

Interactive Session Recorder

Administrator Guide



Release 6.2

F20203-05

January 2021

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Interactive Session Recorder Administrator Guide, Release 6.2

F20203-05

Copyright © 2014, 2021, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

About This Guide

1 Overview

About the ISR	1-1
Session Recording Client Support	1-2
SelectiveCall Recording SIPREC	1-2
SIPREC for Active Recording	1-3
Preserve SIPREC with SIP REFER Header	1-4
Configuring SIPREC	1-4
ISR FACE	1-4
About the ISR Dashboard	1-5
Requirements	
Recommendations	1-5
Security Features	1-5

2 Getting Started

Logging In/Out of the ISR Dashboard	2-1
User Access Levels	2-5
Help Link	2-6
Editing My Settings	2-7
Recordings List Settings	2-9
RSS View Settings	2-9
Change Password	2-10
Dashboard Tools	2-10
Functional Icons	2-10
Paging Tool	2-12
Search Tools	2-12
Basic Search for Recordings	2-12
Advanced Search for Recordings	2-13
More Recording Search Options	2-15
Recording Search by Segment	2-16

Recording Search by Custom Data	2-17
Recording Search by Session	2-17
Basic Search for Routes	2-19
Column Sorting Tool	2-20
Download Tool	2-20
Downloading a Single Recording File	2-20
Downloading a Recording List to a CSV File	2-21
Import Link	2-24
Administrator Menu	2-24

3 Managing Accounts

Managing Accounts	3-1
Adding an Account	3-2
Configuring/ Editing Details for an Account	3-3
Edit General Account Information	3-3
Archival	3-5
Dashboard Configurations	3-8
Permissions	3-11
Route Defaults	3-11
Routes	3-15
Users	3-15
Video	3-15
Deleting an Account	3-15
Importing an Account CSV File	3-16

4 Managing Realms

Managing Realms	4-1
How Realm-based Recording Works	4-1
Adding a Realm	4-3
Associating an Account to a Realm	4-4
Editing a Realm	4-4
Deleting a Realm	4-5

5 Managing Routes

Manage Routes	5-1
Adding a Route	5-2
Adding a Route Configuration	5-2
Examples of Route Patterns	5-4
Configuring and Editing Details of a Route	5-5

Edit General Route Information	5-5
Route Advanced Configurations	5-6
Recording	5-7
Recording Editing Permissions	5-7
Video	5-7
Record and Save Mode	5-8
Capacity	5-8
Archiving	5-8
Upgrade to Route Group	5-8
Adding a Route to a Route Group	5-8
Deleting a Route	5-9
Importing a Route CSV File	5-10

6 Managing Users

Manage Users	6-1
User Access Levels	6-2
Adding a User	6-2
Editing a User Profile	6-5
Showing User Activity	6-7
Deleting a User	6-8
Importing a User Profile CSV File	6-8

7 Managing Authorization Services

Manage Authorization Services	7-1
Adding an Authorization Service	7-2
Editing an Authorization Service	7-3
Deleting an Authorization Service	7-4

8 Custom Data

Viewing and Editing the Custom Data Master List	8-1
Viewing and Editing Custom Data Field Session Values	8-2
Custom Data Fields Advanced Search	8-2

9 External Event Destinations

External Event Notifications	9-1
Configuring External Event Destinations	9-1
External Event Configuration Example	9-2

10 Managing Locales

Manage Locales	10-1
Adding a New Locale	10-1

11 Managing Recording Format Profiles

Editing a Recording Format Profile	11-1
Recording Format Mappings Configuration	11-2
Applying Recording Format Profiles to Accounts	11-2
Applying Recording Format Profiles to Routes	11-3
Route Recording File Permissions	11-4

12 Managing Security Settings

13 Managing Template Definitions

Template Definitions	13-1
Formatting	13-1
Field Parameters	13-1
Adding a New Template	13-3
Recordings with No Media	13-4

14 Viewing Live Sessions

Manage Live Sessions	14-1
----------------------	------

15 Managing Sites

Manage Sites	15-1
Adding a Site	15-2
Managing an RSS	15-3
Sites RSS Summary	15-3
Adding an RSS	15-3
Editing an RSS	15-4
Deleting an RSS	15-7
Managing an RSS Location	15-7
Adding a Location	15-7
Editing a Location	15-11
Deleting a Location	15-11

Managing Archivers	15-12
Adding an Archiver	15-13
Editing an Archiver	15-15
Deleting an Archiver	15-15

16 Managing Recordings

Manage Recordings	16-1
Playing a Recording	16-2
Viewing and Editing Details of a Recording	16-3
Viewing Recording Details	16-4
Notes and Scoring	16-5
Recording Details Custom Data	16-6
Recording Details File Location	16-7
Archiving Recordings Permanently	16-7
Segment Details Configuration	16-7
Segment Recording Details Custom Data	16-8
Recording Supplemental Files	16-8
Segment Session Metadata	16-8
Segment Session Participant Metadata	16-9
Displaying DTMF Data in Segment Details: Routes	16-10
Displaying DTMF Data in Segment Details: Accounts	16-11
Displaying DTMF Data in Segment Details	16-11
Deleting a Recording	16-12

17 Managing Reports

Manage Reports	17-1
Usage Reports	17-2
Generating a Usage Report	17-2
Generating a report by month	17-2
Generating a report by range	17-2
Selecting a route	17-3
Usage Report Bar Graph Descriptions	17-3
Billing Reports	17-5
Generating a Billing Report	17-6
Generating a Report by Month	17-6
Generating a Report by Range	17-6
Selecting a Route	17-7
Billing Report Bar Graph Descriptions	17-7

A Software Diagrams and Call Setup Sequence

ISR Recorder Process Architecture Diagram	A-1
Description of Components	A-1
Record Store Server (RSS)	A-1
Control Index Server (CIS)	A-2
Sequence Diagrams	A-3
Non-SIPREC Call	A-3
ISR Call Setup Sequence Diagram	A-3
SIPREC Call	A-3

B ISR Linux Users and File Permissions

ISR Third-Party Platform File Permissions	B-3
---	-----

C ISR Dashboard Database Failover

Configuring ISR Dashboard Database High Availability	C-1
--	-----

D Logging Into ObserveIT Visual Session Recording

About This Guide

The Interactive Session Recorder (ISR) Administrator Guide provides information including:

- Overview of the ISR and getting started
- Managing and configuring the various components of the ISR Dashboard, including accounts, routes, users, sites, RSS servers, system configurations, accessing recordings, and building reports
- Software diagrams and call setup sequence
- ISR Linux Users and File Permissions
- ISR Dashboard Database Failover
- Accessing ObserveIT Visual Session Recording

Oracle Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Related Documentation

The following table describes the documentation set for this release.

Document Name	Document Description
ISR Release Notes	Contains information about new ISR features, fixes, and known issues.
ISR Installation Guide	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.
ISR User Guide	Contains information about using the ISR Dashboard for all levels of users. Provides information about viewing, playing, deleting recordings, running reports, and managing user profiles.

Document Name	Document Description
ISR Administrator Guide	Contains information about using the ISR Dashboard for the Administrator level user (Super User, Account Administrator, Tenant Administrator). Provides information about creating and managing accounts, routes, and users. Also provides information about configuring the ISR, running reports, viewing active calls, and securing the ISR deployment.
ISR API Reference Guide	Contains information about ISR FACE, VoiceXML Commands, legacy application programming interfaces (APIs), Recording File Types/Formats Supported, Return Codes, sendIPCRCommand.jsp Subdialog, Advanced Options, and Troubleshooting.
ISR Monitoring Guide	Contains information about installing and configuring the ISR Monitor, the Monitor database schema, and the Monitor MIB.
ISR Security Guide	Contains information about security considerations and best practices from a network and application security perspective for the ISR product.

Revision History

Date	Description
September 2018	<ul style="list-style-type: none"> Initial release of ISR 6.2 software.
July 2020	<ul style="list-style-type: none"> Updates "Downloading a Recording List to a CSV File" for clarity regarding custom data fields. Updates the screenshot in "Displaying DTMF Data in Segment Details".
November 2020	<ul style="list-style-type: none"> Updates "Logging In/Out of the ISR Dashboard" and "Importing a User Profile CSV File" with a note regarding username case-sensitivity. Updates the "Managing an RSS Location", "Adding a Location" topic with the Access type, SFTP Port option. Updates the following topics for clarity: <ul style="list-style-type: none"> Advanced Search for Recordings Showing User Activity Archival Troubleshooting Archival
January 2021	<ul style="list-style-type: none"> Includes note in the following sections regarding CSV file values: <ul style="list-style-type: none"> Importing an Account CSV File Importing a User Profile CSV File Importing a Route CSV file Updates "Configuring/Editing Details for an Account", "Archival" to include the SFTP Port option.

1

Overview

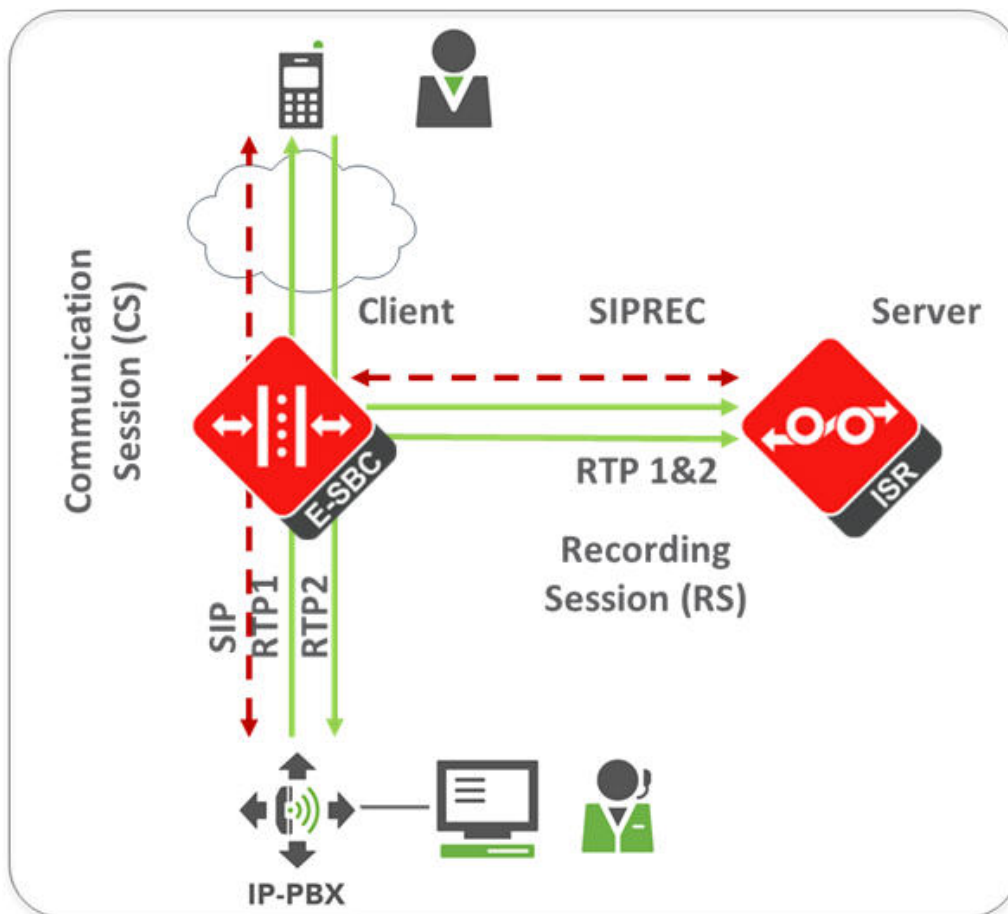
This chapter provides an overview of the ISR. It also provides information about using the ISR Dashboard to access and configure the ISR, and includes requirements and recommendations.

About the ISR

Driven by a profusion of government and industry regulations, enterprises are required to record and store an increasing quantity of communications sessions in order to maintain compliance. Conventional call recording solutions, designed for capturing contact center agent exchanges for training or quality assurance purposes, are not well suited to compliance recording applications. They are difficult to integrate with business applications, offer limited scalability, and can be costly to deploy.

The Oracle Communications Interactive Session Recorder (ISR) is specifically designed to eliminate enterprise compliance recording cost and complexity. The solution features an open, standards-based architecture that dramatically simplifies the capture and storage of real-time IP communications sessions throughout the enterprise. Ideal for a wide range of compliance applications, ISR leverages a modular design for superior scalability and economics, offers an extensive API set for ultimate extensibility and flexibility, and includes integrated support for screen recording using an industry leading user monitoring solution.

The ISR leverages SIPREC and a modular architecture for ease of deployment and scale. SIPREC uses a client/server architecture, where the SIPREC client (the Oracle Enterprise Session Border Controller in the image below) initiates SIPREC sessions with the SIPREC server (the Oracle ISR).



For an introduction to SIPREC and its configuration on the Oracle Session Border Controller, see the "Selective Call Recording/SIPREC" appendix in this guide or .

Session Recording Client Support

The ISR has been tested with the following SIPREC Session Recording Platforms:

- Oracle communications Session Border Controller
- Oracle Enterprise Session Border Controller
- Broadworks Application Server R21

SelectiveCall Recording SIPREC

The SIPREC protocol is the protocol used to interact between a Session Recording Client (SRC) (the role performed by SBC) and a Session Recording Server (SRS) (a 3rd party call recorder or Oracle Communications Interactive Session Recorder'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 a recording server, more robust failovers, and the ability to selectively record. SIPREC also isolates the RSS from the communication session.

The SRC starts a recording session for every call within a configured realm. All call filtering, if desired, must be accomplished by the recording server. The recording server performs the filtering and selection of which sessions it should record.

SIPREC for Active Recording

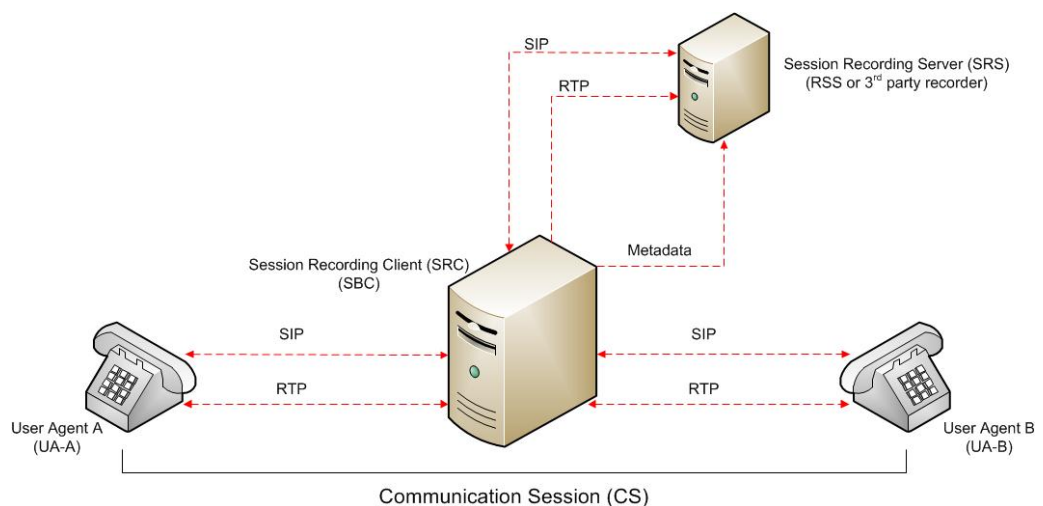
SIPREC supports active recording, where the SBC acting as the SRC, purposefully streams media to the Oracle Communications Interactive Session Recorder's RSS (or 3rd party call recorder) acting as the SRS. The SRC and SRS act as SIP User Agents (UAs). The SRC provides additional information to the SRS to describe the communication sessions, participants and media streams for the recording session to facilitate archival and retrieval of the recorded information.

The SBC acting as the SRC, is the source for the recorded media. The SBC consumes configuration information describing the ecosystem within which it operates. The interface, realm and session agent configuration objects specify the SIPREC configuration. A SIP UA can elect to allow or disallow any network element from recording its media.

During the establishment of a SIP Session, the SBC determines if SIPREC is configured for recording the call. If so, it then duplicates the media prior to initiating the session with the SRS. (Media replication is set up prior to the recording session). The SRS may choose to record, not record, or cancel the recording session, and then communicates via SIP signaling to the SBC. If the call is not to be recorded, the SRS signals termination of the recording session.

The SBC maintains SIPREC metadata information associated with recording sessions. 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 SBC. The SRS is responsible for maintaining call history, etc. The SBC creates and logs call detail records (CDRs) in the current manner, the 3rd party SRS vendor may collate this information if desired.

The following illustration shows two endpoints, User Agent A (UA-A) and User Agent B (UA-B). Their session is being recorded by an SRC (the SBC) and an SRS.



Preserve SIPREC with SIP REFER Header

When the SBC generates a new INVITE as part of terminating a SIP REFER, the SBC evaluates the SIPREC configuration of the realms and session agents involved in the new call leg and responds accordingly. The REFER and Transfer mechanism automatically preserves the UCID, XUCID, GUID, GUCID, and UUI in the metadata, and can forward this information to the Session Recording Server. The SBC can Start, Stop, Pause, and Resume SIPREC sessions in response to any re-INVITE, UPDATE, new INVITE, REFER, or specified SIP Response Message.

The SBC can establish a new session or update the existing session with the SIPREC server in the following ways.

- When the A-B call leg SA-realm-sipinterface is configured for SIPREC, and the B-C call leg SA-realm-sipinterface is not configured for SIPREC, the SBC sends metadata to the Session Recording Server to stop the recording on the sessionID associated with the original call.
- When both the A-B call leg and the B-C call leg have the same SIPREC configuration on their SA-realm-sipinterface, the SBC sends metadata to the Session Recording Server to stop Party A participation and start Party C participation within the same sessionID.
- When the A-B and B-C call legs have a different SIPREC configurations on their SA-realm-sipinterface, the SBC sends metadata to the A-B call leg Session Recording Server to stop the current recording session and sends metadata to the B-C call leg Session Recording Server to start a new recording session with a new sessionID.

Configuring SIPREC

For more information on configuring SIPREC on an SBC, see the *Oracle Communications Session Border Controller Call Monitoring Guide*.

ISR FACE

The ISR supports FACE. FACE is a feature for the aggregation and control of events. It is a centralized component used to control both ISR and integrated third-party services. It can also retrieve audio, video, and detailed metadata for recordings stored in the ISR. The initial third-party integration is with the ObserveIT Visual Session Recording solution. This provides the key activities necessary for desktop screen capture and for associating the captured screens to related audio recordings.

The controls currently available include full recording control (start, stop, split, pause, and resume, where split stops recording the current segment and starts recording a new segment, and where pause and resume can aid in the omission of sensitive information from the recording), retrieval of recorded files and metadata, as well as starting and stopping screen capture on an ObserveIT agent host. FACE also supports a policy system allowing incoming events to trigger actions, with the current set of actions dedicated to screen capture control.

The ISR FACE contains the following components:

- FACE Policy System—Handles automatic actions for specific ISR events.

- External Event Notification Listener—Receives events from ISR components and passes them to Policy System.
- FACE REST API—API for communication and control of ISR components.

For more information on ISR FACE, see the *API Reference 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

The ISR Dashboard has been tested on the following browsers:

- Google Chrome™ 60.0.3112.113
- Firefox 52.3.0
- Microsoft Edge 11.0.9600.18762CO

ISR recording playback errors have been reported for the following web browsers:

- Firefox—For the (historically) most popular transmission codec, g711, Firefox is not supporting playback of the 8-bit/8 kHz audio format set in the **"Default" Recording Format Profile**. The playback controls may appear only briefly before becoming unavailable. To address this issue, changes any routes configured to use the **"Default" Recording Format Profile** to the **"Firefox Supported" Recording Format Profile**, where the g711 transmission codec is converted to the PCM 16-bit/16 kHz recording format.

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

2

Getting Started

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

Prior to logging into the ISR Dashboard for the first time, you must enter a valid email and password. However, if your email and password are not available, you may use the following default email and password, then change the email address and 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 *Managing Users*.

 **Note:**

At the time a user is created, the ISR saves their email address and no one else can create a user with the same email address, regardless of whether it is uppercase or lowercase.

To login to the ISR Dashboard:

- Password must be at least 8 characters long.
- Password must contain at least one number (0-9) and one letter (A-Z and/or a-z).
- Password must contain at least one letter and one special character (for example, @, #, \$).

 **Note:**

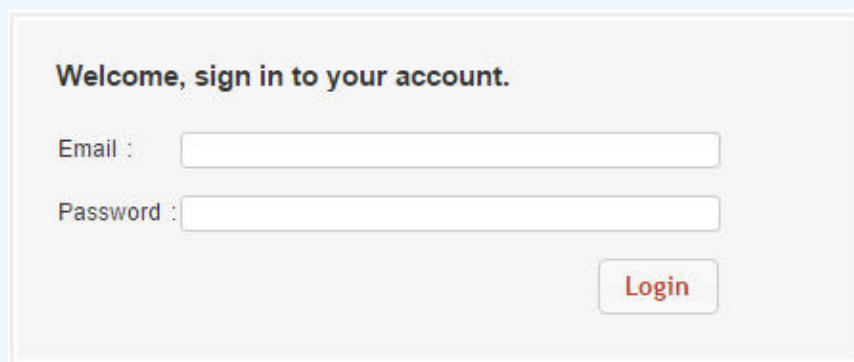
Your password must meet the following requirements:

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.



>Welcome, sign in to your account.

Email :

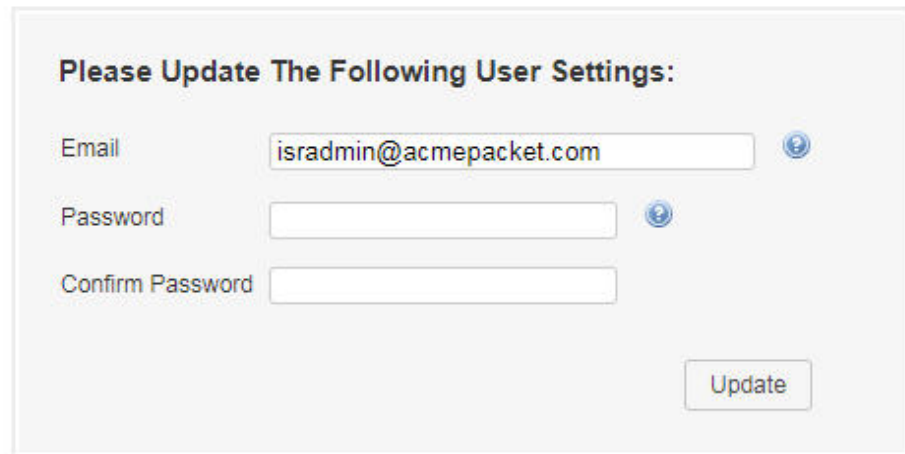
Password :

Login

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 with default user and password, the system prompts you to reset the email address and password.



Please Update The Following User Settings:

Email ⓘ

Password ⓘ

Confirm Password

For security purposes, you should change your password every 45 days.

 **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.


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:

Icon	Description
	<p>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.</p> <p>Note: Displayed recordings are dependent on the level of logged in user. For more information about user levels, see User Access Levels.</p> <p>For more information about Recordings, see Manage Recordings.</p>
	<p>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.</p> <p>Note: For more information about Reports, see Manage Reports.</p>
	<p>Edit My Settings (or Settings in the main menu) — Allows you to view and edit the ISR Dashboard settings such as:</p> <ul style="list-style-type: none">Preferred Time Zone LocaleList refresh rate (seconds)Displayed number of recording entries per pageSpecify the fields (columns) to display in a Recording searchChange your user login password <p>Note: For more information about Dashboard settings, see Editing My Settings.</p>

Icon	Description
	<p>Edit System Configurations (or Admin in the main menu) (displays for a Super User, Account Administrator, and Tenant Administrator only) — Allows you to perform the following Administrator tasks, including:</p> <ul style="list-style-type: none"> • Accounts • Realms • Routes • Users • Authorization Services • Custom Data Fields • External Event Destinations • Locales • Recording Format Profiles • Security Settings • Template Definitions • Thirdparty Services • Live Sessions • Sites (includes Recorders, Locations, Archival) <p>Note: Display of this feature is dependent on the level of logged in user. For more information about user levels, see User Access Levels.</p> <p>For more information about Administrator features, see Managing Realms/Accounts, Managing Routes, Managing Users, Managing Sites, Managing Authorization Services, and Viewing Live Sessions.</p>

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 dependent 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.

