Oracle® Communications Interactive Session Recorder

Administrator Guide

Release 5.1

Formerly Net-Net Interactive Session Recorder

December 2015

ORACLE

Contents

About this Guide

Overview

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

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

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

Audience

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

Supported SBC Platforms

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

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

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

Related Documentation

The following table lists related documents.

Document Name	Document Description
Interactive Session Recorder Release Notes	Contains information about new ISR features and fixed issues in the current release of the ISR.
Interactive Session Recorder Installation Guide, Release Version 5.0	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.

Document Name	Document Description
Interactive Session Recorder User's Guide	Contains information about using the ISR Dashboard for all levels of users. Provides information about viewing, playing, deleting recordings, running reports, managing user profiles (Super User, Account Administrator, and Tenant Administrator only).
Interactive Session Recorder API Reference Guide	Contains information about Methods for Recording, VoiceXML Commands, representational state transfer (REST) application programming interface (API), Recording File Types/Formats Supported, Return Codes, sendIPCRCommand.jsp Subdialog, Advanced Options, Troubleshooting.
Interactive Session Recorder Monitoring Guide	Contains information about installing and configuring the ISR Monitor. It also includes the Monitor database schema as well as the Monitor MIB.
Interactive Session Recorder Remote Archival Web Services Reference Guide	Contains information about the Remote Archival Web Service, its Control methods, WSDL definitions, DataType Definitions, sample responses to requests, and importing the Remote Archival Web Service's certificate into the client keystore.

Revision History

This section contains the revision history for this document.

Date	Release	Description
July 31, 2013	Revision 1.00	• Initial release of the ISR 5.1 software.
September 10, 2013	Revision 1.01	• Updates the Securing the ISR chapter.
September 11, 2013	Revision 1.02	• Updates editing the /opt/jboss/standalone/configuration/standalone.xml file in the Securing the ISR chapter.
October 31, 2013	Revision 1.03	• Updates commands in the SSL-Enabling the Remote Archival Webservice section.
November 20, 2013	Revision 1.10	• Changes Enabling Serving Pages with SSL section title to SSL-Enabling the ISR Dashboard and updates this section.
May 16, 2014	Revision 1.11	• Replaces NN-ISR with ISR. • Adds "Adding User Accounts on the RSS".
September 2014	Revision 1.12	• Updates the Securing the ISR chapter.
May 2015	Revision 1.20	• Adds "SSL-Enabling the RSS ISR API" section to the Securing the ISR chapter. • Updates the "SSL-Enabling the Remote Archival Webservice" section in the Securing the ISR chapter.

Date	Release	Description
August 2015	Revision 1.21	• Updates “Generating a PEM Format Keystore” section.
December 2015	Revision 1.21	• Adds the Interactive Session Recorder Remote Archival Web Services Reference Guide to the list of Related Documentation.

1 Overview

Introduction

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

About the ISR

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

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

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

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

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

SIPREC Support

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

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

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

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

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

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

About the ISR Dashboard

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

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

Requirements/ Recommendations

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

Browser Requirements

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

- Microsoft® Internet Explorer 9 (IE9) with full regression specifically on IE Version 9.0.8112.16421

- Mozilla Firefox® 8.0
- Google Chrome™ 16.0.912.63
- Other browsers (please contact Oracle Customer Service before using other browsers)

Recording Playback Recommendations

To listen to recordings, the following are recommended:

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

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

Security Features

The following security features have been implemented in the ISR:

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

ISR Third-Party Licensing

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

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

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

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

- more /cxc_common/ISR/LEGALTXT

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

2 Getting Started

Introduction

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

Logging In/Out of the ISR Dashboard

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

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

Email: isradmin@acmepacket.com

Password: admin123

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

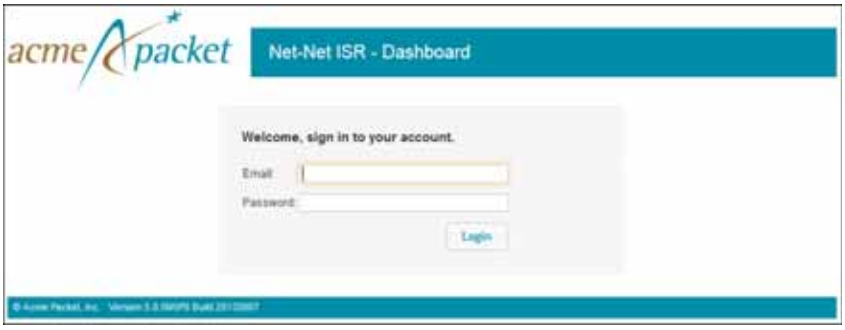
To login to the ISR Dashboard:

1. Open your Internet Web browser (see compatible browser requirements in the Requirements/Recommendations section.).
2. Enter the following URL in the URL field:

   ```
   http://<host name or IP>/
   ```

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

   The Login page displays.



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

   ```
   Email: isradmin@acmepacket.com
   Password: admin123
   ```

   On first-time login, the system prompts you to reset your password.
5. **New Password**—Enter a new password.

   Note: Your password must contain at least eight characters and one of the following characters in addition to lowercase letters: Capital letter and/or special character (e.g. @, #, $, etc.)
6. **Confirm Password—**Enter the same password again and click <**Update**>.

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

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

After changing your password, the ISR Dashboard Home page (default) displays.

The home page provides all of the options available to a user based on their user type.

This page allows you to perform the following:

Icon	Description
	Find Recordings (or "Recordings" in the main menu) — Allows you to view, play, delete and search recordings currently in the ISR database. Also allows you to download the recording metadata to a comma-separated value (CSV) file. For added convenience, after completing a recording search, you can save the search by assigning it a name. You can also create categories and add recordings to the category as applicable. **Note**: Displayed recordings are dependant on the level of logged in user. For more information about user levels, see User Access Levels. For more information about Recordings, see Manage Recordings.
	Build a Report (or "Reports" in the main menu) — Allows you to generate Usage and Billing reports for routes configured on the ISR. These reports display the information in a Bar Graph as well as in a Data Graph. **Note**: For more information about Reports, see Manage Reports.

Icon	Description
	**Edit My Settings (or "Settings" in the main menu) —** Allows you to view and edit the ISR Dashboard settings such as: • Preferred Time Zone • Page refresh rate (seconds) • Displayed number of recording entries per page • Specify the fields (columns) to display in a Recording search • Change your user login password **Note**: For more information about Dashboard settings, see Editing My Settings.
	**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: • Manager Realms • Manage Accounts • Manage Routes • Manage Authorization Services • Manage Users • Manage Sites • View live session information **Note**: Display of this feature is dependant on the level of logged in user. For more information about user levels, see User Access Levels. For more information about Administrator features, see Managing Realms/Accounts, Managing Routes, Managing Users, Managing Sites, Managing Authorization Services, and Viewing Live Sessions.

To logout of the ISR Dashboard:

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

User Access Levels

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

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

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. (Permissions to edit/delete must be assigned.)	Yes	Yes	Yes (Can manage all EXCEPT Super User and sites)
Tenant Administrator	View own recordings only. (Permissions to edit/delete must be assigned.)	Yes (Reports include info from own accounts only)	Yes	Yes (Can manage own Accounts, Routes, Tenant Admin, Tenant User only)

User Type	Find Recordings (Recordings)	Build Reports (Reports)	Edit My Settings (Settings)	Edit System Configurations (Admin)
Tenant User	View own recordings only. (Permissions to edit/delete must be assigned.)	Yes (Reports include info from own accounts only)	Yes	No
Remote Archiver User	N/A	N/A	N/A	N/A

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

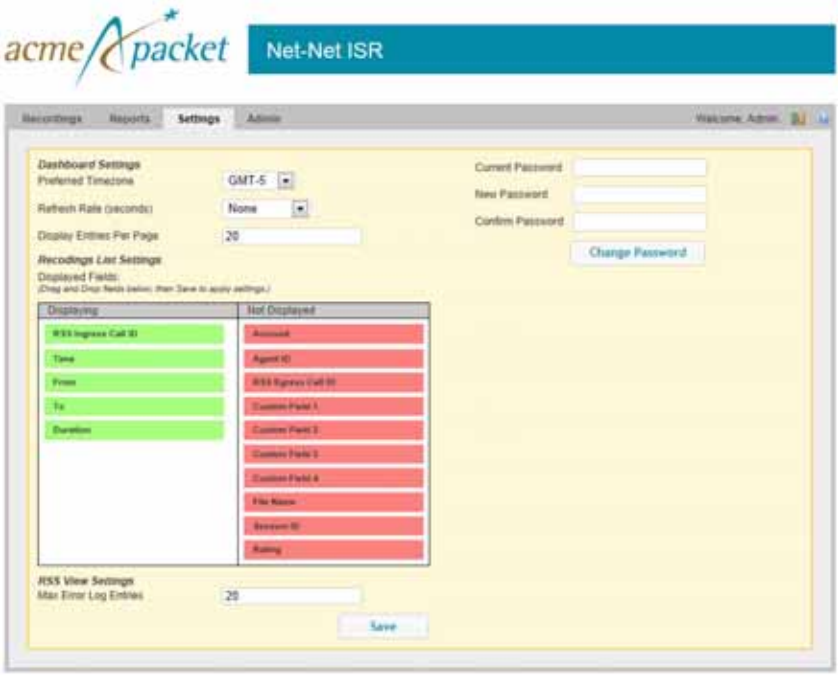
For more information about user login levels, see Chapter 6, Managing Users.

