route_config.route_id info that will be sent to this webservice</td>
</tr>
<tr>
<td>max_retries</td>
<td>tinyint(5)</td>
<td>NOT NULL</td>
<td></td>
<td>5</td>
<td>number of attempts to send a record to webservice before marked as failures: 0 = unlimited attempts</td>
</tr>
<tr>
<td>max_simultaneous_connections</td>
<td>tinyint(5)</td>
<td>NOT NULL</td>
<td></td>
<td>12</td>
<td>maximum number of simultaneous connections; unlimited</td>
</tr>
<tr>
<td>url_1</td>
<td>varchar(255)</td>
<td>NOT NULL</td>
<td></td>
<td>NULL</td>
<td>Primary web service URL</td>
</tr>
<tr>
<td>url_2</td>
<td>varchar(255)</td>
<td>NOT NULL</td>
<td></td>
<td>NULL</td>
<td>Secondary web service URL</td>
</tr>
<tr>
<td>url_3</td>
<td>varchar(255)</td>
<td>NOT NULL</td>
<td></td>
<td>NULL</td>
<td>Tertiary web service URL</td>
</tr>
<tr>
<td>webservice_state</td>
<td>tinyint(2)</td>
<td>NOT NULL</td>
<td>0 = paused, 1 = unpaused</td>
<td>0</td>
<td>Webservice state</td>
</tr>
<tr>
<td>delete_enabled</td>
<td>tinyint(2)</td>
<td>NOT NULL</td>
<td>0 = disabled, 1 = enabled</td>
<td>0</td>
<td>Can web service delete</td>
</tr>
<tr>
<td>pusher_host</td>
<td>varchar(100)</td>
<td>NULL</td>
<td></td>
<td>NULL</td>
<td>current pusher host name</td>
</tr>
</tbody>
</table>