User Type	Find Recordings (Recordings)	Build Reports (Reports)	Edit My Settings (Settings)	Edit System Configurations (Admin)
Super User	Yes	Yes	Yes	Yes (Can manage all)
Account Administrator	View only.	Yes	Yes	Yes (Can manage all EXCEPT Super User and sites)

User Type	Find Recordings (Recordings)	Build Reports (Reports)	Edit My Settings (Settings)	Edit System Configurations (Admin)
Tenant Administrator	View and delete own recordings only. (Permissions to edit must be assigned.)	Yes (Reports include info from own accounts only)	Yes	Yes (Can manage own Accounts, Routes, Tenant Admin, Tenant User only)
Tenant User	View and delete own recordings only. (Permissions to edit must be assigned.)	Yes (Reports include info from own accounts only)	Yes	No
API User	N/A	N/A	N/A	N/A

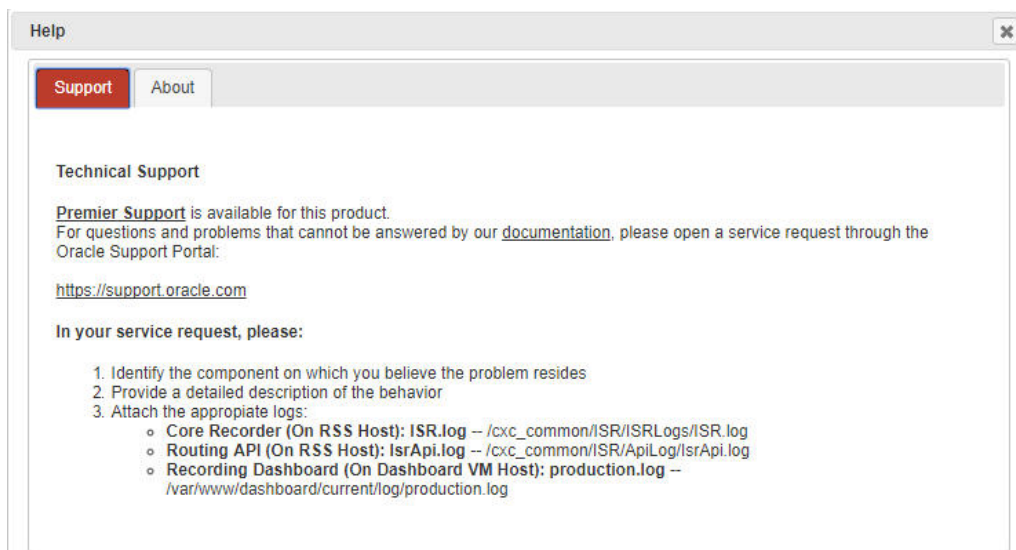
API users are currently specific to the ISR FACE REST API only and cannot log into the ISR Dashboard.

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

Help Link

Online support is available for the ISR Dashboard by clicking on the Help link (the question mark symbol '?') in the upper right corner of any page in the Dashboard.

The Help window has two tabs, Support, which provides the Oracle Support Portal's website, as well as all of the information to include in a service request. The About tab provides the ISR software version and build numbers you are running.



Note:

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

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

The screenshot shows the 'Edit My Settings' page with the following settings:

- Dashboard Settings**
- Preferred Language: en
- Preferred Time Zone: Eastern Time (US & Canada)
- List Refresh Rate (Seconds): None
- List Entries Per Page: 20

Using the Dashboard Settings, you can:

- Set your preferred language
- Set your preferred time zone locale
- Set the number of seconds that the pages in the dashboard are refreshed
- Set the number of entries you want displayed per page

To configure the Dashboard settings:

1. **Preferred Language**—Select the language you prefer.
2. **Preferred Time Zone Locale**—Select the time zone locale associated with your location or location of the user. The following table provides the valid values for this field.

Abu Dhabi	Copenhagen	London	Sapporo
Adelaide	Darwin	Madrid	Sarajevo
Alaska	Dhaka	Magadan	Saskatchewan
Almaty	Dublin	Marshall Is.	Seoul
American Samoa	Eastern Time (US & Canada)	Mazatlan	Singapore
Amsterdam	Edinburgh	Melbourne	Skopje
Arizona	Ekaterinburg	Mexico City	Sofia
Astana	Fiji	Mid-Atlantic	Solomon Is.
Athens	Georgetown	Midway Island	Srednekolymsk

Atlantic Time (Canada)	Greenland	Minsk	Sri Jayawardenepura
Auckland	Guadalajara	Monrovia	St. Petersburg
Azores	Guan Hanoi	Monterrey	Stockholm
Baghdad	Harare	Montevideo	Sydney
Baku	Hawaii	Moscow	Taipei
Bangkok	Helsinki	Mountain Time (US & Canada)	Tallinn
Beijing	Hobart	Mumbai	Tashkent
Belgrade	Hong Kong	Muscat	Tbilisi
Berlin	Indiana (East)	Nairobi	Tehran
Bern	International Date Line West	New Caledonia	Tijuana
Bogota	Irkutsk	New Delhi	Tokelau Is.
Brasilia	Islamabad	Newfoundland	Tokyo
Bratislava	Istanbul	Novosibirsk	UTC
Brisbane	Jakarta	Nuku'alofa	Ulaanbaatar
Brussels	Jerusalem	Osaka	Urumqi
Bucharest	Kabul	Pacific Time (US & Canada)	Vienna
Budapest	Kaliningrad	Paris	Vilnius
Buenos Aires	Kamchatka	Perth	Vladivosotok
Cairo	Karachi	Port Moresby	Volgograd
Canberra	Kathmandu	Prague	Warsaw
Cape Verde Is.	Kolkata	Pretoria	Wellington
Caracas	Krasnoyarsk	Quito	West Central Africa
Casablanca	Kuala Lumpur	Rangoon	Yakutsk
Central America	Kuwait	Riga	Yerevan
Central Time (US & Canada)	Kyiv	Rihadh	Zagreb
Chatham Is.	La Paz	Rome	Zurich
Chennai	Lima	Samara	N/A
Chihuahua	Lisbon	Samoa	N/A
Chongqing	Ljubljana	Santiago	N/A

- List Refresh Rate Seconds**—Select the number of seconds that the dashboard waits before refreshing the recordings list. Valid values are:
 - None (default)
 - 30 seconds
 - 1 minute
 - 2 minutes
 - 5 minutes
- List 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 100. Default is 20.

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 “Displaying” column. After clicking **Update**, 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.

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.

Heading	Description
Time (default)	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).
From (default)	The number that the caller dialed from (i.e., Caller ID).
To (default)	Displays the number that the caller dialed.
Duration (default)	Displays the length of the recording (in seconds)
Session ID	Displays the Session ID derived from the X-ISR-UCID.
RSS Egress Call ID	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).
RSS Ingress Call ID (default)	Displays the unique ingress call ID derived from the call-id received in the initial SIP INVITE.
Custom Data Fields	Displays a Custom Data field name as a Recordings list heading, and a valid Custom Data field value displays in that column for each recording.

2. Click **Update** to save the recordings list settings.

The headings listed in the Displaying column (green boxes) display as column headings on the Recordings List page.

RSS View Settings

Using the RSS View Settings, you can set the maximum entries to include from the RSS error logs.

To configure the RSS view settings:

1. **Max Error Log Entries**—Enter the number of entries to show on each RSS error log page. Valid values are 1-255. Default is 20.

2. Click **Save** to save the RSS view settings.

Change Password

Use the Change Password tab to change your current ISR login password to a new password.

To change your password:

1. **Current Password**—Enter the current password you use to log into the Dashboard.
2. **Password**—Enter your new password for logging into the Dashboard. Your password must meet the following requirements:
 - Password must be at least 8 characters long.
 - Password must contain at least one number (0-9) and one letter (A-Z and/or a-z).
 - Password must contain at least one letter and one special character (for example, @, ##, \$).
3. **Confirm Password**—Reenter your new password to confirm the new Dashboard password.
4. Click **Update** to save your new password.

 **Note:**

Default security settings require a new password not be the same as one used in the previous four attempts. If you attempt to enter a new password that was previously used, an error message appears.








Dashboard Tools



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

- Functional Icons
- Paging Tool
- Search Tools
- Column Sorting Tool
- Download Tool
- Import Link

Functional Icons

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

Functional Icon	Description
	Logout - Allows you to logout of the ISR Dashboard.
	Help - Displays information about contacting Technical Support for help with the ISR Dashboard.
	Add - Adds a new item to a list
	Delete - Removes an item from the list.
	<p>Play - Immediately opens and plays a .wav file recording stored in the ISR.</p> <p>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).</p>
	<p>Download - 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.</p>
	<p>Details - Displays additional details about the item in the list. Some items allow for additional editing after clicking this tool.</p>

Functional Icon	Description
	View User Audit Trail (managing User feature) - Displays details about the actions of the User in the ISR Dashboard. Information includes: <ul style="list-style-type: none"> • Time - Time of the action. • Action - Description of the action. • Object - The object that the action was performed on. • IP Address - IP address of the user who initiated the action.
	Events (managing Session Agent feature) - Displays specific events that occurred on a Session Agent within a Site.

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 **Settings, List 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 perform a basic search for a specific recording. A basic search uses an exact match on a single common search field.

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 displays.

RSS Ingress Call ID	Time	From	To	Duration	CustomDataField1
1-25460@10.10.248.209	2018-08-28 05:50:45 pm	sipp_sd_siprec	rss_sd_siprec	2 minutes 0 seconds	CustomDataValue1
1-25425@10.10.248.209	2018-08-28 05:38:04 pm	sipp_sd_siprec	rss_sd_siprec	1 minute 59 seconds	
1-25415@10.10.248.209	2018-08-28 05:34:31 pm	sipp_sd_siprec	rss_sd_siprec	2 minutes 0 seconds	
1-25256@10.10.248.209	2018-08-28 04:30:15 pm	sipp_g711_ulaw	rss_g711_ulaw	5 seconds	CustomDataValue2
1-25252@10.10.248.209	2018-08-28 04:29:49 pm	sipp_g711_ulaw	rss_g711_ulaw	3 seconds	

- 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
- In the text box, enter the information required dependent on the selection you made in Step 2.

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.

- 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. Advanced searches allow more search options, including multiple search fields and partial matching.

To perform an advanced search for a recording:

- On the Recordings page, click **advanced search**.

The following dialog box displays.

Advanced Search ✕

Search Mode

Partial Match

Session ID

From

To

Label

Search Date **By Relative** **By Range**

[▶ More Recording Search Options](#)

[▶ By Segment Search Options](#)

[▶ By Custom Data Search Options](#)

[▶ By Session Search Options](#)

- 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 Search Date as "Today", then the results of the search show all recordings with a start date matching the current date, AND a value of "123" in the From field, AND file name of "Recording1".
 - **OR**—Returns results where recordings match ANY of the fields you specify. For example, if you specify From as "123", File Name as "Recording1", and Search Date as "Last 7 Days", then the results of the search show any recordings with a value of "123" in the From field, OR a file name of "Recording1", a start date within the last seven days (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**—The unique Session ID derived from the X-ISR-UCID on which to perform the search.
- 5. From**—The From SIP URI to perform the search on.
- 6. To**—The To SIP URI to perform the search on.

7. **Label**—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 search for recordings that happened "**Today**" (default), within the **Last 7 Days**, or within the **Last 30 Days**.

By Range—Allows you to perform a recording search, based on the date range you specify.

 **Note:**

Search Date is always included in the advanced search terms. Therefore, when using Search Mode "OR" with a large date range, many recordings may be returned.

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 Date** and **To Date** boxes, select the time in the format HH:MM for which you want to search for recordings. The time displayed shows the time zone set by the logged in user. By default, the **From Date** is always behind the **To Date** time by 4 hours.

In the "**From Date** and **To Date** boxes, select the time in the format HH:MM for which you want to search for recordings.

 **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.

More Recording Search Options

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.

▼ More Recording Search Options

File Name	<input type="text"/>
Duration	Min <input type="text"/> s Max <input type="text"/> s
Agent ID	<input type="text"/>
RSS Ingress Call ID	<input type="text"/>
RSS Egress Call ID	<input type="text"/>
Categories	<input type="text"/>

- Duration Min**—The minimum duration, in seconds, of a recording. Valid values are numeric characters. For example, 15.
- Duration Max**—The maximum duration, in seconds, of a recording. Valid values are numeric characters. For example 24.
Using the examples in Steps 3 and 4, the results would include all recordings that had a recording duration between and including 15 and 24 seconds.
- Agent ID**—The ID of the agent that answered the call. This is the value set in the Dashboard or API.
- RSS Ingress Call ID**—The ingress call ID derived from the call-id received in the initial SIP INVITE.
- RSS Egress Call ID**—The egress call ID derived from the call-id used in the egress call leg for the recording, if using pass-thru mode.
- Categories**—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. For more information about creating and searching categories, see Recording Details.
- Click **Search** to find all recordings based on the search criteria. All matching recordings display in the recordings list.

Recording Search by Segment

You can search for recordings by segment.

To search for recordings based on segment:

- In the Advanced Search dialog box, click **By Segment Search Options** to expand the dialog box.
- Media Type**—Select the recorded file type, either Audio or Video.
- File Name**—Enter the segment file name, for example, 1-9599@10.1.2.3.4.seg0.wav.

Recording Search by Custom Data

You can search for recordings by custom data values.

To search for recordings based on custom data values:

1. In the Advanced Search dialog box, click **By Custom Data Search Options** to

The screenshot shows a portion of the Advanced Search dialog box. At the top, there is a tab labeled 'More Recording Search Options'. Below it, a dropdown menu is expanded to show 'By Custom Data Search Options'. Under this dropdown, there are two input fields: 'CustomDataFieldName1' and 'CustomDataFieldName2'. Below these fields is a horizontal scrollbar. At the bottom of the dialog box, there is a 'Search' button.

expand the dialog box.

2. The currently configured Custom Data Field names are listed. Enter the value(s) for which you want to search next to the corresponding Custom Data Field name(s).
3. Click **Search** to find all recordings based on the specified custom data. All matching recordings display in the recordings list.

Note:

Custom Data search parameters are applied in addition to any other search options defined, including date ranges.

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.

Advanced Search
✕

▼ By Session Search Options

SIPREC Session ID	<input type="text"/>
Participant AOR	<input type="text"/>
apkt:ucid	<input type="text"/>
extTrackingID	<input type="text"/>
serviceProviderID	<input type="text"/>
userID	<input type="text"/>
groupID	<input type="text"/>
callID	<input type="text"/>
callingPartyNumber	<input type="text"/>
calledPartyNumber	<input type="text"/>
newExtTrackingID	<input type="text"/>
apkt:realm	<input type="text"/>
apkt:P-Asserted-Identity	<input type="text"/>
apkt:Diversion	<input type="text"/>
apkt:request-uri	<input type="text"/>

2. **SIPREC Session ID**—The SIP recording session ID number for which you want to search.

 **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**—The participant's address of record (AOR) associated with the call that was recorded.
4. **apkt:ucid**—The Universal Call ID (UCID) of the incoming caller.
5. **extTrackingID**—The external tracking ID that was used when an incoming call was transferred to another recipient.
6. **ServiceProviderID**—The Service Provider ID that was used on the incoming call.
7. **userID**—The user ID on the incoming call.
8. **groupID**—The group ID on the incoming call.
9. **callID**—The call ID of the incoming call.
10. **callingPartyNumber**—The source number of the incoming call.
11. **calledPartyNumber**—The destination number of the incoming call.
12. **newExtTrackingID**—The new external tracking ID that was used when an incoming call was transferred a second time to another recipient.

 **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**—The name of the ISR realm that received the SIPREC session (in-realm).
14. **apkt:P-Asserted-Identity**—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.
15. **apkt:Diversion**—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.
16. **apkt:request-uri**—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.
17. Click **Search** to perform the search based on the recording session parameters you specified. All matching recordings display in the recordings list.

 **Note:**

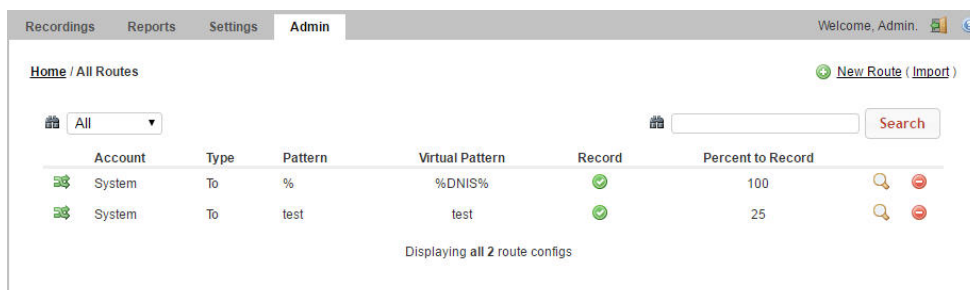
Session search parameters are applied in addition to any other search options defined, including date ranges.



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 **Routes**. A list of routes display in the routes list.



Account	Type	Pattern	Virtual Pattern	Record	Percent to Record
System	To	%	%DNIS%		100
System	To	test	test		25

Displaying all 2 route configs

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 by clicking on the row to bring up the Recording Details page. Click the segment(s) (for example, the Segment 1 tab) and click the Download icon for that recording.

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.

 **Note:**

The names of these options may vary between browsers.

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 recorded files).

 **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, including those columns, not listed in the current recording list. Custom data fields will appear as one column with key and value pair in the form of array (for example, [{"recordcount"=>"23"}, {"Custom"=>"custom1"}]).

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

 **Note:**

The names of these options may vary between browsers.

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

Example CSV file with recordings and no detail specified

	A	B	C	D	E
1	RSS Ingress Call ID	Time	From	To	Duration
2	24-1841@172.30.58.237	11/17/2016 12:27	sipp_g711	rss_g711	10
3	23-1841@172.30.58.237	11/17/2016 12:27	sipp_g711	rss_g711	10
4	22-1841@172.30.58.237	11/17/2016 12:27	sipp_g711	rss_g711	10
5	21-1841@172.30.58.237	11/17/2016 12:26	sipp_g711	rss_g711	10
6	20-1841@172.30.58.237	11/17/2016 12:26	sipp_g711	rss_g711	10
7	19-1841@172.30.58.237	11/17/2016 12:26	sipp_g711	rss_g711	10
8	18-1841@172.30.58.237	11/17/2016 12:26	sipp_g711	rss_g711	10
9	17-1841@172.30.58.237	11/17/2016 12:26	sipp_g711	rss_g711	10
10	16-1841@172.30.58.237	11/17/2016 12:26	sipp_g711	rss_g711	10
11	15-1841@172.30.58.237	11/17/2016 12:25	sipp_g711	rss_g711	10
12	14-1841@172.30.58.237	11/17/2016 12:25	sipp_g711	rss_g711	10
13	13-1841@172.30.58.237	11/17/2016 12:25	sipp_g711	rss_g711	10
14	12-1841@172.30.58.237	11/17/2016 12:25	sipp_g711	rss_g711	10
15	11-1841@172.30.58.237	11/17/2016 12:25	sipp_g711	rss_g711	10

Example CSV file with recordings and detail specified

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	From	To	Session ID	Rating	RSS Ingress Call ID	RSS Egress Notes	Hours	From	File Name	Duration	OTMP Events	Custom Data	Session Extension Data	
2	rs_g711	11/17/2016 12:27	x-isr-ucid-24-1841@172.30.58.237	0	24-1841@172.30.58.237			0	sipp_g711	10.207		[{"envy_offset_mn":3000,"origin_source":"d","dmf_dig":{"examplefield1":"w11","examplefield2":"w12"},"snpk_ucid":"50FAD800300054010C20","encoding":"hex"}]		
3	rs_g711	11/17/2016 12:27	x-isr-ucid-23-1841@172.30.58.237	0	23-1841@172.30.58.237			0	sipp_g711	10.207		[{"envy_offset_mn":3000,"origin_source":"d","dmf_dig":{"examplefield1":"w11","examplefield2":"w12"},"snpk_ucid":"50FAD800300054010C20","encoding":"hex"}]		
4	rs_g711	11/17/2016 12:26	x-isr-ucid-22-1841@172.30.58.237	0	22-1841@172.30.58.237			0	sipp_g711	10.207				
5	rs_g711	11/17/2016 12:26	x-isr-ucid-21-1841@172.30.58.237	0	21-1841@172.30.58.237			0	sipp_g711	10.207				
6	rs_g711	11/17/2016 12:26	x-isr-ucid-20-1841@172.30.58.237	0	20-1841@172.30.58.237			0	sipp_g711	10.207				
7	rs_g711	11/17/2016 12:26	x-isr-ucid-19-1841@172.30.58.237	0	19-1841@172.30.58.237			0	sipp_g711	10.207				
8	rs_g711	11/17/2016 12:26	x-isr-ucid-18-1841@172.30.58.237	0	18-1841@172.30.58.237			0	sipp_g711	10.207				
9	rs_g711	11/17/2016 12:26	x-isr-ucid-17-1841@172.30.58.237	0	17-1841@172.30.58.237			0	sipp_g711	10.207				
10	rs_g711	11/17/2016 12:26	x-isr-ucid-16-1841@172.30.58.237	0	16-1841@172.30.58.237			0	sipp_g711	10.207				
11	rs_g711	11/17/2016 12:25	x-isr-ucid-15-1841@172.30.58.237	0	15-1841@172.30.58.237			0	sipp_g711	10.207				
12	rs_g711	11/17/2016 12:25	x-isr-ucid-14-1841@172.30.58.237	0	14-1841@172.30.58.237			0	sipp_g711	10.207				
13	rs_g711	11/17/2016 12:25	x-isr-ucid-13-1841@172.30.58.237	0	13-1841@172.30.58.237			0	sipp_g711	10.207				
14	rs_g711	11/17/2016 12:25	x-isr-ucid-12-1841@172.30.58.237	0	12-1841@172.30.58.237			0	sipp_g711	10.207				
15	rs_g711	11/17/2016 12:25	x-isr-ucid-11-1841@172.30.58.237	0	11-1841@172.30.58.237			0	sipp_g711	10.207				

The following table identifies some of the columns that can display in the CSV file.

Column Heading	Description
To	Specifies the To SIP URI. This is the URI for where the call is going.
Time	Specifies the starting GMT time and date of the recording in the format YYYY-MM-DD HH:MM:SS, respectively. Note: In the date format, M = month, D = day, and Y = year. In the time format, H = hours, M = minutes, S = seconds.
Session ID	Specifies the Session ID assigned to the incoming call. Format may be specified as x-isr-ucid-<session id>@<local host>.
Rating	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.
RSS Ingress Call ID	Specifies the call ID assigned by the RSS to the incoming call.
RSS Egress Call ID	Specifies the call ID assigned by the RSS to the outgoing leg of the call (pass-thru mode only).
Notes	Specific notes, if any, entered by users through the dashboard.
Hours	Specifies the length of time, in hours, a user spent reviewing, transcribing, and commenting on the recording.
From	Specifies the From SIP URI. This is the URI from where the call session was coming.
File Name	Specifies the name of the recording file.
Duration	Specifies the length of the recording (in seconds).
Custom Fields	Specifies a unique set of meta-data associated with the recording (i.e., Transaction ID, Account Number, Unique Call ID). For more information on Custom Fields, see "FACE Custom Data" in the <i>Oracle Communications Interactive Session Recorder API Guide</i> .
Completed	Specifies whether or not this recording resulted in a complete transaction, added by the dashboard user.