Editing My Settings

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

- Dashboard Settings
- Recordings List Settings
- RSS View Settings

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



Dashboard Settings

Using the Dashboard Settings, you can:

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

To configure the dashboard settings:

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

Time Zone Table

Time Zone	Location
GMT-11	NT - Nome
GMT-10	AHST - Alaska-Hawaii Standard CAT - Central Alaska HST - Hawaii Standard
GMT-9	YST - Yukon Standard

Time Zone	Location
GMT-8	**PST - Pacific Standard** Los Angeles, CA, USA
GMT-7	**MST - Mountain Standard**
GMT-6	**CST - Central Standard** Mexico City, Mexico Saskatchewan, Canada
GMT-5 (default)	**EST - Eastern Standard** Bogota Lima, Peru New York, NY, USA
GMT-4	**AST - Atlantic Standard** Caracas La Paz
GMT-3	Brasilia, Brazil Buenos Aires, Argentina Georgetown, Guyana
GMT-2	**AT - Azores**
GMT-1	**WAT - West Africa** Azores, Cape Verde Islands
GMT	London, England Dublin, Ireland Edinburgh, Scotland Lisbon, Portugal Reykjavik, Iceland Casablanca, Morocco
GMT+1	**CET - Central European** Paris, France Berlin, Germany Amsterdam, The Netherlands Brussels, Belgium Vienna, Austria Madrid, Spain Rome, Italy Bern, Switzerland Stockholm, Sweden Oslo, Norway
GMT+2	**EET - Eastern European** Athens, Greece Helsinki, Finland Istanbul, Turkey Jerusalem, Israel Harare, Zimbabwe
GMT+3	**BT - Baghdad** Kuwait Nairobi, Kenya Riyadh, Saudi Arabia Moscow, Russia
GMT+4	Abu Dhabi, UAE

Time Zone	Location
GMT+5	Kazakhstan (western-Aqtau) Maldives (Male) Pakistan (Islamabad, Karachi) Russia Tajikistan (Dushanbe) Turkmenistan (Ashkhabat) Uzbekistan (Tashkent) India (New Delhi, Calcutta) Sri Lanka (Colombo) Nepal (Katmandu)
GMT+6	Bangladesh Bhutan Kazakhstan Kyrgyzstan Sri Lanka (formerly Ceylon)
GMT+7	Cambodia Christmas Island Indonesia Lao Thailand Vietnam
GMT+8	**CCT - China Coast**
GMT+9	**JST - Japan Standard**
GMT+10	**GST - Guam Standard**
GMT+11	Solomon Islands
GMT+12	**IDLE - International Date Line East** **NZST - New Zealand Standard** Wellington, New Zealand Fiji Marshall Islands

2. **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

3. **Display Entries Per Page—**Enter the number of entries per page to display on the Recordings page. For example, entering a value of "7" in this field displays 7 recording entries per page in the Recordings List. Valid values are 1 to 255. Default is 10.
4. **Current Password—**Enter the current password you use to log into the Dashboard. Valid values are up to 256 alpha-numeric characters.
5. **New Password—**Enter your new password for logging into the Dashboard. Valid values are a combination of at least 8 characters and must include either one case-sensitive letter and/or special character (e.g. @, #, $, etc.).
6. **Confirm Password—**Reenter your new password to confirm the new Dashboard password.
7. Click **Change Password** to save the changes. A message, "*Successfully changed*" displays when the change is successful.

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, the following message displays: "*You must pick a password that you haven't recently used before.*"

8. Click **Save** to save the dashboard settings.

Recordings List Settings

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

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

To configure the Recordings List settings:

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

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

   Note: You can place a maximum of 5 headings in the "Displaying" column.

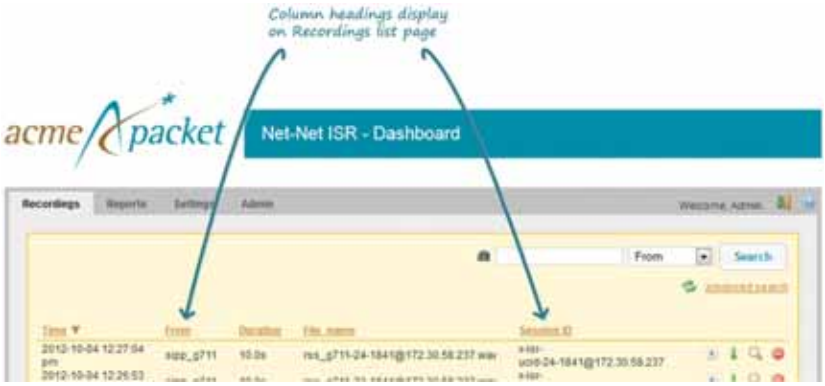
   The following table describes the headings you can select to display in the Recordings list.

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)
File Name	Displays the file name associated with the recording.
Session ID	Displays the Session ID derived from the X-ISR-UCID.
Agent ID	Displays the ID of the Agent answering the call.
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.

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

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

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



RSS View Settings

Using the RSS View Settings, you can:

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

To configure the RSS view settings:

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

Help Link

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

Clicking the Help link displays the following window.

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

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

Dashboard Tools

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

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

Functional Icons

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

Functional Icon	Description
	**Logoff** - 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.
	**Play** - Immediately opens and plays a "*.wav*" file recording stored in the ISR database. **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).
	**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.
	**Details** - Displays additional details about the item in the list. Some items allow for additional editing after clicking this tool.

Functional Icon	Description
	**View User Audit Trail** (managing User feature) - Displays details about the actions of the User in the ISR Dashboard. Information includes: • Time - Time of the action. • Action - Description of the action. • Object - User email ID of the User that was logged in when the action was performed. • IP Address - IP address that was accessed during 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->Display Entries per Page* parameter.

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

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

Search Tools

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

- Recordings
- Routes

Basic Search for Recordings

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

To perform a basic search for a recording:

1. Click **Recordings** in the main menu (or **Find Recordings** on the Home page). A list of recordings stored in the ISR database display.

2. In the drop-down box (at the top-right of the Recordings page), select the information about the recording(s) that you want to search. Valid values are:
   - From - ID of the caller for this call.
   - To - ID of the recipient for the call.
   - Session ID - Session ID derived from the X-ISR-UCID
   - File Name - File name of the recording. This is the file name assigned by the system or by the developer who invoked the recording.
   - Agent ID - ID of the agent that answered the call. This is the value set by the API, or by a User.
3. In the text box, enter the information required dependant on the selection you made in Step 2. Valid values are alpha-numeric characters.

   For example, if you selected “From” in the drop-down box, enter the ID of the caller associated with a recording for which you want to search. All the recordings associated with that caller ID display in a list.

   Note: You can select a recording and click on the Details icon to reference the “Session ID”, “From”, and “To” information for the recording if required.
4. Click <**Search**> to find all recordings based on the search criteria. All matching recordings display in the recordings list.

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

Advanced Search for Recordings

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

To perform an advanced search for a recording:

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

   The following dialog box displays.

2. **Search Mode—**Select whether to perform the search using **AND** or **OR**.

   - AND—Returns results where recordings match ALL fields you specify. For example, if you specify From as “123”, File Name as “Recording1”, and Agent ID as “2”, then the results of the search show all recordings with a value of “123” in the From field, AND file name of “Recording1”, AND Agent ID of “2”.
   - OR—Returns results where recordings match any one of the fields you specify. For example, if you specify From as “123”, File Name as “Recording1”, and Agent ID as “2”, then the results of the search show any recordings with a value of “123” in the From field, OR a file name of names or “Recording1”, OR an Agent ID of “2” (OR a a result that includes all of these).

3. **Partial Match**—When enabled, the ISR finds recordings that partially match the values entered in the search fields.
4. **Session ID—**Enter the unique Session ID derived from the X-ISR-UCID on which to perform the search.
5. **From—**Enter the From SIP URI to perform the search on. Valid values are alpha-numeric characters and may include the “@” or “:” characters.
6. **To—**Enter the To SIP URI to perform the search on. Valid values are alpha-numeric characters and may include the “@” or “:” characters.
7. **Label**—Enter the route label to perform a search on.
8. **Search Date—**Select whether you want to search for recordings **By Relative** or **By Range**:

   By Relative—Allows you to perform a recording search, based on the information you specified in the previous fields AND by recordings that happened “**Today**” (default), the “**Last 7 Days**”, or the “**Last 30 Days”**.

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

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

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

   Note: For convenience, clicking in the text box displays a pop-up calender 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.

2. **File Name—**Enter the file name of the recording. This is the file name assigned by the system or by the developer that invoked the recording. Valid values are alpha-numeric characters and may include the "@" or "." characters.
3. **Duration Min—**Enter the beginning time, in seconds, of a recording. Valid values are numeric characters. For example, 15.
4. **Duration Max—**Enter the ending time, in seconds, of a recording. Valid values are numeric characters. For example 24.

   Using the examples in Steps 3 and 4, the results include all recordings that had a length of time between and including 15 and 24 seconds.
5. **Agent ID—**Enter the ID of the agent that answered the call. This is the value set by the API or by a User. Valid values are alpha-numeric characters.
6. **RSS Ingress Call ID—**Enter the unique ingress call ID derived from the call-id received in the initial SIP INVITE.
7. **RSS Egress Call ID—**Enter the unique egress call ID derived from the call-id used in the egress call leg for the recording, if using pass-thru mode.
8. **Custom Field [1-4] Data—**Enter the unique set of metadata associated with the recordings for which you are searching. These fields identify the customized data defined by the API (for example, Transaction ID, Account Number, Unique Call ID, etc.). The results of this field display all recordings associated with the values you enter in this field(s). Valid values are alpha-numeric characters.
9. **Categories—**Enter the name of the category for which you want to search for recordings. The category you enter in this field must already exist in the database. Valid values are alpha-numeric characters. For more information about creating and searching categories, see Recording Details.
10. Click **Search** to find all recordings based on the search criteria. All matching recordings display in the recordings list.

Recording Search by Session

You can search for recordings by session criteria if required.

To search for recordings based on session criteria:

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

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

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

3. **Participant AOR—**Enter the participant's address of record (AOR) associated with the call that was recorded. Valid values are alpha-numeric characters.
4. **apkt:ucid—**Enter the Universal Call ID (UCID) of the incoming caller. Valid values are alpha-numeric characters.
5. **extTrackingID—**Enter the external tracking ID that was used when an incoming call was transferred to another recipient. Valid values are alpha-numeric characters.
6. **ServiceProviderID—**Enter the Service Provider ID that was used on the incoming call. Valid values are alpha-numeric characters.
7. **userID—**Enter the user ID on the incoming call. Valid values are alpha-numeric characters.
8. **groupID—**Enter the group ID on the incoming call. Valid values are alpha-numeric characters.
9. **callID—**Enter the call ID of the incoming call. Valid values are alpha-numeric characters.
10. **callingPartyNumber—**Enter the source number of the incoming call. Valid values are alpha-numeric characters.
11. **calledPartyNumber—**Enter the destination number of the incoming call. Valid values are alpha-numeric characters.

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

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

13. **apkt:in-realm—**Enter the name of the ISR realm that received the SIPREC session (in-realm). Valid values are alpha-numeric characters.
14. **apkt:P-Asserted-Identity—**Enter the remote party's ID in the SIPREC session. The ISR uses the P-Asserted-Identity header field to convey the proven identity of the originator of a request within a trusted network. Valid values are alpha-numeric characters.
15. **apkt:Diversion—**Enter the call forwarding phone number from the SIPREC session, to which the incoming call was diverted. Diversion is a call forwarding feature that lets an incoming call to a called party be redirected to a third party. Valid values are alpha-numeric characters.
16. **apkt:request-uri—**Enter the Uniform Resource Identifier (URI) in the header of the request message of the SIPREC session. The URI in the request message contains sufficient information to initiate and maintain the SIPREC communication session. Valid values are alpha-numeric characters.
17. Click **Search** to perform the search based on the recording session parameters you specified. All matching recordings display in the recordings list.

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

Basic Search for Routes

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

To perform a basic search for a route:

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

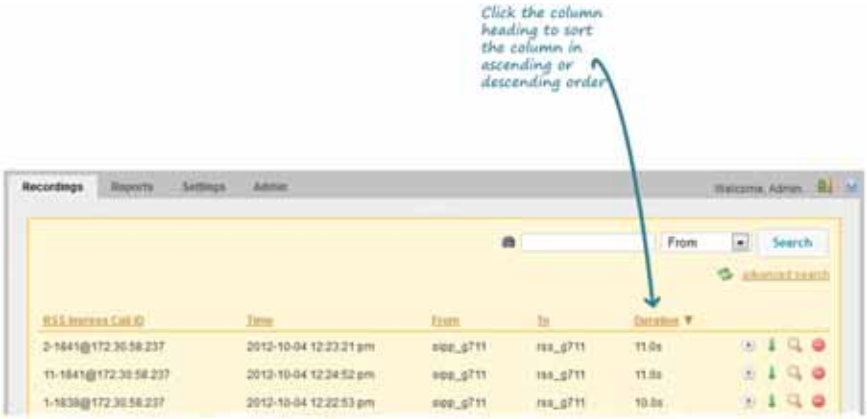
3. In the drop-down box (on the upper-left of the page), select the account for which you want to search for a route(s).

    Note: The values in the drop-down box include any accounts you've added to the ISR database.

4. In the text box (on the upper-right of the page), enter the route pattern for which to search. This field does not support partial matches.
5. Click **Search** to perform the search based on the criteria you specified. All matching routes display in the routes list.

Column Sorting Tool

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



To sort the recording data in the recording list:

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

Download Tool

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

Downloading a Single Recording File

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

To download a single recording file:

1. Click **Recordings** (or **Find Recordings** on the Home page). The recordings list displays.

2. Select a recording and click the Download icon for that recording. The following dialog box displays.

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

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

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

   "*rss_g711-24-1841@172.30.58.237.**(1)**wav*",

   "*rss_g711-24-1841@172.30.58.237(**2**).wav*",

   "*rss_g711-24-1841@172.30.58.237(**3**).wav*", etc.

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

Downloading a Recording List to a CSV File

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

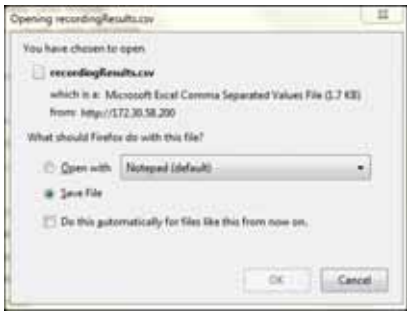
Note: This feature limits the download to 10,000 recordings. Therefore, if the Recordings List exceeds 10,000 recordings, you must perform a search to create a list of results containing less then 10,000 recordings before downloading to a CSV file.

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

1. On the Recordings page, click **Download as CSV file** to download the current list of recordings to a CSV file.
2. **Include Details**—Place a checkmark in the check box to include all details about the recording in the CSV file.

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

The following dialog box displays.