Column Heading	Description
Agent ID	Specifies the ID of the Agent answering the call.

Import Link

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's Import link (located in the top right corner of both the Accounts and Routes pages) . 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 link is for Super User and Account Administrators only.

Administrator Menu

The ISR Dashboard provides a menu that allows Administrators to manage accounts, realms, routes, users, authorization services, custom data fields, locales, recording format profiles, security settings, template definitions, thirdparty services, live sessions on the ISR, and sites.

The screenshot shows the Administrator Menu interface. At the top, there is a navigation bar with tabs for Recordings, Reports, Settings, and Admin (which is selected). To the right of the navigation bar, it says "Welcome, Admin." and includes links for Logout and Help. Below the navigation bar, the main content area is titled "What Would You Like To Manage?" and lists the following menu items, each with a small icon:

- Accounts
- Realms
- Routes
- Users
- Authorization Services
- Custom Data Fields
- External Event Destinations
- Locales
- Recording Format Profiles
- Security Settings
- Template Definitions
- Thirdparty Services
- Live Sessions
- Sites

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 permissions available for each of the ISR's administrator levels.

Admin Function	Account Administrator	Tenant Administrator
Accounts	Manage Accounts	Manage own Accounts only
Realms	Manage Realms	N/A
Routes	Manage Routes	Manage own Routes only
Users	Manage Users (Account Admin, Tenant Admin, and Tenant User only)	Manage Users (Tenant Admin and Tenant User only)
Authorization Services	Manage Authorization Services	N/A
Custom Data Fields	Manage Custom Data Fields and Names	N/A
External Event Destinations	Manage External Events and Notifications	N/A
Locales	Manage Localization	N/A
Recording Format Profiles	Manage Recording Format Profiles	N/A
Security Settings	Manage Security Settings	N/A
Template Definitions	Manage Template Definitions	N/A
Thirdparty Services	Manage Thirdparty Services	N/A
Live Sessions	Manage Live Sessions	N/A
Sites	Manage Sites	N/A

3

Managing Accounts

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

Managing Accounts

Use the **Accounts** link on Admin page 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.





Select **Accounts** from the Admin page to manage Accounts.

Accounts Page



Name	Description	Number of Routes	Recording is	Sessions Capacity
 System	System	1	Enabled	Unlimited

The following table describes the information displayed on the Accounts page.

Column	Description
Name	Name of the account.
Description	Description of the account.
Number of Routes	Number of routes configured for the account.
Recording is	Identifies whether or not recording is enabled or disabled on the account.  Recording is enabled.  Recording is disabled.
Sessions Capacity	Total number of available sessions currently allowed for this account.
	Displays details for the account and allows you to edit the details.
	Deletes the account.

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:

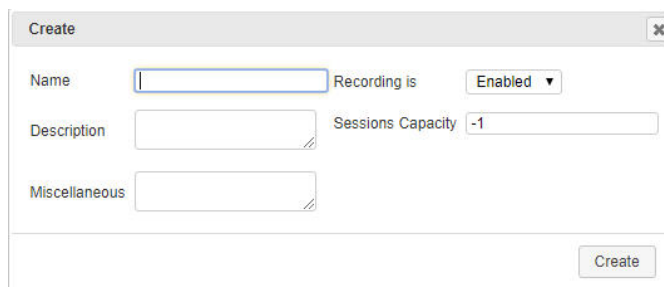
You can create an account using any application that can save to a comma separated value (CSV) file (i.e., Microsoft® Excel, Notepad®, etc.). Using the ISR Dashboard, you can then import the account information from the file (<filename>.csv) to the ISR database.

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

Only a Super User 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 **Accounts**. The Accounts page displays.
3. Click **Create**. The following dialog box displays.



4. **Name**—Enter an account name for this account.
5. **Description**—Enter a description for this account.
6. **Miscellaneous**—(optional) Enter any miscellaneous notes about the account.
7. **Recording is**—Select whether or not to enable recordings on this account. Valid values are:
 - Enabled (default)
 - Disabled
8. **Segmentation State**—Select whether or not to enable recording segmentation via FACE API requests or reINVITE.
9. **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)
 - 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.
10. Click **Create** to create the new account. The Edit Account page displays.

Configuring/ Editing Details for an Account

Super Users 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
- Configure or edit account recording file permissions
- Configure or edit account routes
- View or edit account users

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 **Accounts**. The Accounts page displays.

- Select an account from the list and click the Details icon. The following page displays.

The screenshot shows the Oracle Account Administration interface. At the top, there are navigation tabs: Recordings, Reports, Settings, and Admin (selected). The user is logged in as Admin, with options for Logout and Help. The main content area is titled 'Home / Accounts' and displays the configuration for an account named 'System'. The configuration includes:

- Name:** System
- Description:** System
- Miscellaneous:** System
- Recording is:** Enabled
- Segmentation State:** Enabled
- Sessions Capacity:** -1

An 'Update' button is located at the bottom right of the configuration area. Below the configuration, there is a list of expandable sections:

- Archival
- Dashboard Configurations
- Permissions
- Route Defaults
- Routes
- Users
- Video

- Account Name**—Edit the account name.
- Account Description**—Edit the description for this account.
- Account Miscellaneous**—(optional) Edit any miscellaneous notes about the account.
- Recording is**—Select whether or not to enable recordings on this account. Valid values are:
 - Enabled (default)
 - Disabled
- Segmentation State**—Select whether or not to enable recording segmentation via FACE API requests or reINVITES.
- 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)
 - 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 Managing Reports.

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

Archival

You may define an archival strategy for each account, using the Account page's **Archival** section.

To add an Account-specific Archival destination:

1. On the Admin page, click **Accounts**.
2. Select an account from the Accounts page and click the Details icon for that account.
3. Click **Archival** to expand the archival information.
4. Click **Enable Archival by Account**.



Note:

Archival by account is enabled only when there is a default archiver created.

5. In the **Access Type** field, select one of the following:
 - Local - Local disk
 - Mount - NFS Mount shared directory
 - SFTP - SFTP server
 - SFTP Port - Specify the port number. Valid values are 0 - 65535. The port must be enabled in the specified host.

Note:

"Local" access in Archival by Account is deprecated and Oracle recommends the "Mount" access type in this scenario.

6. In the **Remote Access URL** field, enter the URL in which the recordings are archived. Note that locations created automatically by the addition of a valid RSS configure the URL and serve recordings from it. If you add custom locations, you must configure them to be served by a web server and then set this URL if you want them to be playable via the Dashboard or APIs.
7. In the **Local Recordings Directory** field, specify the directory of the Account's Archival destination Location. When **Access Type** is set to SFTP, the Archiver attempts to move the Account's recordings to the SFTP user "home" path on the SFTP server.
8. The **Advanced Configurations - Checksum** field enables the MD5 Hash for Recordings feature.

For more information on configuring Archival by Account, see "Managing Sites".

 **Note:**

Archival for recordings on the enabled Accounts begins immediately after configuration. To avoid errors, confirm that the Local directory path, NFS share, or SFTP server is valid and accessible with your configuration. Note that for NFS shares, they must be mounted to each host that needs to access them, typically each RSS.

Configuring MD5 Checksum Validation

The ISR may use MD5 Hashing to validate files are moved in their entirety.

1. On the Admin page, click **Accounts**.
2. Select an account from the Accounts page and click the Details icon for that account.
3. Click **Archival** to expand the Archival configuration.
4. Select the Archival Location entry on which you are enabling checksum validation.
5. Click **Advanced Configurations**.
6. Set the **Checksum** field to MD5.
7. Click **Update**.

If a checksum violation occurs, the Recording Details page displays something similar to the following example:



The screenshot shows a red header bar with a dropdown menu labeled "File Location". Below the header, there are three sections:

- Store Indefinitely**: A checkbox that is currently unchecked.
- Archival Status**: Displays "Failed To Archive and Reached Max Number of Attempts (1)" with a "Reset" button.
- Archival Remarks**: Displays "Record failed archival attempt at Fri Jan 12 12:08:00 EST 2018 by archiver ID 2 process ID localhost.localdomainlocalhost.localdomain160eb57ad8c. Reason: Aborting the archive process due to checksum mismatch for recording".

8. Once MD5 Hashing is enabled, you may retrieve the checksum on new recordings. Using an authorized valid token, make a FACE details request. For example:

```
$ curl -k -X GET "https://<face_ip>:8443/Face/audioRecording/
details?token=<token>&filename=<file_name>"
```

The following is a truncated sample response:

```
<?xml version="1.0" encoding="UTF-16"?>

<result><code>0</code><message>ACK</message><recording>
...
<checksum>5941ee64142e6eb45dfaef23203cf54</checksum>
<checksumMismatch>>false</checksumMismatch>
<customDataSets/>
<siprecDataSets/>
<dtmfDigits/>
```

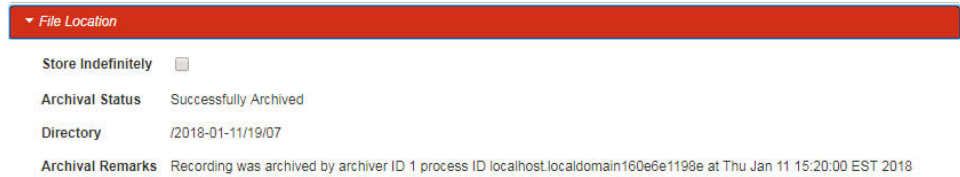
```
</recording>
</result>
```

Verifying Archival Success

To verify successful Archival for a specific recording.

1. Access the Recording Details page.
2. Click the **File Location** section.

The Archival Status and Archival Remarks fields provide information about the Archival of a specific recording.

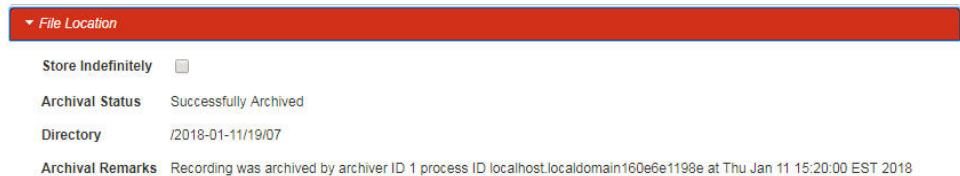


Site Archival Configuration with Account Archival Enabled

Recordings that do not belong to an Account with Account Archival configured may still need to be moved to another Location, converted for playback, or deleted after a certain amount of time. This is configured through the Sites Archival page.

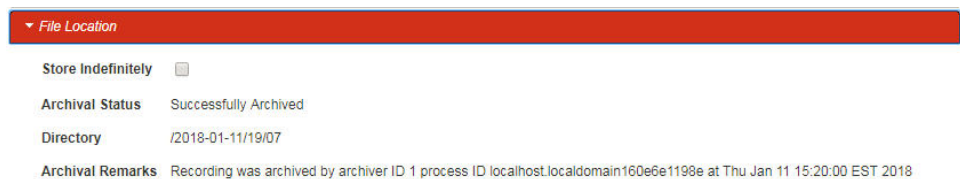
To edit Archival:

1. Select the "Source" Location in the "Update" form. This may be the RSS's "Primary" Location, or another Location specific to your environment.
2. Select the "Destination" Location, in the "Update" form. This could be the RSS's "Secondary" Location, or another Location specific to your environment.
3. Click **Update**.
4. Confirm a recording made on an Account not specifically configured for Archival.



Troubleshooting Archival

1. Access the Recording Details page.
2. Click the **File Location** section.



The **Archival Status** and **Archival Remark** comments provide information about the recording's Archival.

 **Note:**

Only converted and wav formatted recording files will be archived to the destination location if the location type is SFTP.

3. The Administrator may use the **Reset** button to resolve a problem in the architecture and attempt Archival again for the recording.

 **Note:**

Invalid permissions of the destination directory for the Archival process user or Archival SFTP client user are a common source of Archival failures. For example, invalid SFTP credentials yield an **Archival Remark** reason of "Archive is Aborting due to unable to establish SFTP Session for the Location".

Dashboard Configurations

You can customize the ISR Dashboard for each account if required, using the **Account Branding** feature. Via the Account page's Dashboard Configurations section, you can do the following:

- Customize the Dashboard's header and footer color
 - Specify a logo to display
 - Customize Admin and User Help
 - Set the maximum recordings in the list view and in a CSV download
- To apply branding to an account:
1. On the Admin page, click **Accounts**.
 2. Select an account from the Accounts page and click the Details icon for that account.
 3. Click **Dashboard Configurations** to expand the branding information.


Dashboard Configurations

Header and Footer Color	<input type="text" value="#f1392b"/>
Locale	<input type="button" value="en"/> ▾
Logo	<input type="text" value="oracle.png"/> <small>(can be a relative path within the images directory like customer/sample.png or a URL; max width is 250 pixels and max height is 150 pixels)</small>
Product Name	<input type="text" value="Interactive Session Recorder"/>
Admin Help	<div style="border: 1px solid #ccc; padding: 2px; min-height: 40px;"><pre><table cellpadding="0" cellspacing="0" border="0"> <tr> <td valign="top"> <p ><h4>Technical Support</h4></p> </td></tr> <tr><td>Premier Support is</pre></div>
User Help	<div style="border: 1px solid #ccc; padding: 2px; min-height: 40px;">For help, please contact your account administrator.</div>
Max Recording Entries in List View	<input type="text" value="10000"/>
Max Recording Entries in CSV Download	<input type="text" value="10000"/>

Branding Preview

LDAP Configurations

Enable LDAP?	<input type="button" value="No"/> ▾
Host	<input type="text"/>
Port	<input type="text" value="389"/>
TLS CA File Path	<input type="text"/>

4. In the **Header and 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. In the **Locale** field, select the language to use.
6. **Logo**—Enter the file name of the Company logo you want to apply to the header of all the screens in the ISR Dashboard. Enter the file URL of the Company logo. If required, you can store the file on the Dashboard host and set the path relative to the /var/www/dashboard/current/public/images directory. For example, images/Company.png.
7. In the **Product Name** field, enter the name of the product.
8. **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 text or HTML code. For example:

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

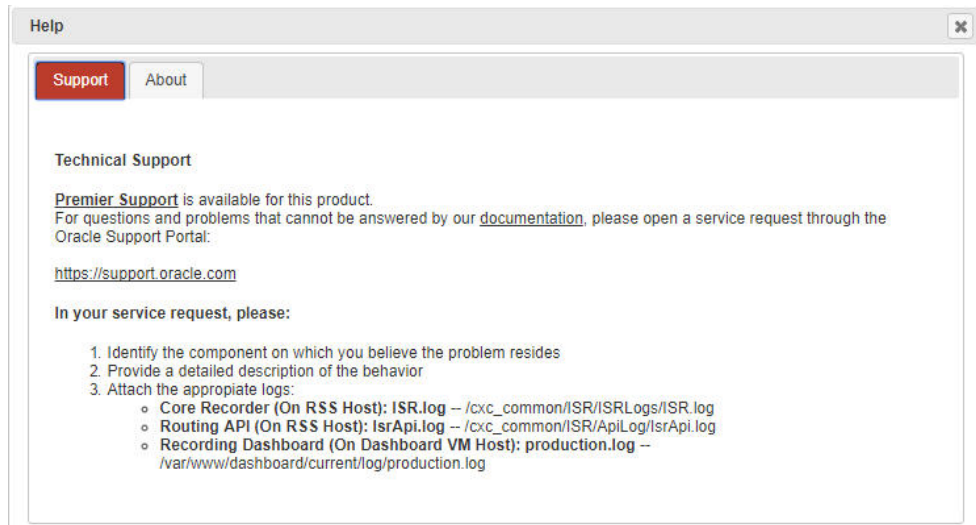
The default value for this field is:

```
<table cellpadding="0" cellspacing="0" border="0"> <tr>
<td valign="top"> <p ><h4>Technical Support</h4></p>
</td></tr> <tr><td><a href="https://support.oracle.com/"
TARGET="_blank"><b>Premier Support</b></a> is available for this
product.</td></tr> <tr><td>For questions and problems that
cannot be answered by our <a href="http://docs.oracle.com/cd/
E50378_01/index.htm" TARGET="_blank">documentation</a>, please open
a service request through the Oracle Support Portal: <br/>
<br/> <a href="https://support.oracle.com" TARGET="_blank">https://
support.oracle.com</a> <h4>In your service request, please:</h4>
<ol> <li>Identify the component on which you believe the
problem resides</li> <li>Provide a detailed description of the
behavior</li> <li>Attach the appropriate logs: <ul> <li><b>Core
Recorder (On RSS Host): ISR.log</b> -- /cxc_common/ISR/ISRLogs/
ISR.log</li> <li><b>Routing API (On RSS Host): IsrApi.log </b> -- /
```

```

cxc_common/ISR/ApiLog/IsrApi.log</li> <li><b>Recording Dashboard
(On Dashboard VM Host): production.log</b> -- /var/www/dashboard/
current/log/production.log</li> </ul> </li> </ol> </td> </tr> </
table>

```



 **Note:**

In the “Admin Help” and User Help fields, you can resize the text box as required by left-clicking and holding your mouse button on the bottom-right corner of the box, and dragging it to the size you require.

9. **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 text or HTML code. For example:

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

The default message in the ISR is:

```
For help, please contact your account administrator.
```

10. **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**.
11. **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**.
12. Click **Preview** to verify the color and logo changes before saving.
13. **LDAP Configurations**—To configure the ISR system for Dashboard logins using LDAP, click on the “System account and configure the following fields:
 - Host—Enter the host URL or IP
 - Port—Enter the port number of the LDAP server

- TLS CA File Path—Choose the TLS certificate file to use for secure LDAP requests
14. Click **Update** to save the changes. The color and logo you specify display on the screens in the ISR Dashboard.

Permissions

The Permissions section of the Edit Account page allows you to configure Account-level playback, deletion, and download recording file permissions through the ISR Dashboard.

Permissions

(Drag and Drop fields below; then Update to apply settings.)

Granted	Available
Play Recording Permission	
Download Recording Permission	
Delete Recording Permission	

Route Defaults

The Route Defaults section 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
- Record and Save Mode Defaults
- Sessions Capacity Defaults

Route Defaults

Recording Defaults

Route Mode: Standard (SIPREC) ▼

Recording is: Enabled ▼

Percent To Record: 100

Always Record As Raw RTP: No ▼

Recording Format Profile: Default

Record DTMF: No ▼

Record and Save Mode Defaults

Record and Save on DTMF: dtmf-pound # ▼

Sessions Capacity Defaults

Session Capacity: 24

Additional Burst Session Capacity: 6

Recording Editing Permissions

Allow Editing of Agent ID: No ▼

Allow Editing of Rating: No ▼

Allow Editing of Completed Transaction: No ▼

Allow Editing of Notes: No ▼

Route Defaults

The **Route Defaults** allow you to specify whether or not recording is enabled by default for the routes that are created 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 **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:
 - Standard (SIPREC)—ISR records as the Session Recording Server (SRS) in a SIPREC architecture.
 - 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.
5. **Recording is**—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.
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

 **Note:**

When a session is not recorded based on this value, the ISR replies to unrecorded INVITEs with a 412 response code, logs the rejected session, and adds the rejected session to the call statistics table.

When this value is set to **0**, the ISR remains connected and available for ad-hoc API recording for all sessions. When you set this value to 0 and update your ISR, the ISR Dashboard provides the following message:

```
Percent To Record has been set to 0%. Each session is accepted
and remains active for ad-hoc recording. To reject sessions due to
percentage-based recording, the value must be greater than 0%.
```

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**.
9. **Record DTMF**—Select whether routes for this account record DTMF digit presses by default. The default value is **Use System Account's Setting**.

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 *Managing Recordings*.

You specify whether or not routes created for the account allow users, by default, to 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 be able to indicate that a recording represents a complete transaction. 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 - Allows editing of notes specified for a recording.
 - No (default) - Prevent editing of notes specified for a recording.

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 **dtmf-disabled** 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-disabled

Sessions Capacity Defaults

The ISR allows you to set the maximum number of sessions available by default for routes created under 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 by default 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**—Enter the maximum number of sessions to assign by default to new routes for the account. Default is 24. Valid values are:
 - -1 to 999999999 (must indicate total number of licensed sessions)
 - -1 indicates no limit (default)
 - 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 Managing Reports.
2. **Additional Burst Session Capacity**—Enter the number of additional call recording sessions to assign by default to routes for the account. These are only used 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)
 - 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 Managing Reports.
3. Click **Update** to save the default route parameters. The Edit Account page displays.

Routes

The Routes section of the Edit Account page allows you to view and edit routes associated with this account.

Routes					
Type	Pattern	Virtual Pattern	Recording is	Percent To Record	
 To	%	%DNIS%		100	

Users

The Users section of the Edit Account page allows you to view and edit users associated with this account.

Account Users			
User Name	Email	Type	Active
 Admin	isradmin@acmepacket.com	Super User	

Video

You can enable or disable video recording for an Account.

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

Video	
Video Recording is	Disabled ▾
Video Access Permission	Enabled ▾

4. In the **Video recording is** field, enable or disable video recording. By default, video recording is disabled.
5. In the **Video Access Permissions** field, specify whether users are allowed to access video recordings. By default, users are enabled.
6. Click **Update**.

Deleting an Account

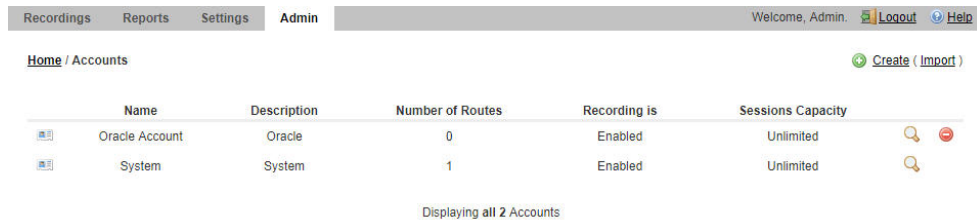
You can delete accounts in the ISR Dashboard as required.

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 **Accounts**.
2. Select an account from the Accounts page and click the Delete icon for that account.



Name	Description	Number of Routes	Recording is	Sessions Capacity
Oracle Account	Oracle	0	Enabled	Unlimited
System	System	1	Enabled	Unlimited

Displaying all 2 Accounts

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

Note:

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.

Note:

Ensure the values provided in the CSV file match the values in the table provided or the ISR will display an error message.

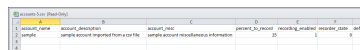
To import account information from a CSV file:

1. Using any application that can save to a CSV file, create a file that contains the parameters required for creating an account.
 - Boolean (yes/no) values must be entered using 0 (yes or enabled) and/or 1 (false or disabled).
 - The ISR does not ignore any leading and/or trailing spaces, so ensure your CSV file does not have any.

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

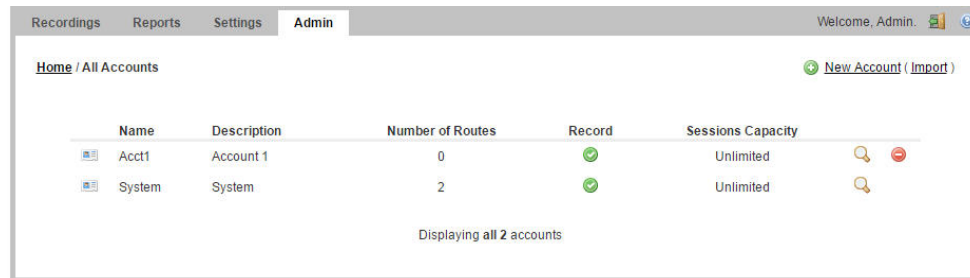
Parameter Heading	Valid Values
account_name	text
account_description	text
account_misc	text
percent_to_record	0 to 100
recording_enabled	0 1
recorder_state	0 1
default_recording_type	1 None: Account or System default (default) 2 WAVE Linear/8bit/8KHz stereo 3 WAVE Linear/16bit/8KHz stereo 4 WAVE Linear/8bit/8KHz mono 5 WAVE Linear/16bit/8KHz mono 6 WAVE uLaw 8bit/8KHz stereo 7 WAVE aLaw 8bit/8KHz stereo 8 WAVE uLaw 8bit/8KHz mono 9 WAVE aLaw 8bit/8KHz mono 10 Raw uLaw 8bit/8KHz mono 11 Raw aLaw 8bit/8KHz mono 12 Raw PCM 8bit/8KHz mono 13 WAVE ADPCM 4bit/8KHz mono 14 WAVE ADPCM 8bit/8KHz stereo
agent_id_editable_flag	0 1
rating_editable_flag	0 1
completed_editable_flag	0 1
notes_editable_flag	0 1
application	pass_through conference record_and_save call_parking vam_sip_test
maximum number of ports	digits (-1 for no limit)
number_of_burst_ports	digits (-1 for no limit)
acct_port_limit	digits

Example File with Parameters and Values



1	2	3	4	5	6	7	8
account_name	account_description	account_misc	percent_to_record	recording_enabled	recorder_state	default_recording_type	agent_id
sample	sample account description from a csv file	sample account miscellaneous information	25	1	0	1	8

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 **Accounts**. The Accounts page displays.