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

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

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

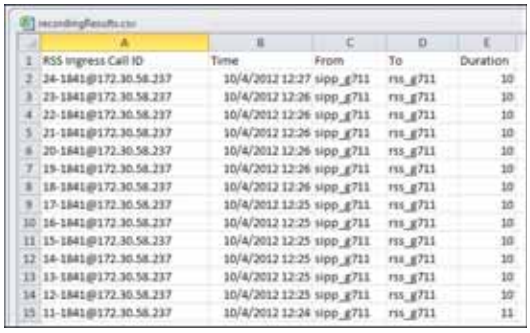
   "*recordingResults(1).csv*"

   "*recordingResults(2).csv*"

   "*recordingResults(3).csv*"

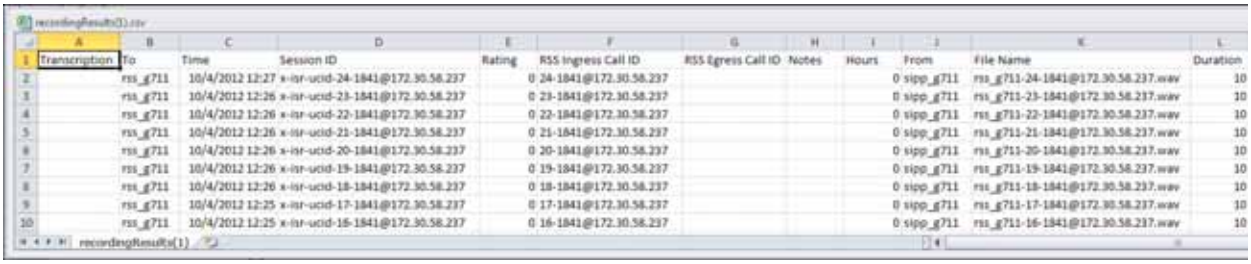
4. Click **OK**. The CSV file opens with the application you specified, or saves the file to your PC for viewing later.

   Example CSV file with recordings and no detail specified



	A	B	C	D	E
1	RSS Ingress Call ID	Time	From	To	Duration
2	24-1841@172.30.58.237	10/4/2012 12:27	sipp_g711	rss_g711	10
3	23-1841@172.30.58.237	10/4/2012 12:26	sipp_g711	rss_g711	10
4	22-1841@172.30.58.237	10/4/2012 12:26	sipp_g711	rss_g711	10
5	21-1841@172.30.58.237	10/4/2012 12:26	sipp_g711	rss_g711	10
6	20-1841@172.30.58.237	10/4/2012 12:26	sipp_g711	rss_g711	10
7	19-1841@172.30.58.237	10/4/2012 12:26	sipp_g711	rss_g711	10
8	18-1841@172.30.58.237	10/4/2012 12:26	sipp_g711	rss_g711	10
9	17-1841@172.30.58.237	10/4/2012 12:25	sipp_g711	rss_g711	10
10	16-1841@172.30.58.237	10/4/2012 12:25	sipp_g711	rss_g711	10
11	15-1841@172.30.58.237	10/4/2012 12:25	sipp_g711	rss_g711	10
12	14-1841@172.30.58.237	10/4/2012 12:25	sipp_g711	rss_g711	10
13	13-1841@172.30.58.237	10/4/2012 12:25	sipp_g711	rss_g711	10
14	12-1841@172.30.58.237	10/4/2012 12:25	sipp_g711	rss_g711	10
15	11-1841@172.30.58.237	10/4/2012 12:24	sipp_g711	rss_g711	11

Example CSV file with recordings and detail specified



Transcription	To	Time	Session ID	Rating	RSS Ingress Call ID	RSS Egress Call ID	Notes	Hours	From	File Name	Duration
	rss_g711	10/4/2012 12:27	x-isr-ucid-24-1841@172.30.58.237	0	24-1841@172.30.58.237			0	sipp_g711	rss_g711-24-1841@172.30.58.237.wav	10
	rss_g711	10/4/2012 12:26	x-isr-ucid-23-1841@172.30.58.237	0	23-1841@172.30.58.237			0	sipp_g711	rss_g711-23-1841@172.30.58.237.wav	10
	rss_g711	10/4/2012 12:26	x-isr-ucid-22-1841@172.30.58.237	0	22-1841@172.30.58.237			0	sipp_g711	rss_g711-22-1841@172.30.58.237.wav	10
	rss_g711	10/4/2012 12:26	x-isr-ucid-21-1841@172.30.58.237	0	21-1841@172.30.58.237			0	sipp_g711	rss_g711-21-1841@172.30.58.237.wav	10
	rss_g711	10/4/2012 12:26	x-isr-ucid-20-1841@172.30.58.237	0	20-1841@172.30.58.237			0	sipp_g711	rss_g711-20-1841@172.30.58.237.wav	10
	rss_g711	10/4/2012 12:26	x-isr-ucid-19-1841@172.30.58.237	0	19-1841@172.30.58.237			0	sipp_g711	rss_g711-19-1841@172.30.58.237.wav	10
	rss_g711	10/4/2012 12:26	x-isr-ucid-18-1841@172.30.58.237	0	18-1841@172.30.58.237			0	sipp_g711	rss_g711-18-1841@172.30.58.237.wav	10
	rss_g711	10/4/2012 12:25	x-isr-ucid-17-1841@172.30.58.237	0	17-1841@172.30.58.237			0	sipp_g711	rss_g711-17-1841@172.30.58.237.wav	10
	rss_g711	10/4/2012 12:25	x-isr-ucid-16-1841@172.30.58.237	0	16-1841@172.30.58.237			0	sipp_g711	rss_g711-16-1841@172.30.58.237.wav	10

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

Column Heading	Description
To	Specifies the To SIP URI. This is the URI from where the call session was coming.
Time	Specifies the starting GMT time and date of the recording in the format MM/DD/YY HH:M:SS, respectively. **Note**: In the date format, M = month, D = day, and Y = year. In the time format, H = hours, M = minutes, S = seconds.
Session ID	Specifies the Session ID assigned to the incoming call. Format is 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 milliseconds).
Custom Fields 1 - 4	Specifies a unique set of meta-data associated with the recording (i.e., Transaction ID, Account Number, Unique Call ID).
Completed	Specifies whether or not this recording resulted in a complete transaction, added by the dashboard user.
Agent ID	Specifies the ID of the Agent answering the call.

Import Tool

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

Note: The import tool is for Super User and Account Administrators only.

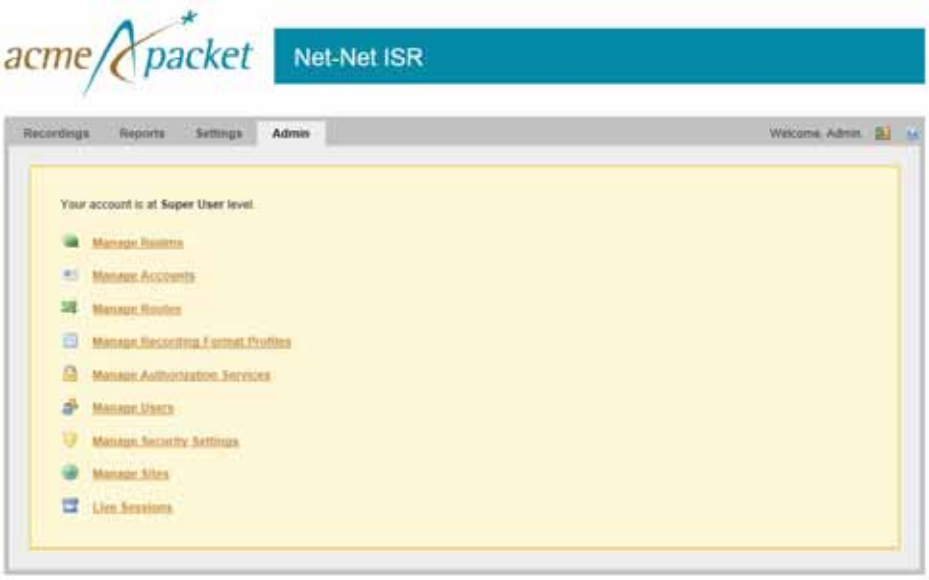
3 Managing Realms/Accounts

Introduction

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

Administrator Menu

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



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

The following table describes the Administrator features available for each level of administrator.