Name	Description	Number of Routes	Record	Sessions Capacity
Acct1	Account 1	0	✓	Unlimited
System	System	2	✓	Unlimited

6. Click **Import**.
7. **CSV File to Upload**—Click **Choose File** and navigate to the CSV file you are importing, select the file and click **Open** to populate the field.
8. Click **Upload** to upload the account CSV file to the ISR database.

 **Note:**

The new accounts are added to your Accounts page and display 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.

4

Managing Realms

This chapter provides information about adding, editing, and deleting realms from the ISR database.

Managing 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 an 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.

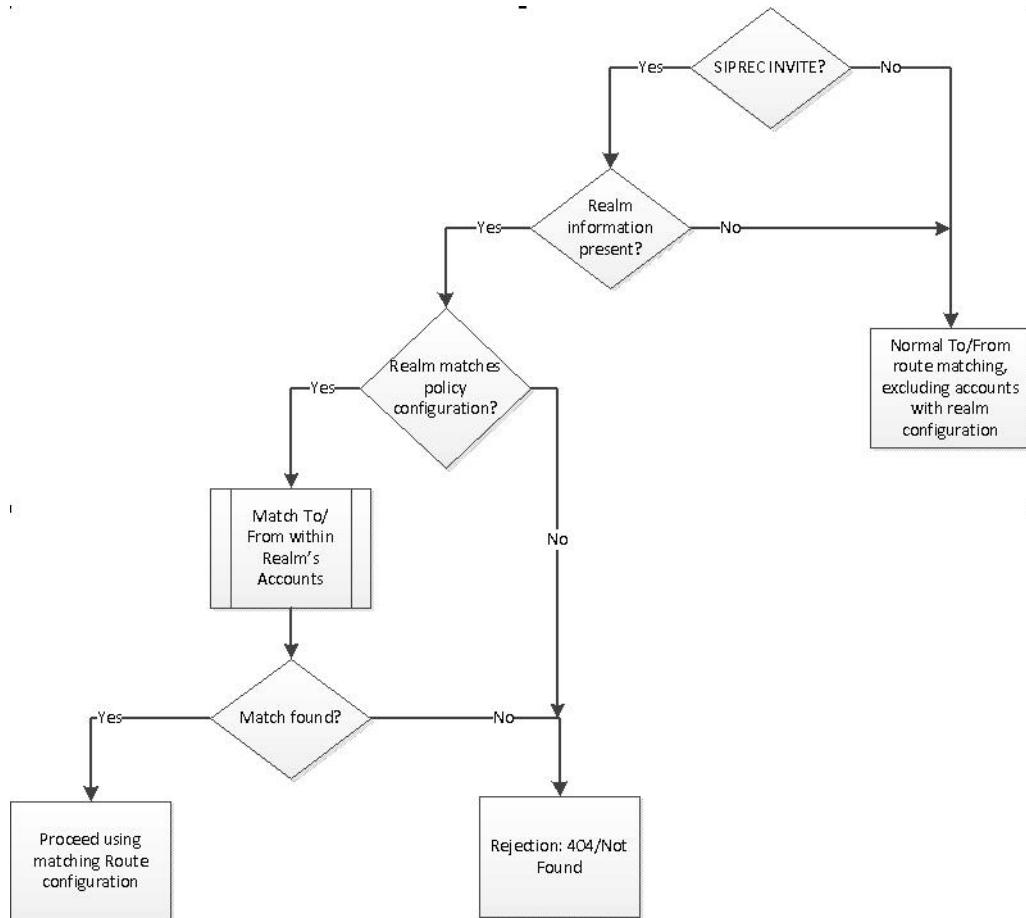
Note:

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 performs 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 routes of the deleted 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.

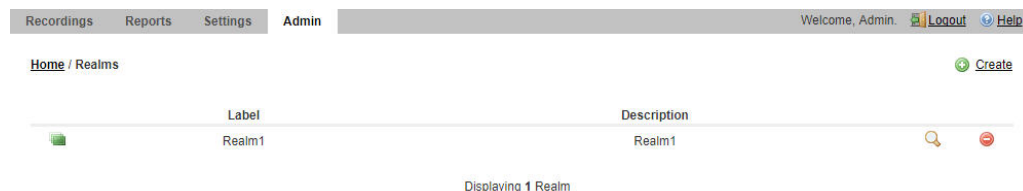
The following rules apply when associating an account(s) to a realm:

- 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 **Realms** option on the Admin page to manage Realms.

Realms Page



The following table describes the information displayed on the Realms page.

Column	Description
Label	Label name assigned to the Realm.
Description	Description of the Realm.
	Displays details about a Realm and allows you to edit the details if required.
	Deletes the Realm.

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 **Realms**. The Realms page displays.
3. Click **Create**. The following dialog box displays.

The screenshot shows a 'Create' dialog box. The dialog has a title bar with the text 'Create' and a close button (X). Inside the dialog, there are two input fields: 'Label' and 'Description'. The 'Label' field is a text box, and the 'Description' field is a text area. At the bottom right of the dialog, there is a 'Create' button.

4. **Label**—Enter the name of the realm to add to the ISR database.

5. **Description**—(optional) Enter a description for the realm you are adding.
6. Click **Create**. The Edit Realm page displays.

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 page displays.

2. Click **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. A prompt displays asking if you are sure you want to add this account.
4. To add the account to the realm, click **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.

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:

1. On the Realm list page, select a realm and click the Details icon. The Edit Realm page displays.

2. **Label**—Edit the name of the realm.
3. **Description**—Edit the description of the realm.
4. Click **Update**. The following message displays when an updated is successful.
Applied update 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.
A prompt appears asking if you are 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.

5

Managing Routes

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.

Manage Routes

Use the **Routes** link on the Admin page 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.

- 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.



Select **Routes** from the Admin page to manage Routes.

Routes Page

Account	Type	Pattern	Virtual Pattern	Recording is	Percent To Record
System	To	%	%DNIS%	Enabled	100

The following table describes the information displayed on the Routes page.

Column	Description
Account	Name of the Account associated with the route.
Type	Specifies the type of route: 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.
Pattern	Specifies the value to match an incoming call's From, To or From/To value, for applying the appropriate rules of the route and account.

Column	Description
Virtual Pattern	Specifies the destination where the calls matching the route pattern are forwarded once recording rules have been evaluated.
Recording is	Identifies whether or not recording is enabled or disabled on the route. enabled - Recording is enabled. disabled - Recording is disabled.
Percent to Record	Percentage of calls that are allowed to be recorded on this route.
	Displays details for the route and allows you to edit the details.
	Deletes the route.

Adding a Route

You can add a route or multiple routes to a specific account(s) using the **Create** 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 [Importing a Route CSV File](#).

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.

Adding a Route Configuration

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 **Routes**. The Routes page displays.
3. Click the **Create** 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. **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. **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 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 Pattern is used in conjunction with the Session Agent defined in Managing Sites. A full SIP URI can be provided to override this value. For examples of virtual route patterns, see Examples of Route Patterns.

 **Note:**

The **Virtual Pattern** parameter is only used for application types of Default Pass-Through and Record and Save.

8. **Label**—Enter a name to assign to this route. For display, such as in the recordings view, the route label replaces the value corresponding to the Route Type. For example, in a 'To' route, the 'To' value is replaced with the route label. This may

be useful to replace the number given by the service provider with a number more familiar to the users.

9. **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 any value for the specified Route Type on the incoming call. In this example, since Route Type is To, any incoming call with a To value will match.

 **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 and Editing Details of a Route

Super Users 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

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 **Routes**. The Routes page displays.
2. Select a route from the list and click the Details icon. The following dialog box displays.

3. **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. **Pattern**—Edit the route pattern to use for this account. This field is based on the Route Type selected in step 3 (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. For examples of virtual route patterns, see Examples of Route Patterns.
-  **Note:**

The Virtual Pattern parameter is used only for application types of Default Pass-Through and Record and Save.
6. **Label**—Edit the name of this route. For display, such as in the recordings view, the route label replaces the value corresponding to the Route Type. For example, in a 'To' route, the 'To' value is replaced with the route label. This may be useful to replace the number given by the service provider with a number more familiar to the users.
 7. **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 allows you to configure:

- Recording parameters
- Recording Editing Permissions

- Record and Save Mode parameters
- Archiving parameters
- Capacity parameters

▼ Advanced Configurations

Recording			
Route Mode	<input type="text" value="Standard (SIPREC)"/>	Video	
Recording is	<input type="text" value="Enabled"/>	Video Recording is	<input type="text" value="Disabled"/>
Percent To Record	<input type="text" value="100"/>	Video Access Permission	<input type="text" value="Enabled"/>
Always Record As Raw RTP	<input type="text" value="No"/>	Record and Save Mode	
Recording Format Profile	<input type="text" value="Default"/>	Record and Save on DTMF	<input type="text" value="dtmf-pound #"/>
Record DTMF	<input type="text" value="No"/>	Archiving	
Recording Editing Permissions		Keep Recordings for	<input type="text" value="365"/> Days
Allow Editing of Agent ID	<input type="text" value="Yes"/>	Sessions Capacity	
Allow Editing of Rating	<input type="text" value="Yes"/>	Session Capacity	<input type="text" value="24"/>
Allow Editing of Completed Transaction	<input type="text" value="Yes"/>	Additional Burst Session Capacity	<input type="text" value="6"/>
Allow Editing of Notes	<input type="text" value="Yes"/>		

Recording

The Recording Segmentation feature to split a session into multiple recordings may be configured for a particular route.

To configure the segmentation state for a route:

1. **Segmentation State**—Specify the type of segmentation recording you want to use for this route.
 - Enabled—Segmentation is always on
 - Disabled—Segmentation is always off
 - Ad-Hoc Only—Segmentation may only occur in the "ad-hoc" recording mode
 - Default to Account—Segmentation follows the Route's Account configuration.

For information on the remaining "Recording Advanced Configuration" fields, see "Recording Defaults".

Recording Editing Permissions

For information about configuring the **Recording Editing Permissions** fields, see Recording Editing Permissions.

Video

You can enable or disable video recording for a Route.

1. On the Admin page, click Routes.
2. Select a route from the Routes page and click the Details icon for that route.
3. Click **Video** to expand the video information.
4. In the **Video recording is** field, enable or disable video recording. By default, video recording is disabled.
5. In the **Video Access Permissions** field, specify whether users are allowed to access video recordings. By default, users are enabled.

6. Click **Update**.

Record and Save Mode

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

Capacity

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

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.

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.



Note:

All Changes made to a Master Route apply to all of the routes in the Route Group.

Adding a Route to a Route Group

To add a route to a Route Group:

1. Ensure you have a route configured that you want to use as the Master Route.
2. On the Admin page, click **Routes**. The Routes page displays.
3. Select the route that you want to use as the Master Route, and click the Details icon. The following dialog box displays.

The screenshot shows the 'Admin' page with a navigation bar containing 'Recordings', 'Reports', 'Settings', and 'Admin'. The user is logged in as 'Admin'. The breadcrumb trail is 'Home / Routes / %'. The 'Upgrade to Route Group' dialog box is open, showing the following fields:

- Account: System
- Type: To (dropdown)
- Pattern: % (text input)
- Virtual Pattern: %DNIS% (text input)
- Label: (text input)
- Priority: 1 (dropdown)

An 'Update' button is located at the bottom right of the dialog box.

4. Click **Upgrade to Route Group**. The **New Member Route** 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. 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. For example of route patterns, see Examples of Route Patterns.

 **Note:**

The Virtual Pattern parameter is used only for application types of Default Pass-Through and Record and Save.

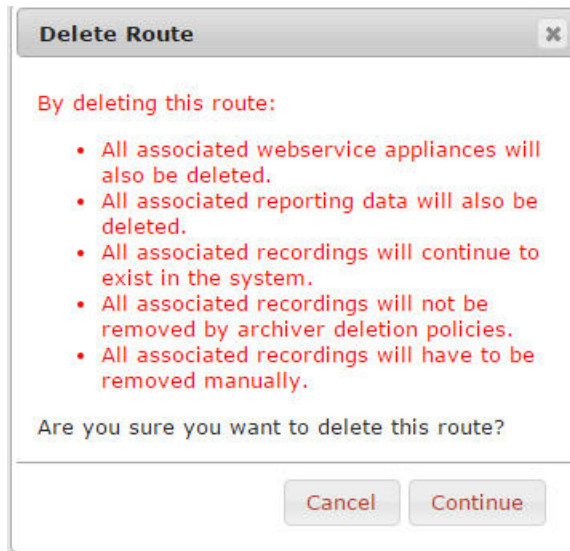
7. Click **Create** to add the Route to the Route Group. The Edit Route page displays with a **Route Members** tab available.
8. Add additional Member Routes to the Route Group if required by clicking **New Member Route** and repeat Steps 5, 6, and 7.

Deleting a Route

You can delete routes in the ISR Dashboard as required.

To delete a route:

1. On the Admin page, click **Routes**.
2. Select a Route from the Routes page and click the Delete icon for that Route. The following message and prompt displays.

 **Note:**

When you delete a route, the recordings associated with the route continue to exist in the system and are not removed by Archiver retention policies. If these recordings need to be deleted, it must be done manually.

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.

 **Note:**

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.

Importing a Route CSV File

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

 **Note:**

Ensure the values provided in the CSV file match the values in the table provided or the ISR will display an image.

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.
 - Boolean (yes/no) values must be entered using 0 (yes or enabled) and/or 1 (false or disabled).
 - The ISR does not ignore any leading and/or trailing spaces, so ensure your CSV does not have any.

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

Parameter Heading	Valid Values
route_type	0 From 1 To 2 From/To
route_pattern	text
virtual_route_pattern	text
label	text
priority	0.1 to 0.9
account_name	alpha-numeric characters
percent_to_record	0 to 100
recording_enabled	0 1
default_recording_type	1 None: Account or System default (default) 2 WAVE Linear/8bit/8KHz stereo 3 WAVE Linear/16bit/8KHz stereo 4 WAVE Linear/8bit/8KHz mono 5 WAVE Linear/16bit/8KHz mono 6 WAVE uLaw 8bit/8KHz stereo 7 WAVE aLaw 8bit/8KHz stereo 8 WAVE uLaw 8bit/8KHz mono 9 WAVE aLaw 8bit/8KHz mono 10 Raw uLaw 8bit/8KHz mono 11 Raw aLaw 8bit/8KHz mono 12 Raw PCM 8bit/8KHz mono 13 WAVE ADPCM 4bit/8KHz mono 14 WAVE ADPCM 8bit/8KHz stereo
agent_id_editable_flag	0 1
rating_editable_flag	0 1
completed_editable_flag	0 1
notes_editable_flag	0 1
application	pass_through conference record_and_save call_parking vam_sip_test
maximum number of ports	digits (-1 for no limit)
number_of_burst_ports	digits (-1 for no limit)
minimum_storage_days	0 to 365

Example File with Parameters and Values

ID	Route Name	Priority	Administrative Distance	Administrative Distance	Administrative Distance	Administrative Distance	Administrative Distance	Administrative Distance	Administrative Distance	Administrative Distance
1	10.10.10.10	10	10	10	10	10	10	10	10	10
2	10.10.10.10	20	20	20	20	20	20	20	20	20

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 **Routes**. The Route page displays.
6. Click **Import**. The following dialog box displays.

Import
✕

CSV File to Import Choose File No file chosen

▶ *Guidelines*

▶ *Sample File*

Import

7. **CSV File to Upload**—Click **Choose File** and navigate to the CSV file you are importing, select the file and click **Open** to populate the field.
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.

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.

6

Managing Users

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 the **Users** link on the Admin page 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 dependent on the user access level assigned to the Administrator. Super Users, Account Administrators, and Tenant Administrators have permissions to manage Users.




Select **Users** from the Admin page to manage Users.

Users Page

Name	Email	ISR Access	Account	User type
Admin	isradmin@oracle.com	Enabled	System	Super User

The following table describes the information displayed on the Users Page.

Column	Description
User Name	Name currently assigned to each User.
Email	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: <username>@<host server>.<domain name system (.com, .org, .net, .edu, etc.)>
ISR Access	Indicates the current status of the User. Status can be: enabled - Status is active. User can perform functions associated with its user type. disabled - Status is inactive. User cannot perform functions associated with its user type. Status detected that an error occurred for this User profile.
Account	Primary Account name for which the user is associated.
Type	User level assigned to this user (Super User, Account Administrator, Tenant Administrator, Tenant User, API User).

Column	Description
	Displays profile details about the User and allows you to edit the details.
	Displays details about the actions of the user. Information includes: Time - Time of the action. Action - Description of the action. Object - Object that was acted upon. IP Address - IP address of the user.
	Deletes the User profile.

User Access Levels

The display of information in the ISR Dashboard is dependent 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.

Functionality	Super User	Account Administrator	Tenant Administrator of	Tenant User	API Users
View/Play Recordings	Yes	Yes	Own Recordings only	Own Recordings only	No
Generate Reports	Yes	Yes	Reports for own Accts only	Reports for own Accts only	No
Edit Dashboard Settings	Yes	Yes	Yes	Yes	No
Manage Realms	Yes	Yes	No	No	No
Manage Accounts	Yes	Yes	Own Accts only	No	No
Manage Routes	Yes	Yes	Routes for own Accts only	No	No
Manage Authorization Services	Yes	Yes	No	No	No
Manage Users	Yes	Yes	Users for own Accts only	No	No
Manage Sites	Yes	View only	No	No	No
View Live Sessions	Yes	Yes	No	No	-

Note:An API User is specific to the FACE REST API and cannot log into the ISR Dashboard.

Adding a User

You can add a user to a specific account using the **New User** link on the **Users** page. Adding a User to the ISR is dependent on your access level permissions. Super Users 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).

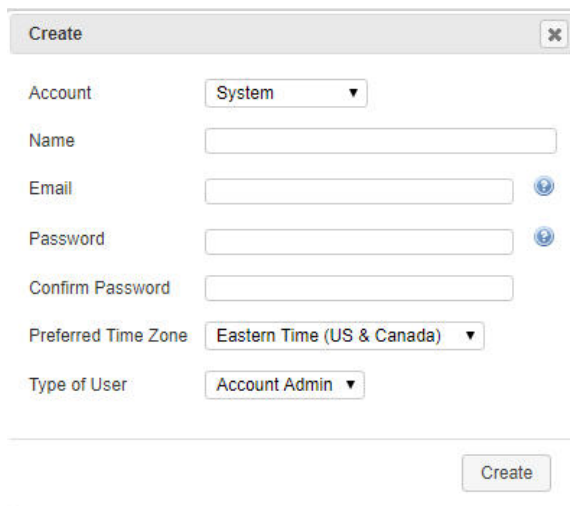
 **Note:**

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 [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 **Users**. The Users page displays.
3. Click **Create**. The following dialog box displays.



4. **Account**—Select the primary account to assign to this User. Valid values are dependent on the accounts currently configured in the ISR, and the permission level of the User. Default is System.
5. **Name**—Enter a name for the user.
6. **Email**—Enter the user's email address. This is the value the User enters in the Email field on the login page.
For example, smith@acmepacket.com.
7. **Password**—Enter a password for the user to specify when logging into the ISR Dashboard. When a user logs into the Dashboard for the first time with their assigned password, the Dashboard prompts the user to change the password for security purposes.

- Both letters and numbers
- At least one case-sensitive letter or special character
- At least 8 characters long

 **Note:**

This password expires based on the value you configure in the **Dashboard Security Settings Users Password Expires in** parameter. For more information on configuring this value, see "Managing User Dashboard Security Settings" in this guide.

- 8. Confirm Password**—Re-enter the password from Step 7 to verify you entered the password correctly.
- 9. Preferred Time Zone Locale**—Select the time zone locale or the location closes to the user. The following table provides the valid values and default for this field.

Abu Dhabi	Copenhagen	London	Sapporo
Adelaide	Darwin	Madrid	Sarajevo
Alaska	Dhaka	Magadan	Saskatchewan
Almaty	Dublin	Marshall Is.	Seoul
American Samoa	Eastern Time (US & Canada)	Mazatlan	Singapore
Amsterdam	Edinburgh	Melbourne	Skopje
Arizona	Ekaterinburg	Mexico City	Sofia
Astana	Fiji	Mid-Atlantic	Solomon Is.
Athens	Georgetown	Midway Island	Srednekolymysk
Atlantic Time (Canada)	Greenland	Minsk	Sri Jayawardenepura
Auckland	Guadalajara	Monrovia	St. Petersburg
Azores	Guan Hanoi	Monterrey	Stockholm
Baghdad	Harare	Montevideo	Sydney
Baku	Hawaii	Moscow	Taipei
Bangkok	Helsinki	Mountain Time (US & Canada)	Tallinn
Beijing	Hobart	Mumbai	Tashkent
Belgrade	Hong Kong	Muscat	Tbilisi
Berlin	Indiana (East)	Nairobi	Tehran
Bern	International Date Line West	New Caledonia	Tijuana
Bogota	Irkutsk	New Delhi	Tokelau Is.
Brasilia	Islamabad	Newfoundland	Tokyo
Bratislava	Istanbul	Novosibirsk	UTC
Brisbane	Jakarta	Nuku'alofa	Ulaanbaatar
Brussels	Jerusalem	Osaka	Urumqi
Bucharest	Kabul	Pacific Time (US & Canada)	Vienna
Budapest	Kaliningrad	Paris	Vilnius
Buenos Aires	Kamchatka	Perth	Vladivosotok

Cairo	Karachi	Port Moresby	Volgograd
Canberra	Kathmandu	Prague	Warsaw
Cape Verde Is.	Kolkata	Pretoria	Wellington
Caracas	Krasnoyarsk	Quito	West Central Africa
Casablanca	Kuala Lumpur	Rangoon	Yakutsk
Central America	Kuwait	Riga	Yerevan
Central Time (US & Canada)	Kyiv	Rihadh	Zagreb
Chatham Is.	La Paz	Rome	Zurich
Chennai	Lima	Samara	N/A
Chihuahua	Lisbon	Samoa	N/A
Chongqing	Ljubljana	Santiago	N/A

10. **Type**—Select the user type from the drop-down list to assign to this user. Valid values are

- Super User
- Account Admin
- Tenant Admin
- Tenant User
- API User

Available selections in the User Type field are dependent on the permission level of the current user. The following table identifies the values available for each level of access.

User Type	Available User Type Values
Super User	Super User Account Admin Tenant Admin Tenant User
Account Administrator	Account Admin Tenant Admin Tenant User
Tenant Administrator	Tenant Admin Tenant User
Tenant User	N/A
API User	N/A

11. Click **Create** to add the new User. The Edit User page displays.

Editing a User Profile

You can edit a User's profile as required. Access to a User profile is dependent 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 **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".
5. **Description**—(optional) Enter a description for the user. This parameter does not appear when adding a user and only appears on the Edit User page.

Note:

If you need more space for the Description field, click and drag the lower right-hand corner of the text box.

6. **Permissions**—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 current User Type. 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. 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 values available for each level of access.