Administrator Menu by User Level

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

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

Manage Realms

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

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

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

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

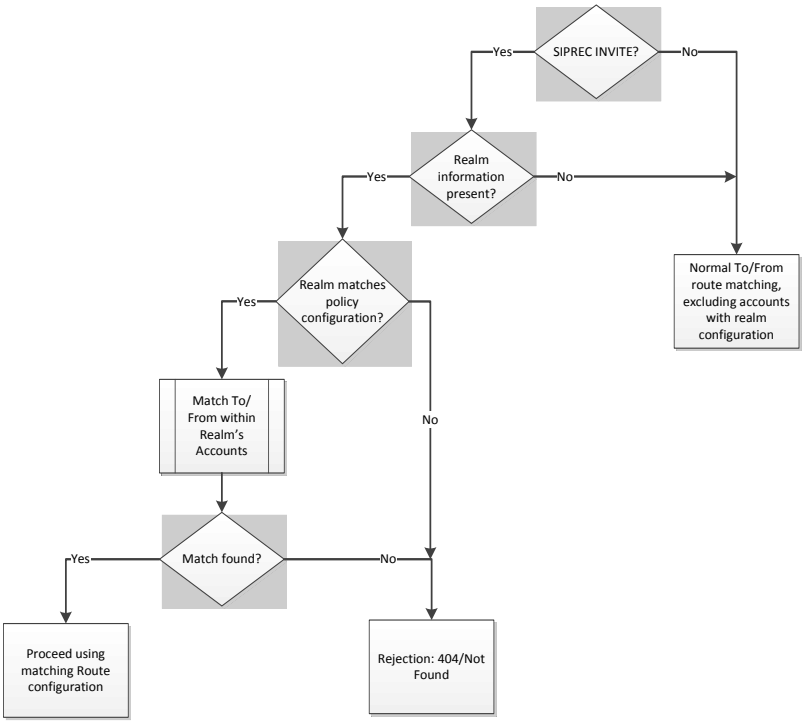
> **Note:** The configured realm must already exist in the SBC before adding it to the ISR.

How Realm-based Recording Works

The ISR performs recording affiliation and route-matching based on the configured route pattern and the associated realm. The ISR only inspects incoming SIPREC INVITEs for the inclusion of a realm label within the SIPREC extension data. If a realm label exists, it is used to search any configured routes associated with an account(s) in the matching

realm. The RSS looks for a To/From match (similar to the way lookups are performed) in the realm's configured accounts and routes.

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



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

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

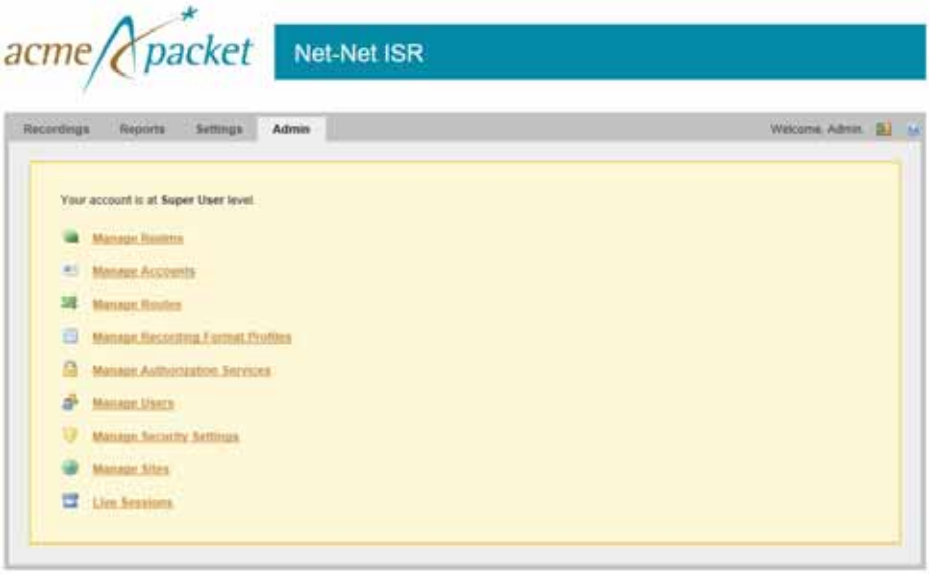
In Realm **edit** view, the associated account(s) in the realm display. In the Accounts edit view, the realm(s) associated with the account display only after adding an associated realm(s) to the ISR.

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

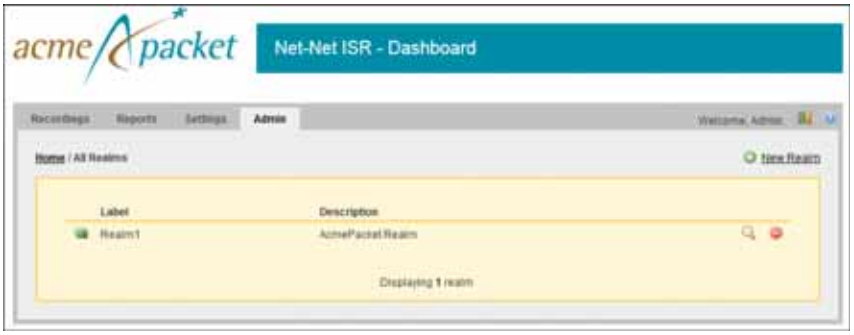
- You can associate multiple accounts to a single realm. Routes created on these accounts must have unique route patterns across the related accounts.
- Wildcard routes:
  - are treated like normal 'pattern' routes. They are unique across realms and accounts.
  - can have any priority.
  - if set with a higher priority than a 'distinct' route, the Dashboard displays a warning that the user is about to set a wildcard route higher than the list of lower priority routes, and prompts the user to confirm whether or not to continue.
- You cannot configure wildcard realms.

- Associating a realm with an account(s) is optional. Routes created across accounts with no realms must be unique. This allows the ISR to support legacy (non-SIPREC) installations, as well as maintain compatibility with other SIPREC compliant Session Recording Clients (SRCs).

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



Realms Page



The following table describes the columns on the Realms page.

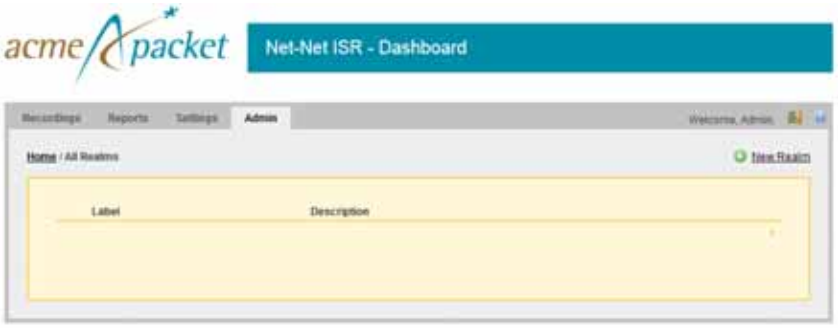
Column	Description
Label	Label name assigned to the Realm.
Description	Description of the Realm.
	Displays details about a Realm and allows you to edit the details if required.
	Deletes the Realm.

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.

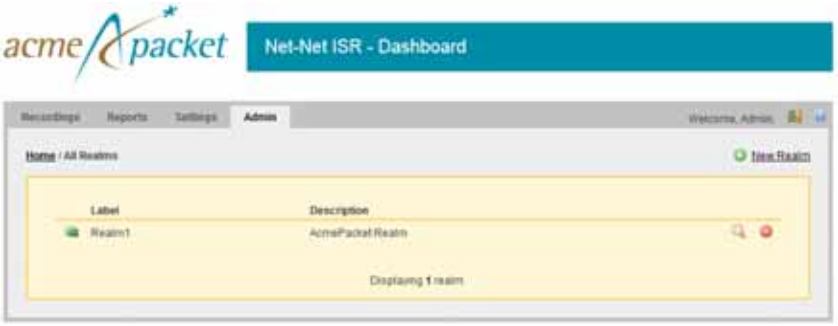
To add a realm:

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



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

4. **Label**—Enter the name of the realm to add to the ISR database. Valid values are alpha-numeric characters.
5. **Realm Description**—(optional)Enter a description for the realm you are adding. Valid values are alpha-numeric characters.
6. Click **Create**. The realm you added displays in the Realms page.

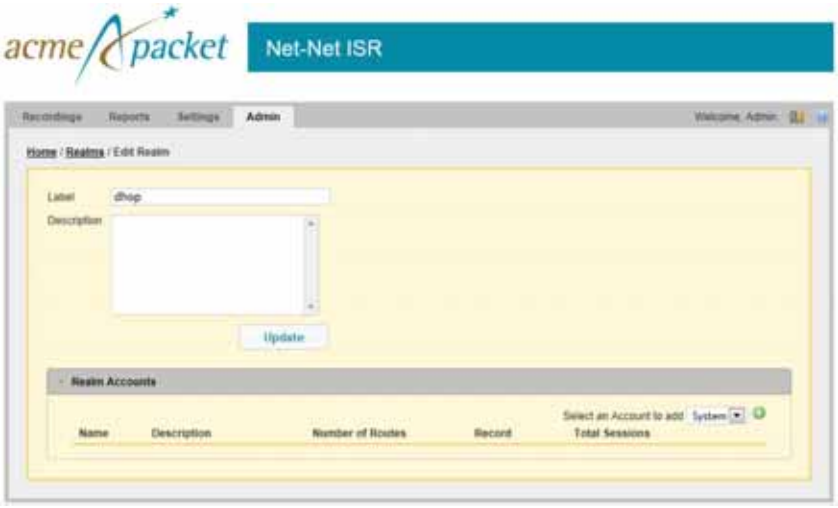


Associating an Account to a Realm

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

To associate an account to a realm:

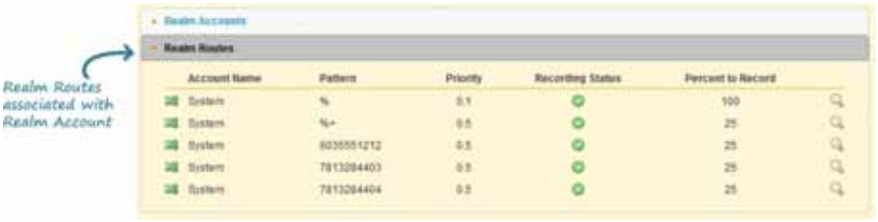
1. On the Realms page, select a realm and click the Details icon. The Edit Realm dialog box displays.



2. Click **Realm Accounts** to expand the realms page.
3. **Select an Account to add**—Select an account from the drop-down box and click the Add icon. The following prompt displays.

   "*Are you sure you want to add this account?*"
4. To add the account to the realm, click **Yes, Continue** or to cancel the add function, click the **X** in the upper-right corner of the prompt box.

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



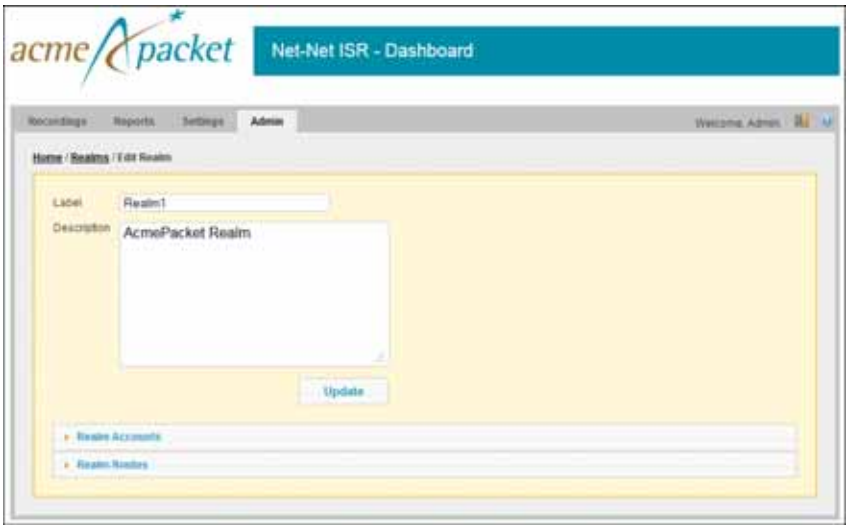
   You can edit these routes if required. For more information about editing routes, see Configuring/Editing Details of a Route.

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 dialog box displays.



2. **Label**—Edit the name of the realm. Valid values are alpha-numeric characters.
3. **Realm Description**—Edit the description of the realm. Valid values are alpha-numeric characters.
4. Click **Update**. The following message displays when an updated is successful.

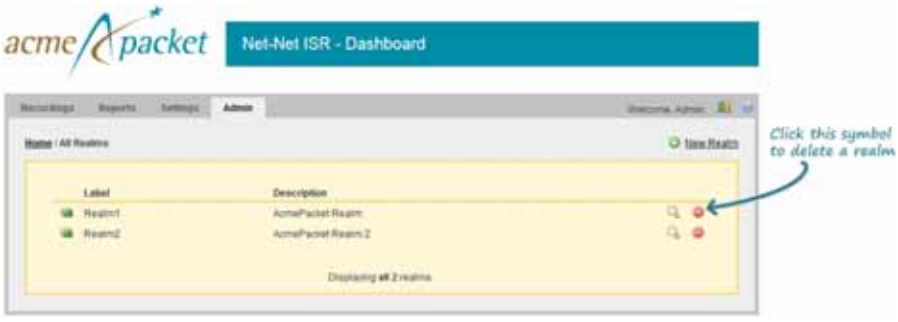
   "*Applied updated successfully*".

Deleting a Realm

You can delete a realm if required.

To delete a realm:

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



   The following message displays:

   "*Are you sure you want to delete this Realm?*"

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

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

Manage Accounts

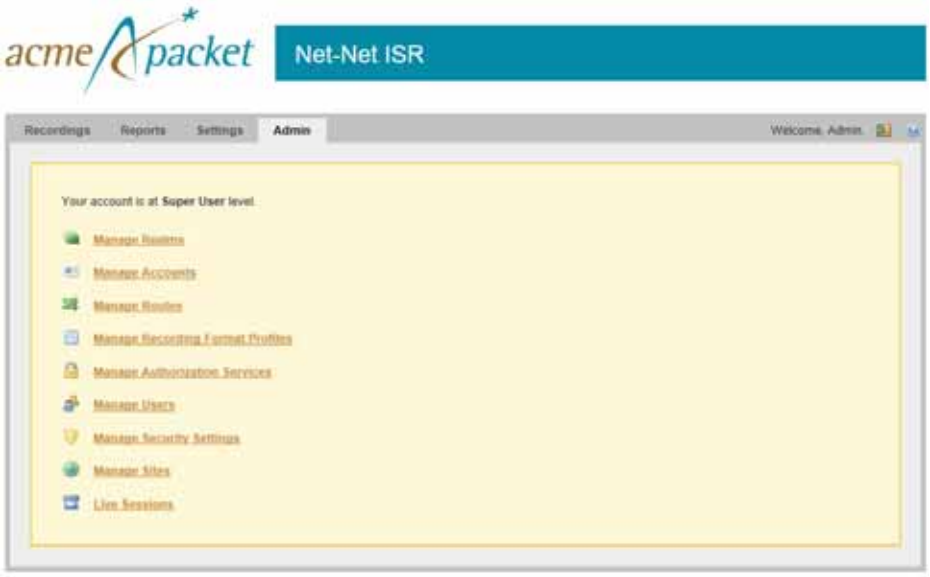
Use the **Manage Accounts** on the Admin Menu of the ISR Dashboard to manage accounts in the ISR network.

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

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

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

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



Accounts Page

The following table describes the columns 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.
Record	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.

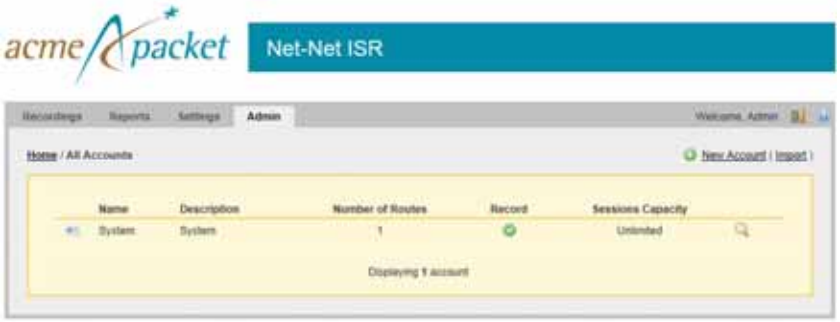
> **Note:** You can create an account using any application that can save to a comma separated value (CSV) file (i.e., Microsoft® Excel, Notepad®, etc.). Using the ISR Dashboard, you can then import the account information from the file (<*filename*>.*csv*) to the ISR database.