User Type	Available Permission and Privileges
Super User	<p>A Super User can assign these permissions to a Tenant Admin and a Tenant User:</p> <ul style="list-style-type: none"> • Delete Recordings Permission • Edit Recordings Permission • Notes and Scoring Permission • Access to all Routes in Accounts Permission (Only applies to Tenant Users) • Download Recordings Permission • Playback Recordings Permission

User Type	Available Permission and Privileges
Account Administrator	An Account Admin can assign these permissions to a Tenant Admin and a Tenant User: <ul style="list-style-type: none"> Delete Recordings Permission Edit Recordings Permission Notes and Scoring Permission Access to all Routes in Accounts Permission (Only applies to Tenant Users) Download Recordings Permission Playback Recordings Permission
Tenant Administrator	A Tenant Admin can assign these permissions to a Tenant User: <ul style="list-style-type: none"> Delete Recordings Permission Edit Recordings Permission Notes and Scoring Permission Access to all Routes in Accounts Permission (Only applies to Tenant Users) Download Recordings Permission Playback Recordings Permission
Tenant User	N/A
API User	N/A

- 7. Accounts**—In addition to User Type, this field specifies which accounts (and their associated recordings) a user can access, add, edit, and delete.
- 8. Routes**—In addition to User Type, this field specifies which routes (and their associated recordings) a user can access, add, edit, and delete.
9. 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 Activity

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 upon which the action was performed.
- IP address of 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 **Users**. The Users page displays.
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.

Time	Action	Object	IP Address
2016-09-02 12:31:07.000-04:00	Default Login		10.138.238.156
2016-09-02 12:32:32.000-04:00	View Sites		10.138.238.156
2016-09-02 12:33:27.000-04:00	Create Site	Site_1	10.138.238.156
2016-09-02 12:33:27.000-04:00	View Sites		10.138.238.156
2016-09-02 12:33:29.000-	View Site	Site_1	10.138.238.156

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

Column Heading	Description
Time	Date and time (based on the time zone of the currently logged in user) when the user performed an action.
Action	Specific action that the user performed.
Object	Object upon which the action was performed.
IP Address	IP address of the User

If more entries exist than can 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 **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.

Importing a User Profile CSV File

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.



Note:

Ensure the values provided in the CSV file match the values in the table provided or the ISR will display an error message.

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.
 - Boolean (yes/no) values must be entered using 0 (yes or enabled) and/or 1 (false or disabled).
 - The ISR does not ignore any leading and/or trailing spaces, so ensure your CSV does not have any.

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

 **Note:**

At the time a user is created, the ISR saves their email address and no one else can create a user with the same email address, regardless of whether it is uppercase or lowercase.

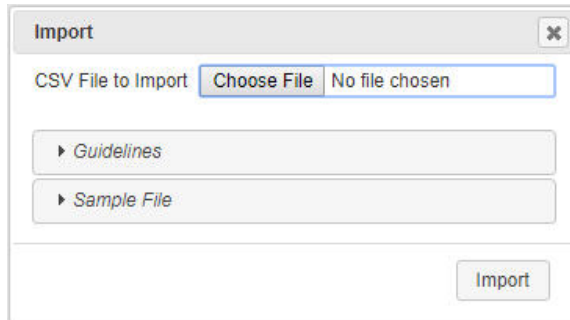
Parameter Heading	Valid Values
user_name	text
user_email	Usually a domain name in the format <username>@<host server>.<domain name system (.com, .org, .net, .edu, etc)>. For example: sample_email@abc.com
description	text
password	text
user_type	Super User Account Admin Tenant Admin Tenant User API User
account_name	text
login_disabled	0 1
time_zone_locale	Name of the Time Zone Locale (for more information, see "Adding a User")
audit_view_permission	0 1
call_control_permission	0 1
edit_recording_data_permission	0 1
notes_and_scoring_permission	0 1
access_to_all_routes_in_account	0 1

Example File with Parameters and Values

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	user_name	user_email	description	password	user_type	account_name	login_disabled	time_zone_locale	audit_view_permission	call_control_permission	edit_recording_data_permission	notes_and_scoring_permission	access_to_all_routes_in_account		
2	sample user	sample_email@sample.com	sample description	Abcd1234	tenant user	sample account	0	system	0	0	0	0	0		
3															

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

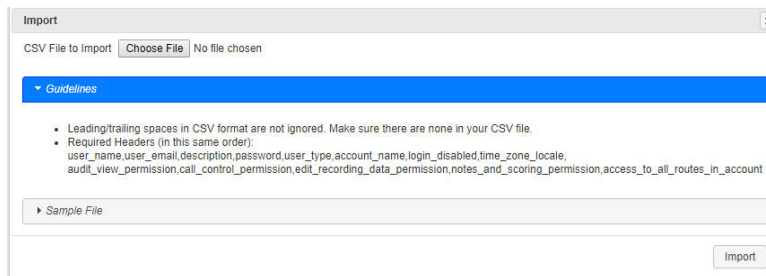
3. Login to the ISR Dashboard.
4. Click **Admin** in the main menu (or **Edit System Configurations** on the Home page).
5. Click **Users**. The Users page displays.
6. Click **Import**. The following dialog box displays.



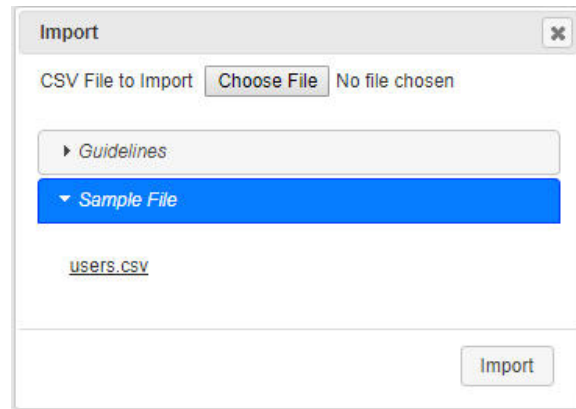
7. **CSV File to Upload**—Click **Choose File** and navigate to the CSV file you want to import, select the file, and click **Open** to populate the field.
8. Click **Upload** to upload the User Profile CSV file to the ISR database.

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.



7

Managing Authorization Services

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 the **Authorization Services** link on the Admin page 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 ISR 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.

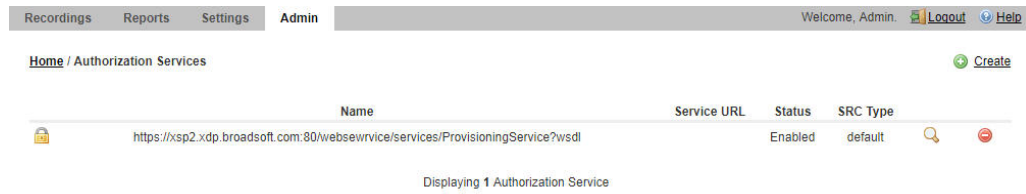
As a default security measure, third-party authorization users have only Tenant User privileges when they first log in. For example, in a deployment enabled for Broadworks third-party authorization, a successful Broadworks log in returns a user ID and group ID unique to that user. Initially the user 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 [Managing Users](#).

Select **Authorization Services** from the Admin page to manage Authorization Services.




 **Note:**

Only Super Users and Account Administrators have access to managing Authorization Services for other users.

Authorization Services Page



The following table describes the information displayed on the Authorization Services page.

Column	Description
Name	Name of the Authorization Service.
Service URL	Specifies the Uniform Resource Locator (URL) associated with the Authorization Service.
Status	Identifies the current status of the Authorization Service on the ISR. Values can be: enabled - Authorization Service is enabled. disabled - Authorization Service is disabled.
	 Authorization Service has an error(s).
SRC Type	Session Recording Client (SRC) type associated with the 3rd Party server. For example, Broadworks. Default is default.
	Displays details of the Authorization Service and allows you to edit the details.
	Deletes the Authorization Service.

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 dependent on your access privileges (Super Users and Account Administrators only).

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 **Authorization Services**. The Authorization Services page displays.
3. Click the **Create** link. The following dialog box displays.

4. **Name**—Enter the name of the Authorization Service (3rd party server).
5. **Service URL**—Enter the Uniform Resource Locator (URL) of the Authorization Service (3rd party server). 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 type of Session Recording Client (SRC) you are using in your ISR network.
8. Click **Create**. The new Authorization Service displays on the Authorization Services page.

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 dependent 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 **Authorization Services**. The Authorization Services page displays.

3. Choose an Authorization Service and click the Details icon for that Service. The Edit Authorization Service dialog box displays.

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 dependent 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 **Authorization Services**. The Authorization Services page displays.
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.

8

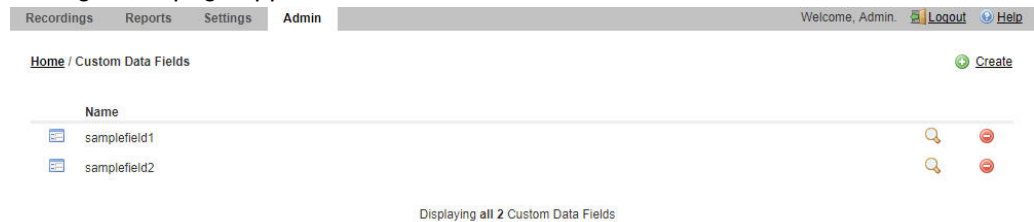
Custom Data

This chapter provides information about viewing and editing the custom data master list, custom data field session values, and using custom data fields advanced search options.

Viewing and Editing the Custom Data Master List

You configure the "master list" of Custom Data Field names via the ISR Dashboard.

Within the **Admin** tab, click **Custom Data Fields**. The Custom Data Field management page appears.



To add a new field name click **Create**.

The 'Create' dialog box has a title bar with 'Create' and a close button. It contains a text input field labeled 'Name' which is currently empty. Below the input field is a 'Create' button.

To edit and view the details of a Custom Data Field, click the Details icon.

The 'Update' dialog box has a title bar with 'Update' and a close button. It contains a text input field labeled 'Name' with the value 'samplefield1'. Below the input field is an 'Update' button.

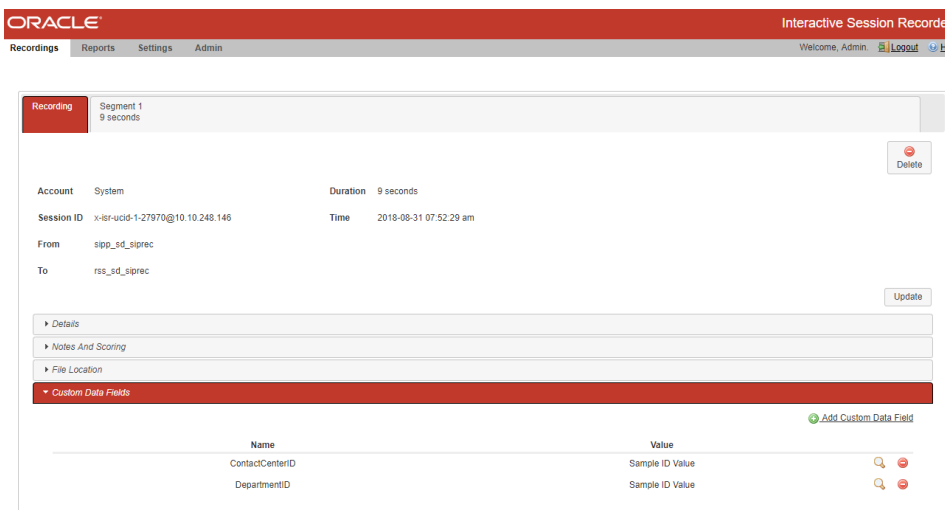
You can delete a Custom Data Field entry by clicking the delete icon.

 **Note:**





If values exist in any recordings for that Custom Field name, that Custom Field name cannot be deleted or edited, the only exception being that letters can be switched between upper and lower case.

Viewing and Editing Custom Data Field Session Values

Once the Master List has been generated and recordings are available in the Dashboard, you may manually add, edit, and delete Custom Data Field values via the Dashboard. In the **Recordings** list, click on a recording to view the details pane. Click on the Recording or any Segments tab, and click the **Custom Data Fields** section for options to add a custom data field, edit an existing value, or delete a value.



The screenshot displays the Oracle Interactive Session Recorder interface. The top navigation bar includes the Oracle logo, the title "Interactive Session Recorder", and tabs for "Recordings", "Reports", "Settings", and "Admin". A user profile section shows "Welcome, Admin" with "Logout" and "Help" links. The main content area shows details for a recording titled "Recording Segment 1" with a duration of "9 seconds". Metadata includes "Account: System", "Duration: 9 seconds", "Session ID: x-8r-ucid-1-27970@10.10.248.146", and "Time: 2018-08-31 07:52:29 am". Call details show "From: sipp_sd_siprec" and "To: rrs_sd_siprec". A sidebar on the right contains "Delete" and "Update" buttons. Below the metadata are expandable sections for "Details", "Notes And Scoring", "File Location", and "Custom Data Fields". The "Custom Data Fields" section is expanded, showing a table with two columns: "Name" and "Value".

Name	Value	
ContactCenterID	Sample ID Value	 
DepartmentID	Sample ID Value	 

An "Add Custom Data Field" button is located at the bottom right of the table.

Custom Data Fields Advanced Search

To find recordings via the Advanced Search option, click the **Recordings** tab's **advanced search** link. Click **By Custom Data Search Options**. Enter a Custom Data Field name and click Search. The ISR returns any recordings associated with the Custom Data Field name and value, along with any other "AND" or "OR" advanced search parameters.

Advanced Search ✕

Search Mode ▼

Partial Match

Media Type ▼

Session ID

From

To

Label

Search Date By Relative ▼

By Range

▶ *More Recording Search Options*

▼ *By Custom Data Search Options*

samplefield1

samplefield2

▶ *By Session Search Options*

9

External Event Destinations

This chapter provides information about viewing and editing the external event destinations.

The External Event Notification feature provides a way to notify RESTful services of events occurring in the ISR. It can be used in two ways: to notify third-party applications of new recordings, new sessions, and updates to existing sessions and recordings, or to notify new ISR components, acting as integrations to third-party platforms, of critical ISR events.

The external event notification system propagating session and recording events to the FACE server, which in turn interoperates with the ObserveIT Visual Session Recording solution is an example of ISR events communicating with a third-party application. These notifications provide data that allows the service to coordinate ISR recordings with ObserveIT screen capture recordings, providing simultaneous audio and video playback on applications such as the ISR Dashboard.

External Event Notifications

The External Event Notification feature provides a way to notify RESTful services of events occurring in the ISR. It can be used in two ways: to notify third-party applications of new recordings, new sessions, and updates to existing sessions and recordings, or to notify new ISR components, acting as integrations to third-party platforms, of critical ISR events.

When communicating with third-party applications, the external event notification system propagates session and recording events to a separate server that interoperates with the ObserveIT Visual Session Recording solution (the ISR FACE feature). The data provided in these notifications allows the service to coordinate ISR recordings with ObserveIT screen capture recordings in order to provide simultaneous audio and video playback on applications such as the ISR Dashboard.

External event notifications may be configured with a series of default settings for interoperation with ISR FACE and the ObserveIT Visual Session Recording solution. For more information on the interaction between ISR FACE and ObserveIT Visual Recording solution, see the "Face Policy System" section of this guide. If you require more extensive external event notification configuration, contact your Oracle representative.

Configuring External Event Destinations

You configure the External Event Destinations via the ISR Dashboard. To add or edit an External Event Destination:

1. After logging into the ISR Dashboard, click Admin in the main menu (or **Edit System Configurations** on the Home page).
2. Click the **External Event Destinations** link.
3. **Event Type**—Select the event type to trigger a notification.

- RECORDING_STARTED_EVENT—Recording has started
 - RECORDING_PAUSED_EVENT—Recording paused
 - RECORDING_RESUMED_EVENT—Recording has resumed
 - RECORDING_ENDED_EVENT—Recording has ended
 - SEGMENT_STARTED_EVENT—Recording segment has started
 - SEGMENT_ENDED_EVENT—Recording segment has ended
4. **Base Service URL**—Enter the URL of the server receiving the HTTP request.
 5. **URL Parameters**—Specify any parameters to be added to the request.

 **Note:**

For more information on event parameters and events, either click the **URL Parameters Help** link or see "External Events Notifications" in the *API Guide*.

External Event Configuration Example

Setting the **Event Type** to `RECORDING_STARTED_EVENT` and **Event Policy By** set to the "System" Account to send requests to the Base Service URL

```
https://myisreventreceiver.oracle.com:8443/handleIsrNotification" with  
the URL Parameters  
"event=AudioRecodingStarted&calledAors=%CALLED_AORS%&ucid=%INGRESS_CALLI  
D%
```

would submit an HTTP request in a similar way to entering the following example URL in your web browser:

```
https://myisreventreceiver.oracle.com:8443/handleIsrNotification?  
calledAors=sip:+12356789000@10.1.2.3&ucid=x-isr-ucid-1-24360@10.10.1.2
```


10

Managing Locales

This chapter provides information about offering the ISR Dashboard in languages other than English.

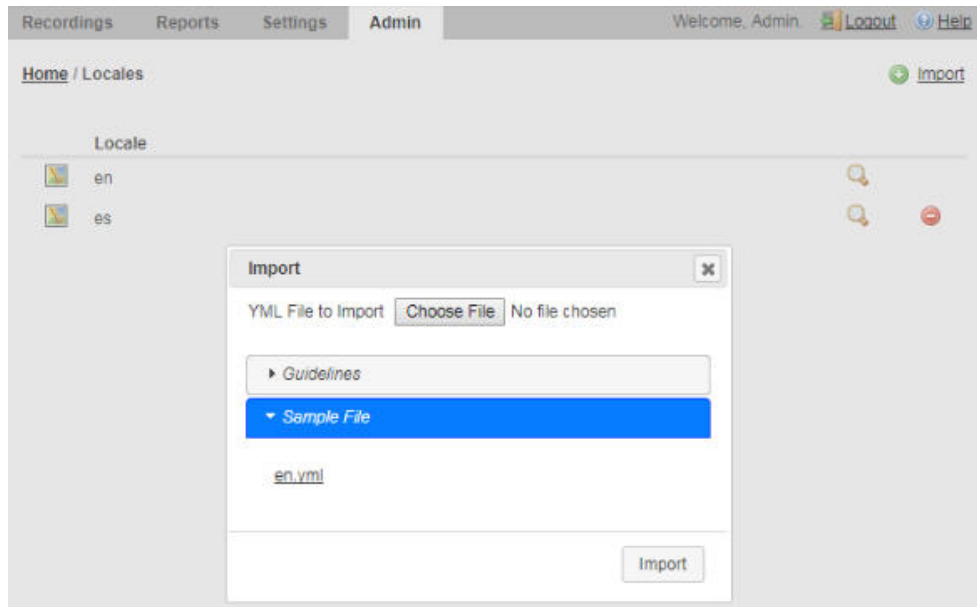
Manage Locales

For users looking to extend their branding and offer the ISR Dashboard in languages other than English, you can upload transcriptions of static dashboard text. Transcriptions are not provided by Oracle, but detailed instructions on how to upload translations, and a sample file are, making it easy to extend the ISR Dashboard.

Adding a New Locale

You can create, import, and set a new locale by completing the following procedure on the Dashboard:

1. In the Admin tab, click **Locales**.
2. Click **Import**.
3. Read the provided guidelines.
4. Click the provided "en.yml" English sample for a template for your locale.
5. Copy the content starting at the root element "en" and ending at "multi_page_html" and paste it into a local text file or editor.
6. Save the file as "<root_element>.yml", where <root_element> is the ISO language code. A comprehensive list of ISO-639-1 language codes can be found in https://www.w3schools.com/tags/ref_language_codes.asp.
7. Update the strings with the translations appropriate for the chosen language/locale.
8. Click **Choose File**, select the file, and click **Import**.



9. Set the "Preferred Language" for the User or Account (in "Branding and Language") to the new locale root element value.
10. Log in and confirm your changes.

11

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 **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 five Recording Format Profiles:

- Best Quality
- Default
- Small
- Smallest
- Firefox Compatible

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.

Editing a Recording Format Profile

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 **Recording Format Profiles**.

A list of all five recording format profiles displays.

3. Click the recording format profile you want to edit.

The Edit Recording Format Profile page appears.

The screenshot shows the 'Edit Recording Format Profile' page. At the top, there are navigation tabs: Recordings, Reports, Settings, and Admin. The user is logged in as Admin. The breadcrumb trail is Home / Recording Format Profiles / Best Quality. The form contains the following fields:

- Name:** Best Quality
- Description:** The best quality recordings

Below the form is a section titled 'Media Codec Mappings' with a table:

Transmission Codec	Recording Format
g.711 mulaw	WAVE ulaw (8bit 8Khz)
g.711 alaw	WAVE alaw (8bit 8Khz)
g.722	WAVE PCM (16bit 16Khz)
g.729	WAVE ulaw (8bit 8Khz)

Below the table is a 'Preferences' section with a 'Small File Size' slider and a 'Best Quality' checkbox. An 'Update' button is located at the bottom right of the preferences section.

4. **Name**—Enter a name for this recording format profile.
5. **Description**—Enter a brief description of this recording format profile.
6. **Recording Preference**—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.

Recording Format Mappings Configuration

To configure Recording Format Mappings:

1. Click **Recording Format Mappings** in the Edit Recording Format 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

To apply 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 **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 **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

To apply 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 **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 **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.
7. Click **Update**.

Route Recording File Permissions

The Route Recording File Permissions on the Routes page allow you to configure route-level playback, deletion, and download recording file permissions through the ISR Dashboard.

Route Recording File Permissions

Recording File Permissions
(Drag and Drop permissions below; then Update to apply.)

Granted	Available
Play Recording Permission	
Download Recording Permission	
Delete Recording Permission	

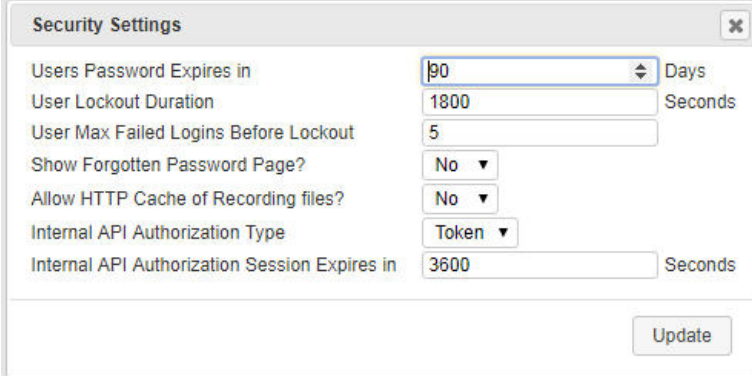
12

Managing 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 **Security Settings**.



The screenshot shows a 'Security Settings' dialog box with the following fields:

Setting	Value	Unit
Users Password Expires in	90	Days
User Lockout Duration	1800	Seconds
User Max Failed Logins Before Lockout	5	
Show Forgotten Password Page?	No	
Allow HTTP Cache of Recording files?	No	
Internal API Authorization Type	Token	
Internal API Authorization Session Expires in	3600	Seconds

An 'Update' button is located at the bottom right of the dialog.

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. **Allow HTTP Cache of Recording files?**—Specify whether the ISR includes the following HTTP header, `Cache-Control: max-age=0, no-cache, no-store`, in response to recording playback requests. When set to **Yes**, the ISR does not include the header. When set to **No**, the ISR does include the header.
8. **Internal API Authorization Type**—Select **token** to enforce authorized communication between the RSS components. Select **none** to disable authorization for RSS component communications. The default is **token**.
9. **Internal API Authorization Session Expires in**—Set the number of seconds before the authorization token expires and a new one is created. The default value is **3600** seconds.