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

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

To add an account:

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



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

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

   Note:

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

Configuring/ Editing Details for an Account

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

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

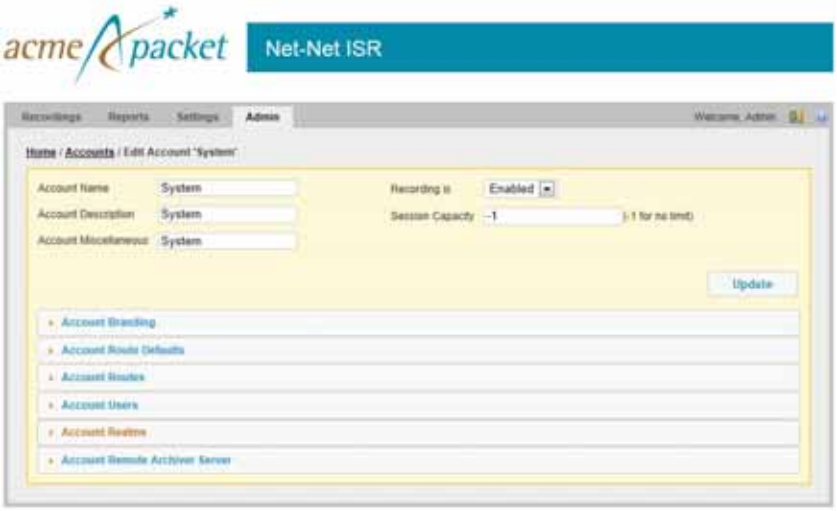
- Edit general account information
- Configure or edit branding features to the account
- Configure or edit account route defaults
- View the routes associated with the account (if any)

Edit General Account Information

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

To edit the general account information:

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



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

   Note:

   - The maximum session limits for an Account are subject to your licensing agreement.
   - After you create an account, you can set the “Additional Burst Sessions” available for routes to use after the maximum number of sessions have been used up. For more information about setting Additional Burst Ports, see Route Capacity Defaults.

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

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

Account Branding

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

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

To apply branding to an account:

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

4. In the **Header/Footer Color** field, click on  and select the company color to apply to the Header and Footer, as well as all the button names in the ISR Dashboard. Or enter the Company's color code, in Hex format, in the text box. For example, #F4AB00.
5. **Logo**—Enter the file name of the Company logo you want to apply to the header of all the screens in the ISR Dashboard. If required, you can specify the path name where the file is currently stored. For example, *images/Company.png.*
6. **Admin Help**—Enter any help information that you want to display when an Administrator clicks the Help icon from any page in the ISR Dashboard. Valid values are alpha-numeric text characters or HTML code. For example:

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

   The default message in the ISR is:

   "Online Support is available for this product.

   For questions and problems that cannot be answered by our documentation, please open a ticket through the Oracle Support Portal:

   https://support.acmepacket.com".

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

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

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

   The default message in the ISR is:

   "Online Support is available for this product.

   For questions and problems that cannot be answered by our documentation, please open a ticket through the Oracle Support Portal:

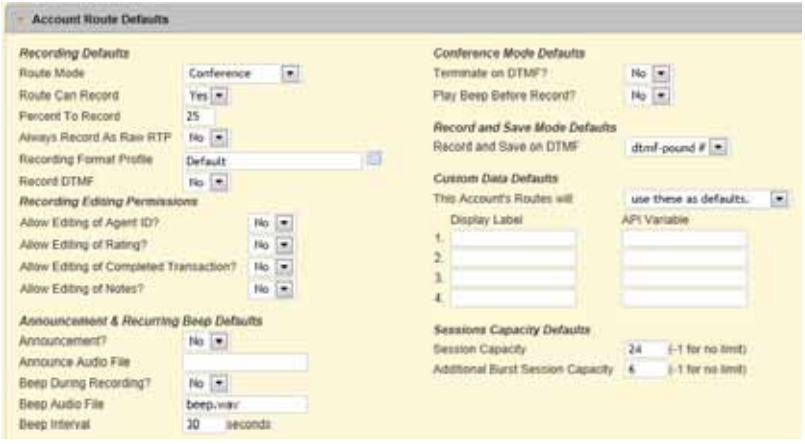
   https://support.acmepacket.com".

8. **Max Recording Entries in List View**—The maxinum number of recording entries that the Dashboard searches for in the Recordings List View. The default value is **10000**.
9. **Max Recording Entries in CSV Download**—The maximum number of recording entries that the Dashboard searches for when preparing a CSV file for download. The default value is **10000**.
10. Click **Preview** to verify the color and logo changes before saving.
11. Click **Update** to save the changes. The color and logo you specify display on the screens in the ISR Dashboard. The following screen illustrates the branding configuration.

Account Route Defaults

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

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



Recording Defaults

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

To configure recording defaults:

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

   Note: Choosing the correct application type is critical to the ISR performance.
5. **Route Can Record**—Select whether or not calls on this route are recorded. Valid values are:
   - Yes (default) - Recording is enabled for all calls on this route.
   - No - Recording is disabled for all calls on this route.

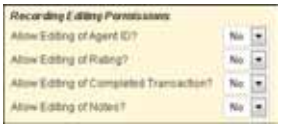
   Use this field to enable/disable recordings on a specific route.
6. **Percent to Record**—Specify a value for the percentage of calls to record on this route. Default is 25. Valid values are:
   - 0 to 100
7. **Always Record As Raw RTP**—Select **Yes** when multiple transmission codecs are present in a session. If set to **No** with multiple transmission codecs present in a session, the ISR does not record the call properly.
8. **Recording Format Profile**—Select the recording format profile you want to assign to this account. The default value is **Use System Account's Profile**.

Recording Editing Permissions

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

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

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



To set recording editing permissions:

1. **Allow Editing of Agent ID?**—Select whether or not you want users for this route to edit the Agent ID for a recording. Valid values are:
   - Yes - Allow editing of Agent ID for a recording.
   - No (default) - Prevent editing of Agent ID for a recording.
2. **Allow Editing of Rating?**—Select whether or not you want users for this route to edit the Rating assigned to a recording. Valid values are:
   - Yes - Allow editing of rating for a recording.
   - No (default) - Prevent editing of rating for a recording.
3. **Allow Editing of Completed Transaction?**—Select whether or not you want users for this route to edit a recording transaction that has been completed. Valid values are:
   - Yes - Allow editing of completed transaction information for a recording.
   - No (default) - Prevent editing of completed transaction information for a recording.
4. **Allow Editing of Notes?**—Select whether or not you want users for this route to edit the Notes specified for a recording. Valid values are:
   - Yes - Allows editing of notes specified for a recording.
   - No (default) - Prevent editing of notes specified for a recording.

Announcement and Recurring Beep Defaults

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

To configure announcements and recurring beep defaults:

1. **Announcement?**—Select whether or not an audio announcement is played for this route before the caller is directed to their end destination (for example, "*Your call will be monitored or recorded.*") Valid values are:
   - Yes - Allows announcement to play before call is redirected to destination.
   - No (default) - Prevents announcement from playing before call is redirected to destination.
2. **Announce Audio File**—(optional)Enter the URL where the file is located, that you want to use as the default announcement file to play for all calls to this account. The filename must have a "*.wav*" extension (for example, *announcement.wav*) AND must be in 8 bit 8kHz ulaw format to guarantee proper playback.

   Note: If providing a custom announce audio file, the file must be an 8-bit 8kHz *.wav* file, and be placed in your ISR install directory (*/cxc_common/ISR/Cache/*).
3. **Beep During Recording?**—(optional)Select whether or not an audio tone is played during the recording of a call on a recurring basis to indicate the call is being recorded. Valid values are:
   - Yes - Allows an audio tone to play during the recording of a call on a recurring basis as the call is recorded.
   - No (default) - Prevents an audio tone from playing during the recording of a call.
4. **Beep Audio File—**(optional) When the **Beep During Recording?** field is set to **Yes**, Enter the name of the file that contains a customized audio tone that you want to play during the recording of a call on a recurring basis to indicate the call is being recorded. The filename must have a "*.wav*" extension (for example, *beep.wav*). Default is *beep.wav*.