10. Click **Update**.

13

Managing Template Definitions

ISR offers the FACE API for customers wishing to connect to ISR to extract recordings for use in other 3rd party or homegrown applications. Some legacy recording vendors require recording metadata be delivered in a pre-defined format. Using Export Templates, customers can create a defined format for data extraction and then call the FACE API, referencing the Template, to extract recording information in the defined format. Export Templates are version controlled and can be updated or replaced as needed. ISR provides the Verint® Import Manager Template, by default.

Template Definitions

Templates can be defined to format the metadata returned by FACE requests for segment details. They can be created, edited, and deleted in the Template Definitions sections of the Admin tab. Users can specify a name for the Template, and a version number is automatically assigned, starting at 1 and incrementing for each update to the Template body with the same name.

 **Note:**

Templates continue to support legacy recordings that contain a single segment.

Formatting

The text contained in the Template body is returned as is, unless it is surrounded by percent symbols (%). When FACE is using a template and comes across a % character, if the next character is also a %, a single % is inserted in the response. Otherwise, it searches for a second % and tries to find a matching Field Parameter for the text between the %s (exclusive). If found, the segment's appropriate value for the Field Parameter Name is inserted in the response. If no default Field Parameter match is found, the Custom Data for the recording is checked, whereupon the value of a matching Custom Data field is appended to the response. In the event that no value can be determined for the given Field Parameter (in both the default list and among the Custom Data), an empty string is inserted in the formatted text returned to the client. If no closing % is found after an opening %, an error code/response is returned, indicating that the template is improperly formatted. Text between and after field parameters (delineated by %) is appended to the response as is.

Field Parameters

The following list contains the currently supported Field parameters with a brief description of each. In addition, any defined Custom Data fields can be included as Field Parameters using the Custom Data field name in the template body (surrounded by percent % signs).

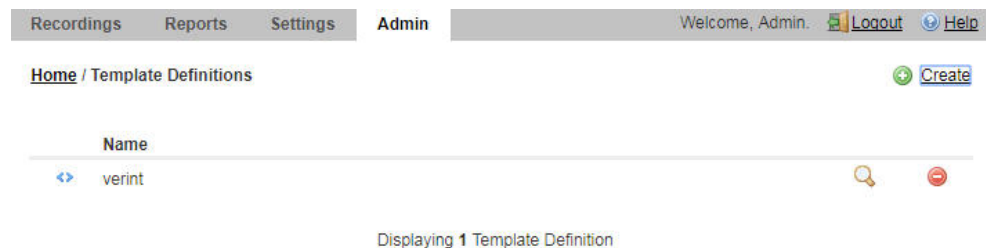
- recordingId—recording ID
- filename—audio recording filename
- directory—audio recording file relative directory
- isrUcid—ISR UCID
- ingressCallId—ingress call ID
- egressCallId—egress call ID
- from—from/ANI
- to—to/DNIS
- accountId—account ID
- routeId—route ID
- rssId—RSS ID
- agentId—agent ID
- duration—duration (milliseconds)
- durationSeconds—duration (seconds)
- startDate—start date (yyyy-MM-dd)
- startTime—start time (HH:mm:ss)
- startDateUtc—start date in UTC (yyyy-MM-dd)
- startTimeUtc—start time in UTC (HH:mm:ss)
- startYear—start date year
- startYearUtc—start date year in UTC
- startMonth—start date month
- startMonthUtc—start date month in UTC
- startDay—start date day
- startDayUtc—start date day in UTC
- startHour—start time hour
- startHourUtc—start time hour in UTC
- startMinute—start time minute
- startMinuteUtc—start time minute in UTC
- startSecond—start time second
- startSecondUtc—start time second in UTC
- startMillisecond—start time millisecond
- startMillisecondUtc—start time millisecond in UTC
- startTimeZone—start time time zone (e.g. EDT)
- startTimeZoneOffse— start time time zone offset (e.g. +0400)
- pauseLength—pause length (milliseconds)
- baseUrl base—URL (from which recording file is served)
- sourceDirectory—archiver source directory

- destinationDirectory—archiver destination directory
- segmentId—segment ID
- checksum—checksum (MD5)
- endDate—end date (yyyy-MM-dd)
- endTime—end time (HH:mm:ss)
- endYear—end year date
- endMonth—end month date
- endDay—end date day
- endHour—end time hour
- endMinute—end time minute
- endSecond—end time second
- endMillisecond—end time millisecond
- endTimeZone—end time zone (for example, EDT)
- endTimeZoneOffset—end time zone offset (for example, +0400)
- endDateUtc—end date in UTC (yyyy-MM-dd)
- endTimeUtc—end time in UTC (HH:mm:ss)
- endYearUtc—end date year in UTC
- endMonthUtc—end date month in UTC
- endDayUtc—end date day in UTC
- endHourUtc—end time hour in UTC
- endMinuteUtc—end time minute in UTC
- endSecondUtc—end time second in UTC
- endMillisecondUtc—end time millisecond in UTC

Adding a New Template

You can create a special formatting template by performing the following procedure on the Dashboard:

1. In the Admin tab, click **Template Definitions**.
2. Click on the provided "verint" template for an example and return to "Template Definitions" when ready.
3. Click **Create**.



4. Assign a **Name**.

5. In the **Body** field, enter any required special formatting characters and the %-surrounded ISR fields represented in "Field Parameters".
6. Click **Create**.

 **Note:**

You may download segment metadata in the new special format using the example provided in "Common FACE Commands" in the *Oracle Communications Interactive Session Recorder API Guide*.

Recordings with No Media

ISR offers the ability to optionally write an empty (0 byte) file when a recording INVITE is received and indexed, but results in no RTP being received. These "missing" recordings can occur when a session terminates so quickly that the Recorder process does not have time to fully initialize, or when media is never offered for an established session.

To better reconcile these situations for certain customer use cases, a new Archival process configuration has been created to ensure a recorded file is created and associated with the existing metadata regardless of whether RTP was ever received.

To enable this functionality, set the **Create Empty Recordings** parameter to **yes** for each Location instance. By default, this parameter is disabled.

Recordings	Reports	Settings	Admin
Home / Sites / dh / Locations			
Name	rss105 (10.10.248.105) Primary		
Remote Access URL	<small>(e.g. http://location1.foo.com/Recordings)</small> http://10.10.249.105:8080/Recordings		
Access Type	Local		
▶ Local/Mount Configurations			
▶ SFTP Configurations			
▼ Advanced Configurations			
Global? (Accessible to all Sites)	No		
Checksum	None		
Able to Delete Recordings	No		
Store in Date Directory	Yes		
Store in Account Directory	No		
Purge Index of Missing Recordings	No		
Create Empty Recordings	No		

When this parameter is enabled, when a missing file for a recording record is encountered, the Archival process writes an empty file in the recording destination Location and logs a message similar to the following example:

```
9/7/17 14:20:00[INFO ]      Thread[ArchiverThread-71,5,main]
(Missing File) creating empty recording for /opt/isr/Recordings/
rss_g711_ulaw-1-2171@10.10.248.128.wav
```

This message can also be found in the **Segment Details, File Location** section of the Dashboard.



File Location	
Store Indefinitely	<input type="checkbox"/>
Archival Status	Successfully Archived
Directory	/2017-09-11/13/09
Archival Remarks	(Missing File) created empty recording: /opt/isr/ArchivedRecordings/2017-09-11/13/09/rss_g711_ulaw-1-28154@10.10.248.209.wav at Mon Sep 11 09:12:00 EDT 2017 by archiver ID 1 process ID ap-isrdev-dh1-3.us.oracle.com15e71116911.

Existing customers who do not wish to change the current ISR behavior should leave the **Create Empty Recordings** parameter set to **No**.

14

Viewing Live Sessions

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

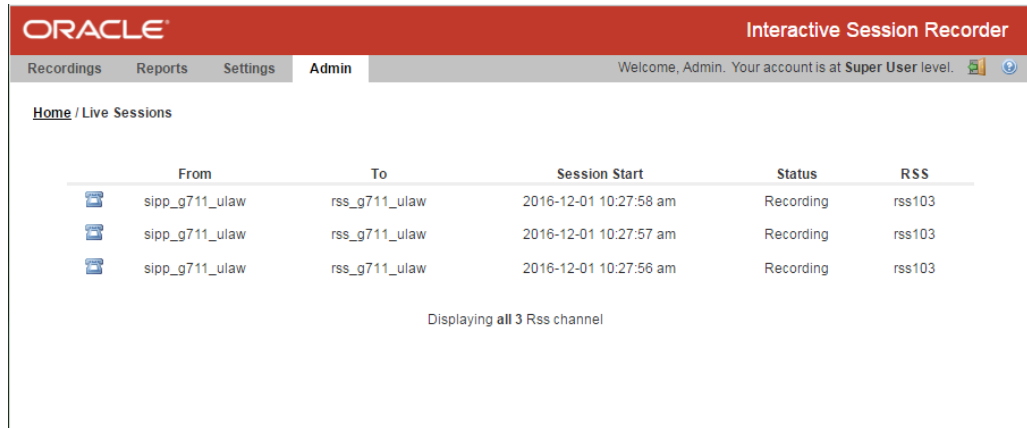
Manage Live Sessions

Use the **Live Sessions** link on the Admin page of the ISR Dashboard to view live call sessions currently occurring.

 **Note:**

Only Super Users and Account Administrators can view live call sessions currently being received by an RSS.

Lives Sessions Page



From	To	Session Start	Status	RSS
sipp_g711_ulaw	rss_g711_ulaw	2016-12-01 10:27:58 am	Recording	rss103
sipp_g711_ulaw	rss_g711_ulaw	2016-12-01 10:27:57 am	Recording	rss103
sipp_g711_ulaw	rss_g711_ulaw	2016-12-01 10:27:56 am	Recording	rss103

Displaying all 3 Rss channel

The following table describes the information displayed on the Live Sessions page.

Column Heading	Description
From	Specifies the From SIP URI. This is the URI from where the call session is coming.
To	Specifies the To SIP URI. This is the URI to where the call session is destined.
Session Start	Specifies the date and time in the user's preferred time zone locale when the active session began.

Column Heading	Description
Status	Identifies whether the session is: Recording - Call session is in progress and the RSS is recording the session. Idle - Call session is in progress but the RSS is not currently recording the session.
RSS	Specifies the name of the RSS receiving the live call session.

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.

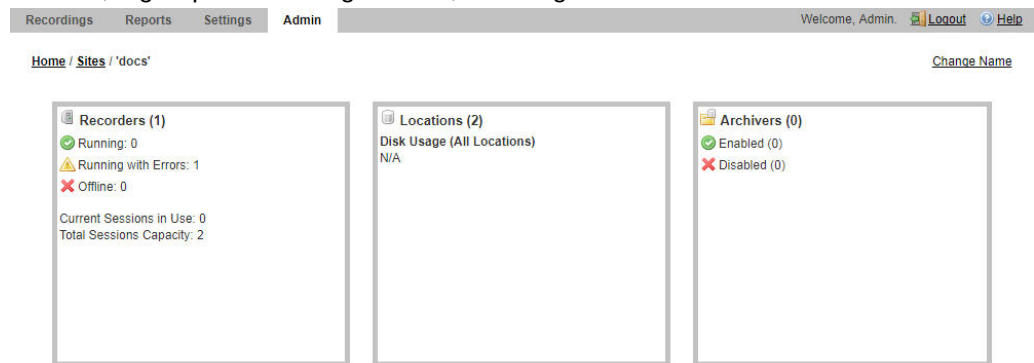
15

Managing Sites

This chapter describes how to configure, manage, and monitor the components of an 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 Sites page under the Administrator menu.

Manage Sites

Use the **Sites** link on the Admin page 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:

Site Item	Description
RSS	Allows you to view RSS (recording server) information, delete an RSS, modify an RSS, or add a new RSS associated with a site. The configuration parameters include the RSS name, IP Address, XML-RPC port number, and utilization of available ports for each RSS.
Location	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.
Archiver	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).

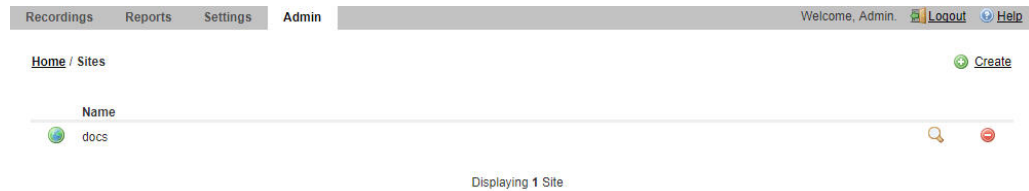
Select **Sites** from the Admin page to manage Sites.





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.

Sites Page



The following table describes the information displayed on the Sites page.

Column	Description
Name	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.

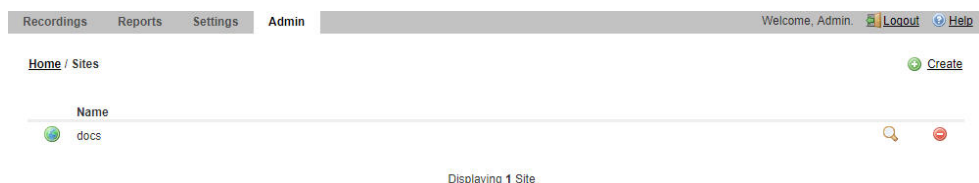
Adding a Site

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

- RSS (required)
- RSS Location (required)
- Archiver (optional)
- Session Agent (optional)
- Web Appliance (optional)

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 **Sites**. The Sites page displays.



- Click the **Create** link in the upper right corner of the page. The following dialog box displays.

- Name**—Enter a name for the Site.
- 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 a 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.

Note:

Oracle recommends you contact your Technical Support representative before adding or changing an RSS configuration.

Sites RSS Summary

The RSS Listing page contains the following information:

RSS Information	Description
Name	RSS name
VoIP IP	RSS Voice network IP address
Status	<ul style="list-style-type: none"> •  - Running •  - Offline •  - Running with errors
Uptime	Number of Days RSS has been available
Current Sessions In Use	Number of active sessions
Sessions Capacity	Total number of simultaneous sessions allowed

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 Sites page displays.

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

Name	VoIP IP	Status	Uptime	Current Sessions in Use	Sessions Capacity
rss197	10.10.248.197	Warning	4 days	0	2

Displaying 1 Recorder

3. Click **Create**. The following dialog box displays.



Create

Name

VoIP IP

Admin IP

Data IP

Sessions Capacity

*A new location will be created for this new RSS with default path configurations (/opt/isr/Recordings).

Create

4. **Name**—Enter a name that describes the RSS you are adding.
5. **VoIP IP**—The RSS Voice network IP address.

Note:

A new location is created for the RSS using this IP Address under the Location component, with a default path value of `opt/isr/Recordings`. You can edit the location if you've installed the RSS on a different filesystem path. For more information, see [Managing an RSS Location](#).

6. **Admin IP**—The IP address to connect to the RSS host over the "Admin" network.
7. **Data IP**—The IP address to connect to the RSS components (for example, the Converter, API, and Recorder processes) over the "Data" network.
8. **Sessions Capacity**—Total number of licensed ports on the RSSs on this Site.
9. Click **Create**. The new RSS displays on the RSS page.

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

4. The following RSS configuration sections are available:

Name	Description
Advanced Configurations	RSS Recorder process connection details
API Configurations	API connection settings
Converter Server Configurations	Converter process settings
Locations	Recorder process Location settings

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

Advanced RSS Configurations

The following fields may be changed in an RSS's Advanced Configurations settings:

- **Name**—Enter a name that describes the RSS you are adding.
- **VoIP IP** —The RSS Voice network IP address.
- **Admin IP** —The IP address to connect to the RSS host over the "Admin" network.
- **Data IP**—The IP address to connect to the RSS components (for example, the Converter, API, and Recorder processes) over the "Data" network.
- **Sessions Capacity**— Total number of licensed ports on the RSSs on this Site.
- **SIP ISR UCID Header Field**— The administrator may set the SIP header name whose value is to be parsed as the ISR's UCID. The default value is "X-ISR-UCID".
- **Config update interval**—How often the Recorder attempts to update its configuration.

- **Webservice SSL Enabled?**—Enables the Recorder webservice for HTTPS communications. This is enabled by default.
- **Rest webservice ssl cert file**— The path of the file offered in the certificate exchange. The default value is `"/opt/isr/security/keys/rss_cert.pem"`.
- **Log Level**— Recorder process logging level. The default value is `"INFO"`.

**Note:**

The remaining fields in the Advanced Configuration section are not available for configuration.

RSS API configurations

The following settings are available to configure the internal RSS API:

- **API URL Scheme**—The protocol used for the API URL. The default value is `"https"`.
- **API URL Port**—The port number on which the API listens. The default value is `"8443"`.
- **API URL Base Path**—The base path serving the API application. The default value is `"/IsrApi/rest/"`.
- **API Cache Update Interval**—The number of seconds before the API cache is updated. The default value is `"300"`.

RSS Converter Server Configurations

The following settings are available for configuring the Converter Process:

- **Codec map update interval**— The number of seconds between Codec Map updates of transmission and playable codecs. The default value is `"300"`.
- **Config update interval**— The number of seconds before the Converter updates its broader configurations. The default value is `"300"`.

**Note:**

The remaining fields in the Converter Server Configurations section are not available for configuration.

RSS Locations

The following settings configure where the Recorder process writes its files:

- **Location**— The primary location for writing recorded files. The default value is `"<RSS name (IP)> Primary"`.
- **Failover location**— The failover location for writing recorded files. The default value is `"<RSS name (IP)> Secondary"`.

RSS Ports Status

The RSS's Ports Status section offers a listing of Recorder process ports and some details on the status of each.

RSS Logs

The RSS's Logs section provides the most recent logs written by the Recorder process.

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 RSS 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.



Note:

Once you delete an RSS, it cannot be recovered.

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 in the ISR system where the recordings are stored. You can add a new Location or change an existing Location if required. You can also delete the location if necessary.



Note:

When you add your first RSS, the ISR automatically adds an **RSS Primary Location** to the **Locations** page.

Adding a Location


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

 **Note:**

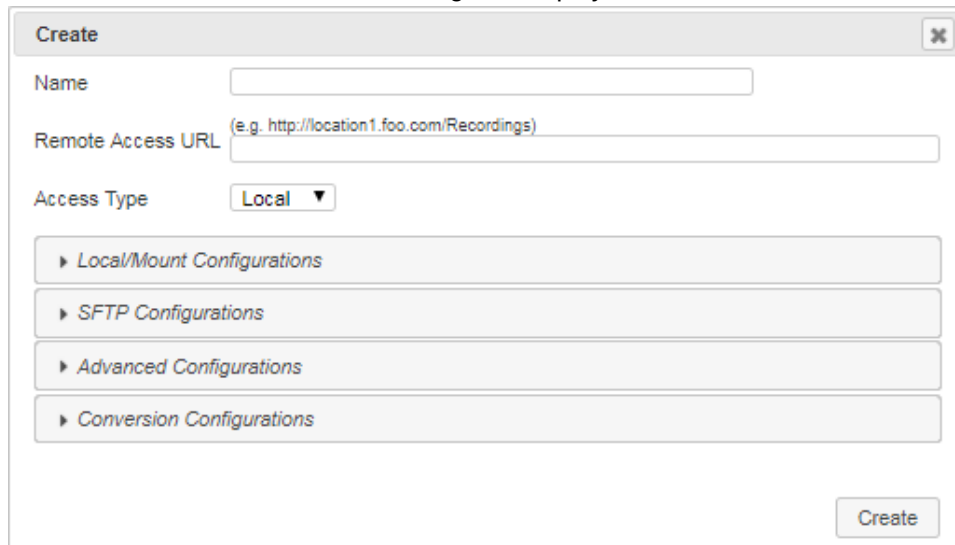
A single configured Archiver can move recordings to only one destination location. If you need recordings to go to other destination locations, you must configure an Archiver for each of those locations. For more information about configuring an Archiver, see *Managing Archivers*.

To add a new RSS Location:

1. From the Sites page, choose a Site and click the Details icon. The Sites page displays.
2. Click on the **Location** component. The following table describes the information displayed on the Location page.

Column	Description
Name	Name of the RSS Location.
Local Recordings Directory	Specifies the directory path associated with the Location.
Remote Access URL	Specifies the Web URL path for accessing the recordings via a browser.
Disk Usage	Indicates the percentage of storage disk used for recordings in the directory location. Valid values are 0% to 100%.
	Delete the RSS Location from the ISR database.

3. Click **Create**. The New Location dialog box displays.



4. **Name**—Enter a name that describes the Location you are adding. For example, RSS1 (1.1.1.1) Primary.
5. **Remote Access URL**—Enter the URL that identifies the Web location for accessing the recordings via a browser. For example, http://location1.foo.com/Recordings.

 **Note:**

Locations created automatically by the addition of a valid RSS configure the URL and serve recordings from it. If you add custom locations, you must configure them to be served by a web server and then set this URL if you want them to be playable via the Dashboard or APIs.

6. Access Type—Select one of the following:

- Local - Local disk
- Mount - NFS Mount shared directory
- SFTP - SFTP server
- SFTP Port - Specify the port number. Valid values are 0 - 65535. The port needs to be enabled in the specified host.

The following sections describe the additional configuration parameters available in the Location page's section. When you are finished configuring all of the parameters for your environment, click **Create** to complete creating the Location.

Local/Mount Configurations - Local Recordings Directory

The Local/Mount Configurations according allows you to specify the directory of the Account's Archival destination Location.

- Local Recordings Directory—Specifies the directory path to where the Archiver stores the recordings on the RSS associated with the Location. For example, /opt/isr/Recordings.

 **Note:**

When **Access Type** is set to **SFTP**, the Archiver attempts to move the Account's recordings to the SFTP user "home" path on the SFTP server.

SFTP Configurations

The SFTP configuration section allows you to configure the Location's SFTP properties.

- SFTP Host—Specify the Location's SFTP host.
- SFTP User—Specify the Location's SFTP user.
- SFTP Password—Specify the Location's SFTP password.

Advanced Configurations

The Advanced Configurations section allows you to configure several advanced configuration properties for the Location.

- Global? (Accessible to all Sites)—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.

- Checksum—Enables the MD5 Hash for Recordings feature. For more information, see "Configuring MD5 Checksum Validation".
- Able to Delete Recordings—Select whether or not this Archiver has permission to delete recordings and metadata stored longer than specified in Route and Account configurations. Valid values are:
 - Yes (default) - Archiver deletes files older than specified in Route and Account configurations.
 - No - Archiver does not delete files, regardless of the date specified in the Route and Account configurations.
- 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.
- Store in Account Directory—Select whether or not the Archiver stores the recording files in a folder identified by the associated account. Valid values are:
 - Yes - Archiver stores recordings in a folder by account.
 - No (default) - Archiver does not store recordings in a folder by account.
- Purge Index of Missing Recordings—Select whether or not the Archiver removes recording entries containing no recorded media files, from the main recording table, and sends them to a different "problem" table that can be reviewed at a later time. By enabling this feature, you prevent a user from viewing recording files with no recorded media files when they perform a search. However, an Administrator can view the "problem" table if required, for troubleshooting purposes. When this field is disabled, the Archiver keeps the recording file with no recorded media in the main recording table. Valid values are:
 - Yes - Archiver moves recordings containing no recorded media from the main recording table to a "problem" table. Users cannot view these recordings, but Administrators may view the "problem" table.
 - No (default) - Archiver keeps recordings with no recorded media files in the main recording table. Users may view these recordings.
- Create Empty Recordings—When enabled, the Archiver creates a recorded file even when no media was available for writing (for example, a session terminates immediately after INVITE is negotiated). Valid values are:
 - Yes - Archiver creates an empty recorded file when media is not available for writing.
 - No (default) - No empty recorded files are created.

Conversion Configurations

Configure how and when the Archiver converts RPDD recording files to .wav files prior to moving them to their destination location via the Conversion Configurations section.

- **Converter IP Address**—Enter the IP address (in dotted decimal format) of the media converter (RMC). For example, 172.53.45.6.

 **Note:**

For more information on managing the media converter, see "ISR RMD".

- **Converter REST Webservice SSL Enabled?**—Enables or disables secure communications with the Converter process webserver. The default is "Yes".
- **Mode**—Select whether all RPDD recordings (currently G.729 recordings or recordings from routes set to **Always record as raw RTP**) are converted, a percentage of recordings are converted, or no recordings are converted when the Archiver moves them to the destination location.
 - Disabled (default) - The RMC does not convert RPDD recordings from .rpdd format to .wav format.
 - Convert All - The RMC converts all RPDD recordings from .rpdd format to .wav format
 - Convert by Percentage - The RMC converts only a percentage of all RPDD recordings from .rpdd format to .wav format, based on the value entered for the **Percent of Recordings to Convert** parameter.
- **Percent of Recordings to Convert** - Select a number to indicate the percentage of recordings to be converted by the RMC. 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.

Editing a Location

You can edit an existing Location if required.

To edit a Location:

1. On the Sites page, choose a Site with a Location and click the Details icon. The Viewing Site page displays.
2. Click on the **Locations** component. The Locations page displays.
3. Choose a Location to edit and click the Details icon. The Update 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 Locations page.

Deleting a Location

You can delete a Location if required.

To delete a Location:

1. On the Sites page, choose a Site with a Location and click the Details icon. The Viewing Site page displays.
2. Click on the **Locations** component. The Locations page displays.
3. Choose a Location to delete and click the Delete icon. A prompt asking, "Are you sure you want to delete this Location?" displays.

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.

 **Note:**

Once you delete a Location, it cannot be recovered.

Managing Archivers

You configure an Archiver(s) to store recordings. The Archiver(s) moves recording files from one Location to another Location, often 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 recordings are written 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 `/opt/isr/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 `/opt/isr/ArchivedRecordings`).

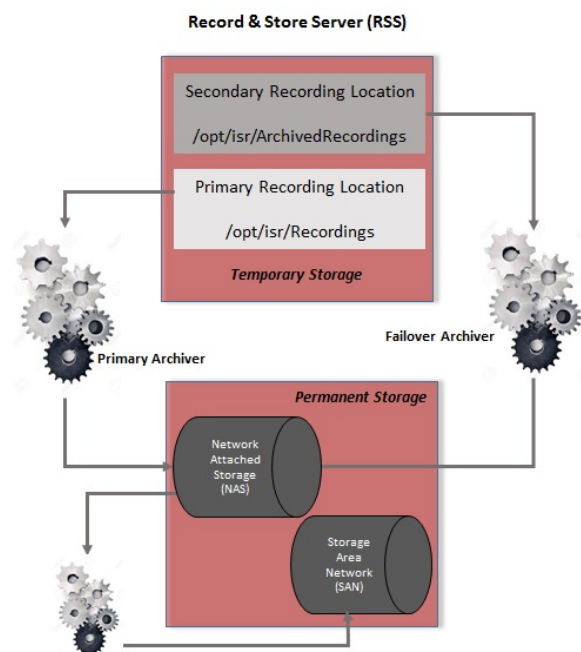
 **Note:**

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.



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

Archivers Information	Description
✔ Enabled	Total number of Archivers enabled on this Site.
✘ Disabled	Total number of Archivers disabled on this Site.

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.

Note:

You may also configure Archiving on a per Account basis. For more information, see "Archival" in the "Managing Accounts" chapter.

To add an Archiver:

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





The Sites page displays.

- Click on the **Archivers** component. The Archivers page displays.

IP Address	Source	Destination	Status	Threads	Move Attempts	Mode
172.30.12.103	RSS197 (10.138.217.197) Primary	RSS197 (10.138.217.197) Primary	Enabled	3	3	Primary

Displaying 1 Archiver

The following table describes information displayed on the Archivers page.

Column	Description
IP Address	IP Address of the 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.) to which the Archiver moves the recordings for storage. When the Archiver moves the recording files to the destination location, it can create subdirectories in this path to sort by account, date, and time.
Status	Identifies whether the Archiver is enabled (active) for moving recording files, or temporarily disabled (paused). Status can be:  Enabled  Disabled
Mode	Specifies the 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.
	Displays details of the Archiver and allows you to edit the details.
	Deletes the Archiver from the ISR database.

- Click **Create**. The new Archivers dialog box displays.
- 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, 134.35.43.56).
- Source**—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.

 **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**—Select the location of the storage devices (NAS, SAN, etc.) to which the Archiver moves the recordings for storage.
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 source location to the destination location. If the Archiver fails to move the recording files the first time, it repeats the attempts to move the files the number of times you set for this field. 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. 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.
2. Click on the **Archivers** component. The Archivers page displays.
3. Choose an Archiver to edit and click the Details icon. The Archivers dialog box displays.
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 **Archivers** component. The Archivers page displays.
3. Choose an Archiver to delete and click the Delete icon. You are prompted to confirm the delete.
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.

 **Note:**

Once you delete an Archiver, it cannot be recovered.

16

Managing Recordings

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

Manage Recordings

All user levels can be configured to view, edit, delete, download, and/or play recordings stored on the ISR (or other configured storage facility). However, a Tenant Administrator and Tenant User, if granted the appropriate permissions, can edit, play, download, and delete their own recordings only.

 **Note:**

Recordings that display are dependent on the level of user currently logged into the ISR Dashboard.

In addition to viewing, editing, playing, downloading, 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 from 1 star to 5 stars, with 5 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

RSS Ingress Call ID	Time	From	To	Duration	CustomDataField1
1-25460@10.10.248.209	2018-08-28 05:50:45 pm	sipp_sd_siprec	rss_sd_siprec	2 minutes 0 seconds	CustomDataValue1
1-25425@10.10.248.209	2018-08-28 05:38:04 pm	sipp_sd_siprec	rss_sd_siprec	1 minute 59 seconds	
1-25415@10.10.248.209	2018-08-28 05:34:31 pm	sipp_sd_siprec	rss_sd_siprec	2 minutes 0 seconds	
1-25256@10.10.248.209	2018-08-28 04:30:15 pm	sipp_g711_ulaw	rss_g711_ulaw	5 seconds	CustomDataValue2
1-25252@10.10.248.209	2018-08-28 04:29:49 pm	sipp_g711_ulaw	rss_g711_ulaw	3 seconds	

The following table describes each possible column on the Recordings page.

Column Heading	Description
Time	Specifies the start date and time of the recording. This column is based on the User's preferred time zone locale.
From	Specifies the calling party.
To	Specifies the called party.
RSS Ingress Call ID	Specifies the call-id from the SIP headers of the initial INVITE.
RSS Egress Call ID	Specifies the call-id from the SIP header of a secondary call leg. Only applicable for pass-through or Record & Save routes.
Duration	Specifies the length of time, in seconds, of the recording.
Session ID	Specifies the unique X-ISR-UCID for this recording.
	Downloads the selected recording to a file on your PC.
	Deletes the Recording from the ISR system.
	Screen recording playback is available.
	Video playback is available.

Playing a Recording

After a recording occurs on the ISR, it is saved as an audio, and optionally video, file so a user can review the details of the recording and playback the audio and video. Play a recording by first choosing it in search results or the default listing to bring up the Recording Details page, then clicking the Segment tab and the play button for that recorded Segment file.



Note:

The recording's metadata is saved in the ISR database.

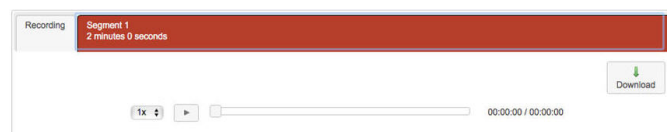
The Recordings page displays all up-to-date recordings that meet the search parameters and access level restrictions of the user. Depending on the size of your storage device (Network Attached Storage (NAS), Storage Area Network (SAN)), older

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.

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. Click on the row of a recording to show the details, then click the **Segment 1** tab. If you have the appropriate permissions, you may play the recording using the play button at the top of the screen.



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 in **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 file(s) automatically opens 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:

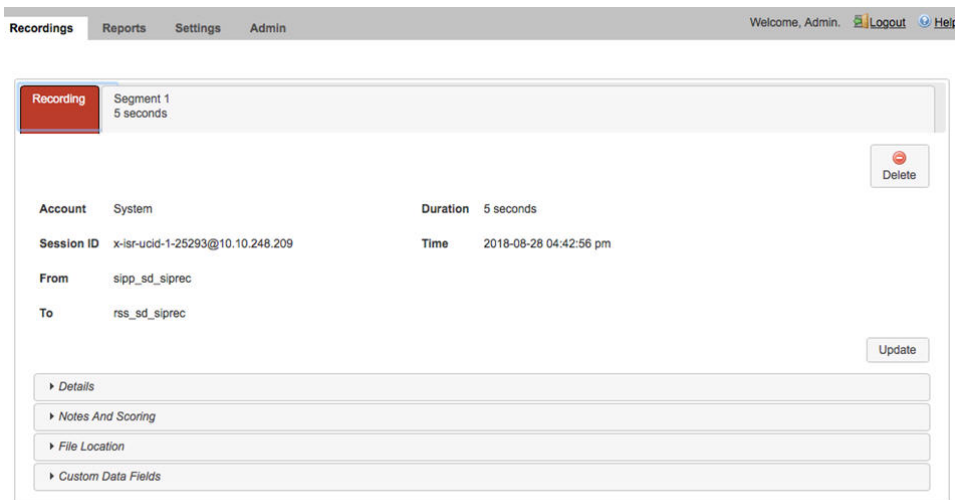
- Play a recording.
- Assign custom data fields to a recording.
- Specify whether or not the recording is completed.
- Assign a length of time, in hours/minutes that the reviewer spent reviewing/transcribing the recording.
- Specify notes pertaining to the recording.
- Assign a rating to the recording.
- 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 Recording Details page displays.



The following table describes information displayed on the Recording Details page.

Column Heading	Description
Account	Specifies the Account name associated with the recording.
Session ID	The unique session identifier for the session that contains the recording segment(s).
From	Specifies the calling party.
To	Specifies the called party.
Duration	Specifies the length of time, in seconds, of the recording.
Start Time	Specifies the date and time when the active session began. This is displayed in the user's preferred time zone locale.

To play the recording, click the appropriate segment tab. For example, Segment 1 and the play button at the top of the segment details.

When the recording is retrieved, the file(s) automatically opens 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 more information.

Viewing Recording Details

To display details:

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

The screenshot shows the Oracle Recordings interface. At the top, there are navigation tabs: Recordings, Reports, Settings, and Admin. The user is logged in as Admin. The main content area displays a recording segment with the following details:

Account	System	Duration	2 minutes 0 seconds
Session ID	x-tsr-ucid-1-28605@10.10.248.209	Time	2018-08-29 03:00:54 pm
From	sipp_sd_siprec		
To	rss_sd_siprec		

Below the details, there are expandable sections: Details, Notes And Scoring, File Location, and Custom Data Fields. There are also buttons for Delete and Update.

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.

Notes and Scoring

To specify transaction notes and rating, select the Notes and Scoring section of the Recordings page. The following information displays.

1. **Complete**—Select whether or not the call session represents a completed transaction 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) - The transaction occurring during this recording is not yet complete.
 - Yes - The transaction occurring during this recording is complete.

Note:

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

2. **Hours**—Enter the length of time, in hours that the reviewer spent reviewing/transcribing the recording. Valid values are in decimal format using numeric characters. For example, 6.5, where 6 indicates the hours and .5 indicates 1/2 hour.
3. **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 rating, and 5 being the best rating. 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.

4. **Category**—Enter a category name to associate with the recording, and press **<Tab>**.
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 4.
5. **Notes**—Enter notes pertaining to the current recording. Adding more than will fit in this box displays scroll bars in the window that allow you to scroll through multiple screens of the note.

 **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.

6. **Transcription**—Enter the conversation that took place during the current recording. Adding more characters than will fit in this box displays scroll bars in the window that allow you to scroll through multiple screens of the transcription.
7. Click **Save Changes** to save the details for the recording.






 **Note:**

The above agent-focused fields are available through Dashboard and FACE at the overall session level, but not for individual Segments in the session. These fields are replaced with a much more flexible workflow using Custom Data in Segments and soon deprecated for overall session-level details as well.

Recording Details Custom Data

Specifies custom data values to associate with this recording. This information is specific to this recording

Create custom data fields via the Admin page's **Custom Data Fields** link. For more information on configuring Custom Data, see "Custom Data".

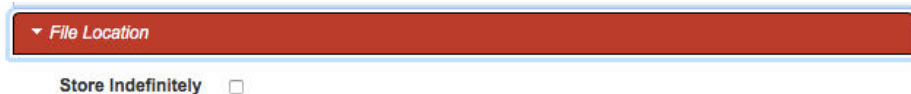
▼ Custom Data Fields			
	Name	Value	
	sampleField1	sample value 1	 
	sampleField2	sample value 2	 

 **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".

Recording Details File Location

The File Location section on the Recording Details page provides information about storing a recording indefinitely.



Archiving Recordings Permanently

You can view archival status of a recording 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, select the recording you want to flag, and click File Location on the Recording's detail page.



2. **Store Indefinitely**—Check the box to ensure this recording is never deleted due to expiration.
3. Click **Save Changes**.

Segment Details Configuration

To display and specify Segment details:

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

- Click the **Segment #** tab and the Segment details display.

Recording Segment 1
2 minutes 0 seconds

Download

1x ▶ 00:00:00 / 00:00:00

File Name	rss_sd_siprec-1-28605@10.10.248.209.seg0.wav
Duration	2 minutes 0 seconds
Start Time	2018-08-29 03:00:54 pm
End Time	2018-08-29 03:02:54 pm
Secured Media	No Secured Media

- ▶ Details
- ▶ File Location
- ▶ Custom Data Fields
- ▶ Session Metadata
- ▶ Session Participant Metadata

Segment Recording Details Custom Data

Specifies custom data values to associate with this recording segment.



Create custom data fields via the Admin page's **Custom Data Fields** link. For more information on configuring Custom Data, see "Custom Data".

Note:

To add or change detailed information about a recording segment, 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".

Recording Supplemental Files

The Supplemental Files section of Recording Details includes any additional recorded files associated with the session such as files in MP4 format from recording of a video session. If the user's permissions allow, these files may be downloaded by clicking the download icon for each file.

Supplemental Files		
File Name	File Type	
raf-ae6f19af0308b0e125b32a92b5b528dd@10.138.217.133-1.mp4	video	
raf-ae6f19af0308b0e125b32a92b5b528dd@10.138.217.133-2.mp4	video	

Segment Session Metadata

To view Segment Session Metadata:

1. On the Recordings page, choose a recording and click the Details icon. The Recording Details page displays.
2. Click **Session Metadata**. The following information displays.

Session Metadata	
SIPREC Session ID	Hbp8WXmmRVZPI4FSEU1mlg==
Start Time	2017-09-05 01:57:58 pm

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 time the call recording session began. The date and time are based on the time zone configured for the User.

The **Session Extension Metadata** displays additional extension metadata associated with the session. The metadata types that may be present here include:


- apkt:ucid
- calledPartyNumber
- callID
- callingPartyNumber
- extTrackingID
- groupID
- newExtTrackingID
- serviceProviderID
- userID

Segment Session Participant Metadata


You can view specific participant metadata, including extension metadata, 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 Recording Details page displays.
2. Click **Session Participant Metadata**. The following information displays.

Session Participant Metadata				
SIPREC Participant ID	Name	Participant AOR	Start Time	End Time
swWEGj0SSbBs39Y53GllKw==	leo	sip:leo@10.138.239.179	2017-09-05 01:57:58 pm	
LMbgTxCjRw5FPXmO3+FjwCQ==	raf	sip:raf@10.138.237.213	2017-09-05 01:57:58 pm	

The following table describes each field on the Session Participant Metadata page.

Column Heading	Description
SIPREC Participant ID	Specifies the ID of the SIPREC participant on the recording.
Name	Specifies the SIP URI name of the SIPREC participant.
AOR	Specifies the address of record (AOR) associated with the participant.
Start Time	Specifies the date and time when the active session recording began.
End Time	Specifies the date and time when the active session recording ended.
	Displays extension metadata information about the participant if it exists.

- Choose a SIPREC Participant ID and click the Details icon to display extension metadata information about the participant.

Information in this box can include metadata for:

- apkt:-realm
- apkt:P-Asserted-Identity
- apkt:Diversion
- apkt:request-uri

For more information about these parameters, see Recording Search by Session.

Displaying DTMF Data in Segment Details: Routes

You can configure the ISR to display DTMF data within a call's recording details for digits transmitted via RFC 2833 and SIP INFO. The **Record DTMF** 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:

- After logging into the ISR Dashboard, click **Edit System Configurations** or click **Admin** in the top menu bar.
- Click **Routes**.
A list of all routes configured on the ISR displays.
- Click the route on which you want to enable the recording of DTMF data.
- Click **Route Advanced Configurations**.

▼ Advanced Configurations

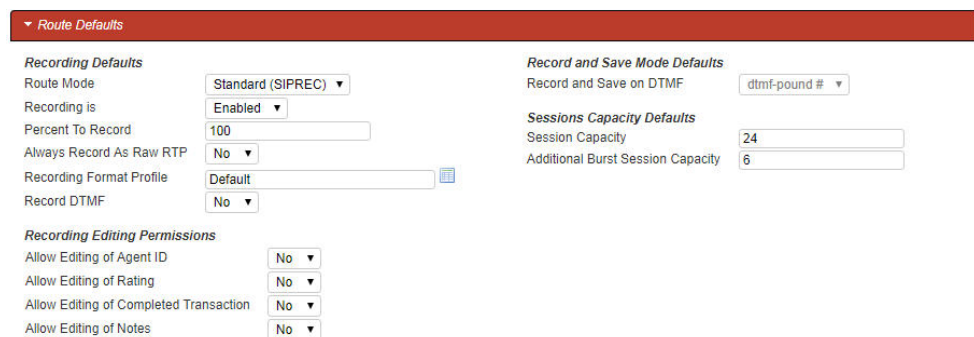
Recording		Video	
Route Mode	<input type="text" value="Standard (SIPREC)"/>	Video Recording is	<input type="text" value="Disabled"/>
Recording is	<input type="text" value="Enabled"/>	Video Access Permission	<input type="text" value="Enabled"/>
Percent To Record	<input type="text" value="100"/>	Record and Save Mode	
Always Record As Raw RTP	<input type="text" value="No"/>	Record and Save on DTMF	<input type="text" value="dtmf-pound #"/>
Recording Format Profile	<input type="text" value="Default"/>	Archiving	
Record DTMF	<input type="text" value="No"/>	Keep Recordings for	<input type="text" value="365"/> Days
Recording Editing Permissions		Sessions Capacity	
Allow Editing of Agent ID	<input type="text" value="Yes"/>	Session Capacity	<input type="text" value="24"/>
Allow Editing of Rating	<input type="text" value="Yes"/>	Additional Burst Session Capacity	<input type="text" value="6"/>
Allow Editing of Completed Transaction	<input type="text" value="Yes"/>		
Allow Editing of Notes	<input type="text" value="Yes"/>		

5. **Record DTMF**—Select whether or not to display DTMF data. Valid values are:
 - Use Account's Setting—This route defaults to its account's behavior.
 - No—No DTMF data appear in the recording details.
 - Yes—data details appear in the recording details.
6. Click **Update**.

Displaying DTMF Data in Segment Details: Accounts

To enable the ISR to display DTMF data 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 **Accounts**.
A list of all accounts configured on the ISR displays.
3. Click the account on which you are want to enable the recording of DTMF data.
4. Click **Route Defaults**.

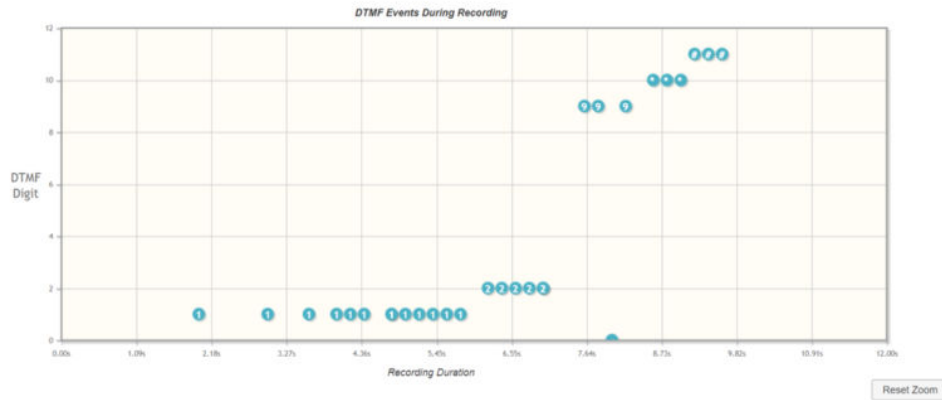


5. **Record DTMF**—Select whether or not to display DTMF details. Valid values are:
 - No—No DTMF data appear in the recording details.
 - Yes—DTMF data appear in the recording details.
 - Use System Account's Setting—This account defaults to the System account's behavior. This is the default value.
6. Click **Update**.

Displaying DTMF Data in Segment Details

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.



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.
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.

Note:

Once a recording is deleted, it cannot be recovered. The file is deleted from disk and the metadata is removed from the database.

17

Managing Reports

The ISR allows you to generate call usage and billing statistical reports using date and route filters. This chapter describes the types 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:

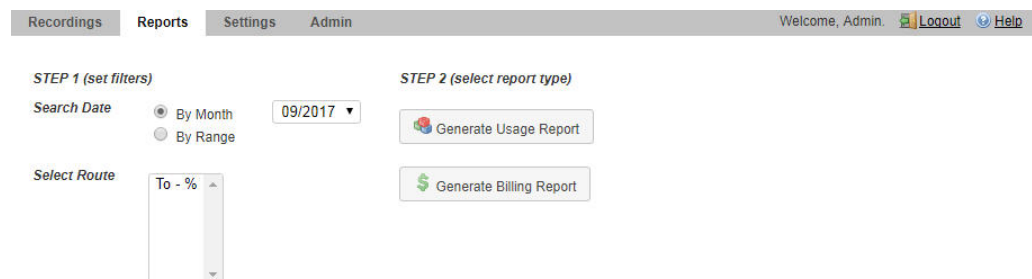
- **Usage Reports**- Generates a report that includes call recorder usage information by date range and/or by route.
- **Billing Reports** - Generates a report that includes billing information by date range and/or by route.

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).



Reports Page



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.

Generating a Usage 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.

Generating a report by month

To generate a report by month:

1. Select **By Month**.
2. In the drop-down box, select the month for which you want to generate the report. Valid values are dependent on the dates for calls stored in the ISR database.

Generating a report by range

To generate a report by range:

1. Select **By Range**. The **From Date** and **To Date** fields display.
2. **From Date**—Click the cursor in the text box or click the Calendar icon to display the calendar.

3. Click the date from where you want to begin to include the report data. Use the arrow keys in the calendar to change months.
4. **To Date**—Click the cursor in the text box or click the Calendar icon to display the calendar.
5. 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.

Selecting a route

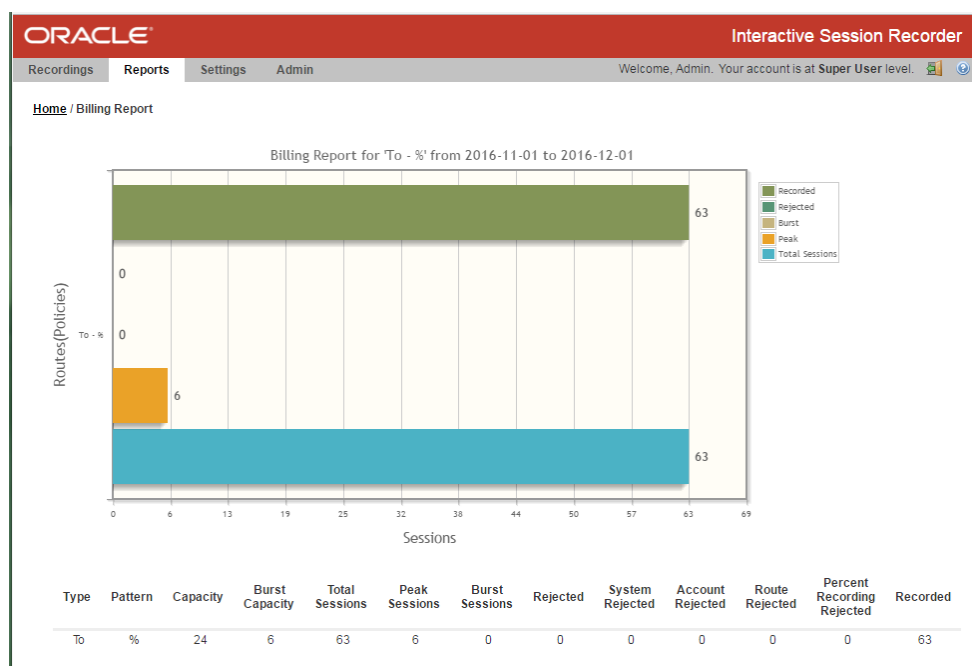
To select a route:

1. **Select Route**—Select a route or routes to include in the report. Valid values are dependent 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.

2. Click **Usage Reports**. The **Generate Report** button displays.
3. 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.

Usage Report Bar Graph Descriptions

The following table identifies the information in the bar graph section of the report.

Usage Report Bar Graph Descriptions

Graph Information	Description
Routes (Policies)	Indicates the route(s) selected for this report.
Sessions	Indicates the number of sessions handled by the route.
Recorded	Indicates total number of recorded sessions on the route during the reported period.
Rejected	Indicates total number of rejected sessions on the route during the reporting period.
Burst	Indicates total number of burst sessions on the route during the reporting period. Burst sessions are sessions handled by the Burst Ports.
Peak	Indicates maximum number of simultaneous sessions on the route during the reporting period.
Total Sessions	Indicates total number of sessions on the route during the reporting period.




The following table describes each column in the data format section of the report.

Usage Report Data Format Descriptions


Column	Description
Type	The type of route policy (for example, To, From, or To/From).
Pattern	The route pattern that the RSS looks for when searching for a route policy.
Capacity	Total concurrent sessions allocated to the route.
Burst Capacity	Number of concurrent sessions available for call recording when the provisioned capacity has been depleted.
Total Sessions	The total number of sessions for this reporting period.
Peak Sessions	The maximum number of concurrent sessions that occurred during this reporting period.
Burst Sessions	The total number of sessions that occurred after the provisioned capacity had been depleted.
Rejected	Total number of rejected sessions on this route during this reporting period.
System Rejected	The total number of rejected sessions by the ISR during this reporting period.

 **Note:**

This data is only available in a day by day breakdown.

Column	Description
Account Rejected	The total number of rejected sessions by this account during this reporting period.
	<div style="border: 1px solid #0070C0; padding: 5px;"> <p> Note:</p> <p>This data is only available in a day by day breakdown.</p> </div>
Route Rejected	The total number of rejected sessions by this route during this reporting period.
	<div style="border: 1px solid #0070C0; padding: 5px;"> <p> Note:</p> <p>This data is only available in a day by day breakdown.</p> </div>
Recorded	Total number of recorded sessions on this route during this reporting period.
Percent Recording Rejected	Total number of sessions rejected during this reporting period because of the route's percent to record setting.
	<div style="border: 1px solid #0070C0; padding: 5px;"> <p> Note:</p> <p>This data is only available in a day by day breakdown.</p> </div>

After you have generated a usage report, you can click on the details icon for a specific route within the report to view a day by day breakdown of the statistics.

Detailed Stats for Route '%'										
Date	Total Sessions	Peak Sessions	Burst Sessions	Rejected	System Rejected	Account Rejected	Route Rejected	Percent Recording Rejected	Recorded	
2016-11-30	55	5	0	0	0	0	0	0	55	
To	%	24	6	55	5	0	0	55		

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.

Generating a Billing Report

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.

2. **Search Date**—Select whether you want to generate a report by the month or by date range.

Generating a Report by Month

To generate a report by month:

1. Select **By Month**.
2. In the drop-down box, select the month for which you want to generate the report. Valid values are dependent on the dates for calls stored in the ISR database.

Generating a Report by Range

To generate a report by range:

1. Select **By Range**. The **From Date** and **To Date** fields display.
2. **From Date**—Click the cursor in the text box or click the Calendar icon to display the calendar.
3. Click the date from where you want to begin to include the report data. Use the arrow keys in the calendar to change months.
4. **To Date**—Click the cursor in the text box or click the Calendar icon to display the calendar.

- 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.

Selecting a Route

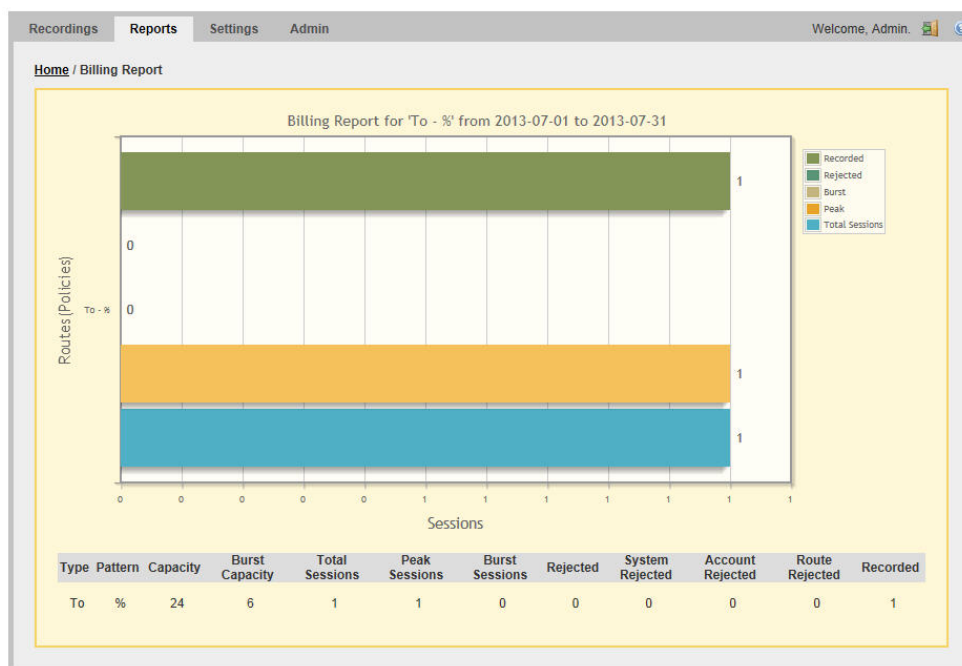
To select a route:

- Select Route**—Select a route or routes to include in the report. Valid values are dependent 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.

- Click **Billing Reports**. The **Generate Report** button displays.
- 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.

Billing Report Bar Graph Descriptions

The following table identifies the information in the bar graph section of the report.

Billing Report Bar Graph Descriptions

Graph Information	Description
Routes (Policies)	Indicates the route(s) selected for this report.

Graph Information	Description
Sessions	Indicates the number of sessions handled by the route.
Recorded	Indicates total number of recorded sessions on the route during the reported period.
Rejected	Indicates total number of rejected sessions on the route during the reporting period.
Burst	Indicates total number of burst sessions on the route during the reporting period. Burst sessions are sessions handled by the Burst Ports.
Peak	Indicates maximum number of simultaneous sessions on the route during the reporting period.
Total Calls	Indicates total number of sessions on the route during the reporting period.

The following table describes each column in the data format section of the report.

Billing Report Data Format Descriptions

Column	Description
Type	The type of route policy (i.e., To, From, or To/From).
Pattern	The route pattern that the RSS looks for when searching for a route policy.
Capacity	Total concurrent sessions allocated to the route.
Burst Capacity	Number of concurrent sessions available for call recording when the provisioned capacity has been depleted.
Total Sessions	The total number of sessions for this reporting period.
Peak Sessions	The maximum number of concurrent sessions that occurred during this reporting period.
Burst Sessions	The total number of sessions that occurred after the provisioned capacity had been depleted.
Rejected	Total number of rejected sessions on this route during this reporting period.
System Rejected	The total number of rejected sessions by the ISR during this reporting period.
Account Rejected	The total number of rejected sessions by this account during this reporting period.
Route Rejected	The total number of rejected sessions by this route during this reporting period.
Recorded	Total number of recorded sessions on this route during this reporting period.
Percent Recording Rejected	Total number of sessions rejected during this reporting period because of the route's percent to record setting.

 **Note:**

This data is only available in a day by day breakdown.

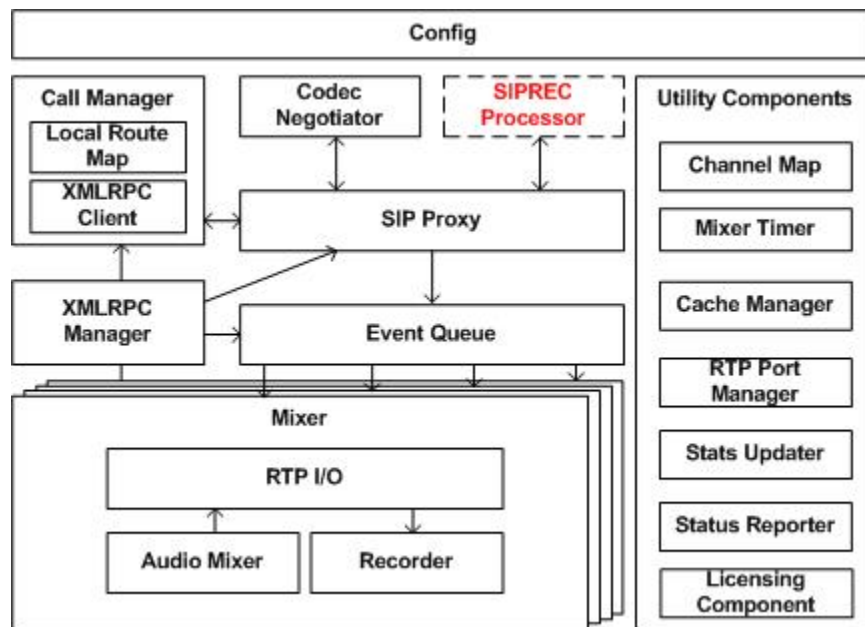
A

Software Diagrams and Call Setup Sequence

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 Recorder Process Architecture Diagram

The following is a diagram of the ISR recorder process 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.
- 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.
- 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).
 - 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 Index
- ISR User Dashboard
- ISR Monitor

- ISR FACE

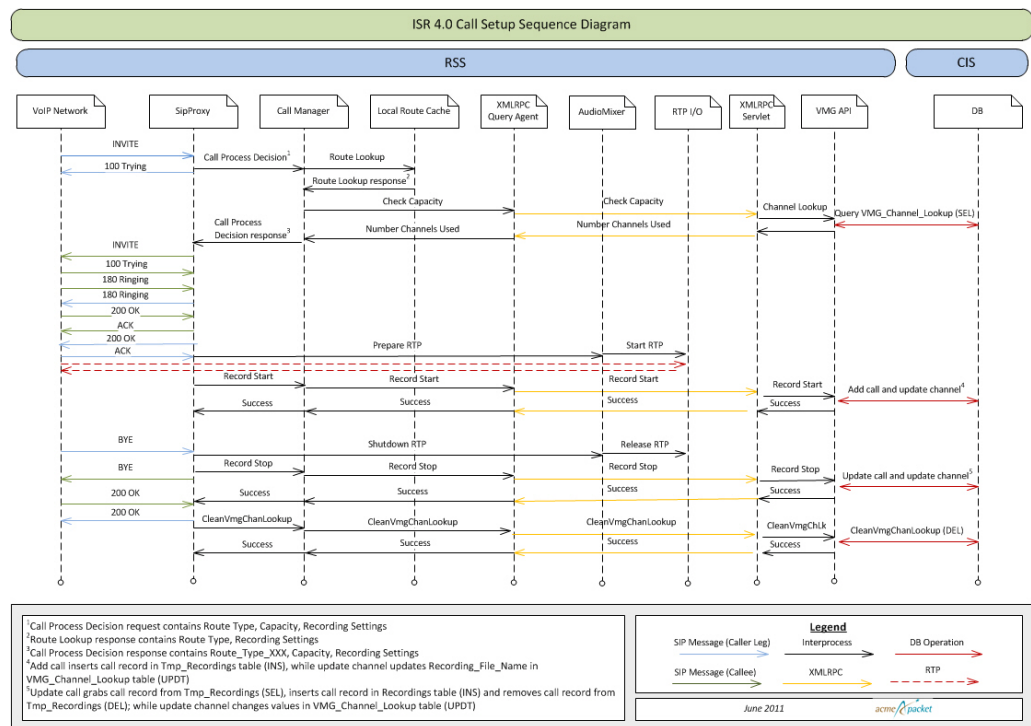
Sequence Diagrams

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.

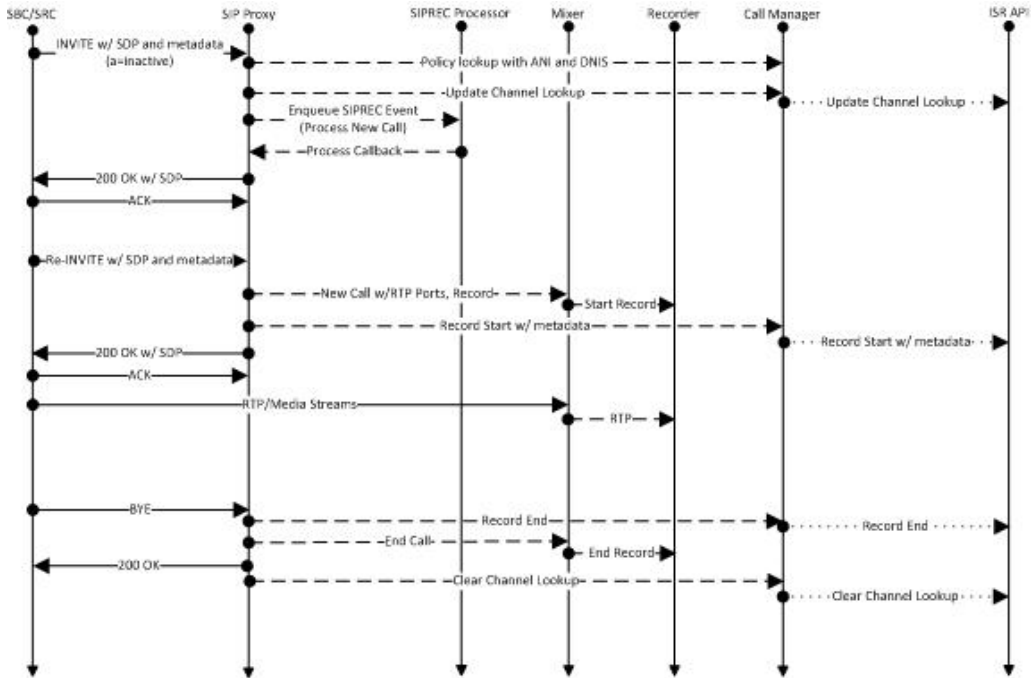
The simple call flow below reflects a single successful call which applies to a route configured for pass-through mode and recording of 100% of calls. The diagram highlights some of the features in the ISR, such as IVR-skip mode. Previously, the ISR architecture required a VoiceXML platform to make routing, recording and availability decisions. This information now resides locally in the Local Route Cache or is referenced in the database through API commands.



ISR Call Setup Sequence Diagram

SIPREC Call

The following sequence diagram applies to the ISR configuration in SIPREC environment.



B

ISR Linux Users and File Permissions

This section lists the ISR Linux Users and File Permissions.

Component	Type	File Name	Permissions	Owner
Recorder	log	/opt/isr/logs/ recorder/ ISRService.log	-rw-rw-rw-	isr
Recorder	log	/opt/isr/logs/ recorder/ recorder.log	-rw-r--r--	isr
Recorder	recordings	/opt/isr/ Recordings/*.*	-rw-rw-rw-	isr
Recorder	binary	/opt/isr/rss/isrl.elf	-rwxr-xr-x	isr
Converter	log	/opt/isr/logs/ converter/ converter.log	-rw-r--r--	isr
Converter	log	/opt/isr/logs/ converter/ converterService. log	-rw-r--r--	isr
Converter	binary	/opt/isr/rss/ converterl.elf	-rwxr-xr-x	isr
API	log	/opt/isr/logs/api/ api.log	-rw-r--r--	tomcat
API	config	/var/lib/tomcat/ webapps/IsrApi/ WEB-INF/ web.xml	-rwxr--r--	tomcat
API	code	/var/lib/tomcat/ webapps/ IsrApi/**/*.*	-rw-r--r--	tomcat
EEN	log	/opt/isr/logs/ ApiLog/ IsrApiEvent.log	-rw-r--r--	tomcat
Archiver	log	/opt/isr/logs/ Archiver/ ISRArchivalServi ce.log	-rw-r--r--	tomcat
Archiver	recordings	/opt/isr/ ArchivedRecordin gs/*.*	-rwxrw-r--	tomcat
Archiver	code	/var/lib/tomcat/ webapps/ ISRArchivalServi ce/**/*.*	-rw-r--r--	tomcat

Component	Type	File Name	Permissions	Owner
Archiver	config	/var/lib/tomcat/ webapps/ ISRArchivalService/ WEB-INF/ web.xml	-rw-r--r--	tomcat
RSS Web Server	log	/etc/tomcat/ server.xml	-rw-rw-r--	tomcat
RSS Web Server	log	/var/log/tomcat/ catalina.<yyyy- mm-dd>.log	-rw-r--r--	tomcat
RSS Web Server	log	/var/log/tomcat/ localhost_access _log.<yyyy-mm- dd>.txt	-rw-r--r--	tomcat
RSS Web Server	log	/etc/tomcat/ server.xml	-rw-rw-r--	tomcat
Dashboard	log	/var/log/puma/ puma.log	-rw-r--r--	puma
Dashboard	config	/opt/isr/puma/ puma_config.rb	-rw-r--r--	puma
Dashboard	binary	/usr/bin/puma*	-rw-r--r--	puma
Dashboard	siyrce	/usr/lib64/ruby/ gems/2.3.0/gems/ puma-3.4.0/**/*	-rw-r--r--	puma
Dashboard	log	/opt/isr/logs/ dashboard/ production.log	-rw-r--r--	puma
Dashboard	config	/var/www/ dashboard/ current/config/*.*	-r--r--r--	puma
Dashboard	source	/var/www/ dashboard/ current/app/**/*	-r--r--r--	puma
Face	log	/opt/isr/logs/Face/ Face.log	-rw-r--r--	tomcat
Face	config	/var/lib/tomcat/ webapps/Face/ WEB-INF/ web.xml	-rw-r--r--	tomcat
Face	code	/var/lib/tomcat/ webapps/ Face/**/*.*	-rw-r--r--	tomcat
Index	config	/etc/my.cnf	-rw-r--r--	mysql
Index	log	/var/lib/mysql/ index.err	-rw-r-----	mysql
Index	log	/var/log/ mysqld.log	-rw-r-----	mysql
Index	data	/var/lib/mysql/**/*	-rw-r--r--	mysql

ISR Third-Party Platform File Permissions

The following set of users are added to the "isr" group due to platform dependencies of the ISR applications.

- tomcat
- mysql
- puma

C

ISR Dashboard Database Failover

To support a high availability (HA) Index environment, the ISR Dashboard supports both primary and secondary production databases.

The Dashboard always attempts to connect to the primary Index first and the secondary database is only used when the Dashboard fails to connect to the primary database. If the Dashboard cannot connect to the secondary Index database, the ISR displays an error.

Configuring ISR Dashboard Database High Availability

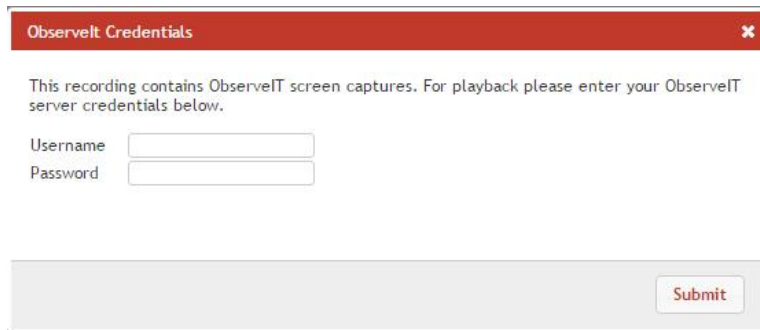
The Dashboard's `/opt/isr/configIsr.sh` script has two options which allow you to configure Dashboard database HA. After starting the script, select the **d** option to add or modify the secondary Index host database configuration. Select the **r** option to delete the secondary Index host database configuration. For either option, follow the on-screen options when prompted.

D

Logging Into ObserveIT Visual Session Recording

When the ISR Dashboard encounters a valid FACE configuration accompanied by a recording playback request with associated screen capture "slides", Dashboard playback functionality launches. This begins with a single request for ObserveIT Visual Session Recording credentials to authorize the ISR Dashboard session for screen capture playback.

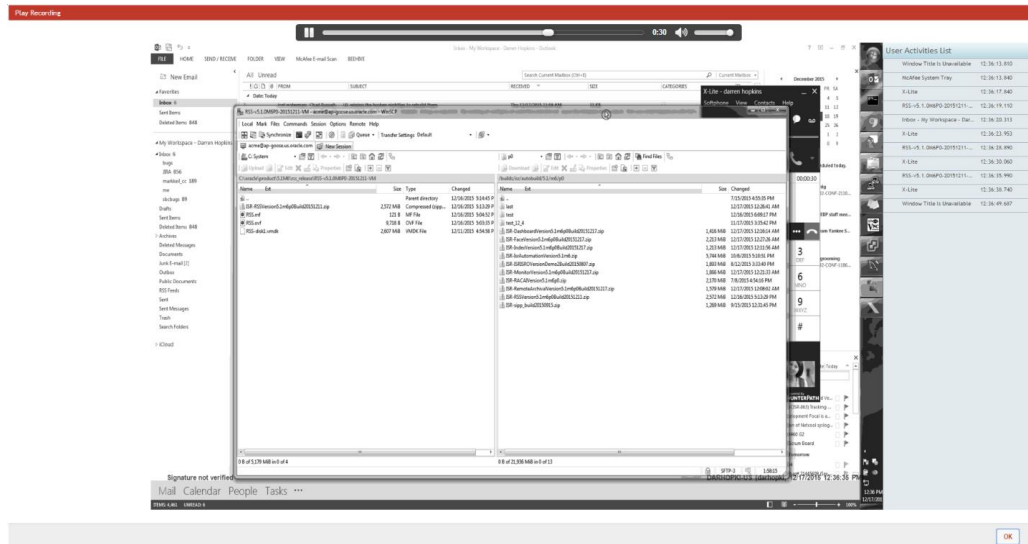
The following login screen appears prompting you for these credentials:



The image shows a login dialog box titled "ObserveIT Credentials". It contains the text: "This recording contains ObserveIT screen captures. For playback please enter your ObserveIT server credentials below." Below this text are two input fields: "Username" and "Password". At the bottom right of the dialog is a "Submit" button.

Once you successfully enter the **Username** and **Password**, both audio and screen capture video begin playing and a sliding bar appears with the controls for pause/resume and volume, as well as a display marking the current playback time within the recorded session. An interactive **User Activities List** panel also appears which contains a list of notable user events. By clicking on any of these items in the list, the recording jumps playback to the specified event.

The following example displays playback of audio and screen capture:



The image shows a screenshot of the ObserveIT playback interface. At the top, there is a "Play Recording" bar with a play button, a progress slider, and a "0:30" time display. Below this, the main window displays a Windows desktop environment. A "User Activities List" panel is visible on the right side of the screen, listing various user events with timestamps. The desktop background shows a Windows 7 desktop with a taskbar and several open windows, including a file explorer window showing a list of files and folders.

Click the **OK** button to return to the previous page once you are finished with playback.