   Note: If providing a custom audio tone, the file must be an 8-bit 8kHz *.wav* file and be placed in your ISR install directory (*/cxc_common/ISR/Cache/*).
5. **Beep Interval—**(optional) When the **Beep During Recording?** field is set to **Yes**, specify the amount of time, in seconds, between each recurring beep tone. Default is 30. Valid values are:
   - 1 through 9999

Conference Mode Defaults

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

To set the conference mode default:

1. **Terminate on DTMF?—**Select whether or not a recording should stop when a Dual-tone Multi-frequency (DTMF) (keypress) is received. Valid values are:
   - Yes - Allows a recording to stop when a DTMF tone is received.
   - No (default) - Prevents a recording from stopping when a DTMF tone is received.
2. **Play Beep Before Record?—**Select whether or not an audio tone plays to alert the caller that a recording is about to start. Valid values are:
   - Yes - Allows an audio tone to play to alert the caller that a recording is starting.
   - No (default) - Prevents an audio tone from playing before a recording starts.

Record and Save Mode Defaults

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

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

To set the record and save mode defaults:

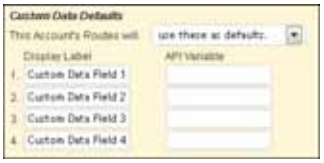
- **Record and Save on DTMF—**Select the type of keypress that allows the caller to save their recording from their phone's keypad. This parameter allows you to assign a specific DTMF key (keypress), that when pressed by the caller, stores the recording at their location. The value **disable dtmf** disables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

Custom Data Defaults

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

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

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



To set custom data defaults:

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

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

IF	THEN
you are a Super User or Account Administrator	you CAN set/change the "**This Account's Routes will**:" field for all accounts. you CAN specify/change the "**Display Label**" and "**API Variable**" for all accounts.
you are a Tenant Administrator	you CANNOT set/change the "**This Account's Routes will**:" field for your own accounts you CAN specify/change the "**Display Label**" and "**API Variable**" for your own accounts.

2. **Display Label**—(Optional) Enter the custom data label you want the route to use to identify custom data stored in this field. For example, enter "Billing" as a label to identify the route used for Billing. Valid values are alpha-numeric characters.
3. **API Variable**—(Optional) Enter the variable that the API uses to identify the "Display Label" field. The API variable must match the name passed in the API. For example, if the Display Label is "Billing", enter the API variable as **billing**. If the Display Label is "Account Number", enter the API variable as **accountnumber**. Valid values are alpha-numeric characters.
4. (optional) For the remaining **Display Label** fields and **API Variable** fields, repeat steps 2 and 3. You can specify up to 4 display labels and API variables.

Sessions Capacity Defaults

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

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

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

   Note:

   - The maximum session limits for an Account are subject to your licensing agreement.
   - The maximum session limit data is included in the Usage and Billing Reports. For more information about generating reports, see Chapter 10, Managing Reports.
2. **Additional Burst Session Capacity**—(Optional) Enter the number of additional call recording sessions available for the current account to use after the maximum number of sessions has been depleted. Default is 6. Valid values are:
   - -1 to 999999999 (must indicate total number of licensed sessions)

- -1 indicates no limit (default)

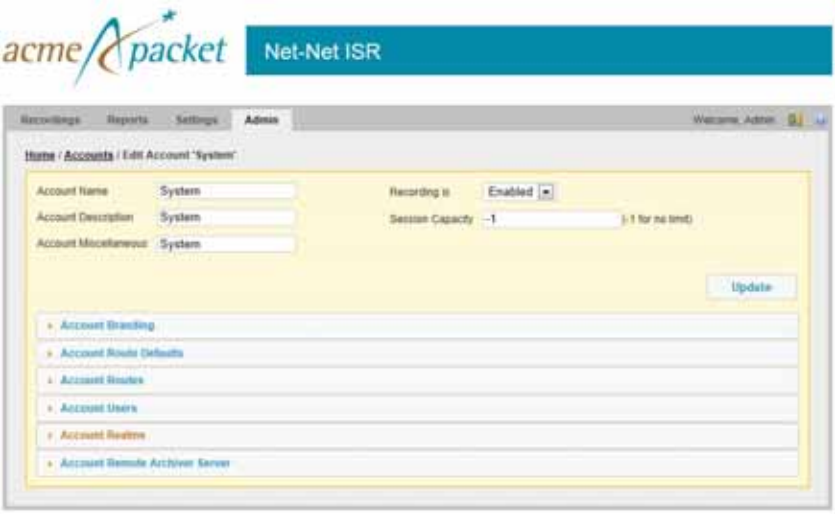
Note:

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

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

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

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



Account Routes

To view and edit routes associated with this account:

1. Click **Account Routes**.

   All routes associated with the account appear.

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

Account Users

To view and edit users associated with this account:

1. Click **Account Users**.

All users associated with the account appear.

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

Account Realms

To view and edit realms associated with this account:

1. Click **Account Realms**.

   All realms associated with the account appear.

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

Account Remote Archiver Server

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

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

   The remote archiver server associated with the account appears.

2. **Client IP Address**—Enter the Remote Archival client's IP address.
3. **Remove Recordings**—When set to On, the files are deleted from the source RSS/NAS/SAN after a successful push. Valid values are **On** and **Off**. The default value is **Off**.
4. **Max Allowed Attempts**—The maximum number of attempts the Webservice client can can make when requesting a recording. The default value is **3**.
5. Click **Update**.

Deleting an Account

You can delete accounts in the ISR Dashboard as required.

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

To delete an account:

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

The following message and prompt displays.

"*Deleting this account will delete all recordings, routes, and user types associated with it!*

Are you sure you want to delete this account?"

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

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

Importing an Account CSV File

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

To import account information from a CSV file:

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

   Notes:

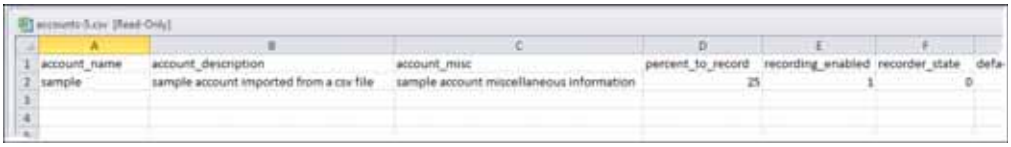
   - Boolean (yes/no) values must be entered using 0 (yes or enabled) and/or 1 (false or disabled).
   - All parameters must be entered with no spaces (use underscores instead of spaces).

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

Parameter Heading	Valid Values
account_name	alpha-numeric characters
account_description	alpha-numeric characters
account_misc	alpha-numeric characters
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
announce_enabled	0 | 1
default_announce_audio_text	alpha-numeric characters
custom_data_1_name	alpha-numeric characters
custom_data_1_friendly_name	alpha-numeric characters
custom_data_1_editable_flag	0 | 1
custom_data_2_name	alpha-numeric characters
custom_data_2_friendly_name	alpha-numeric characters
custom_data_2_editable_flag	0 | 1
custom_data_3_name	alpha-numeric characters
custom_data_3_friendly_name	alpha-numeric characters
custom_data_3_editable_flag	0 | 1
custom_data_4_name	alpha-numeric characters
custom_data_4_friendly_name	alpha-numeric characters
custom_data_4_editable_flag	0 | 1

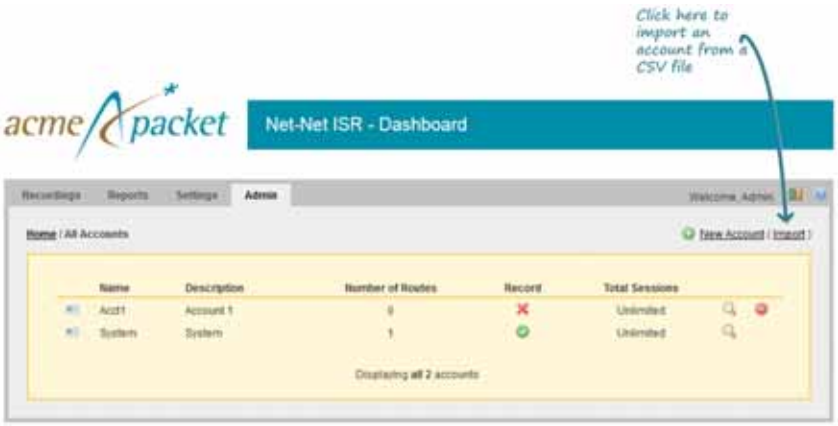
application	pass_through conference record_and_save call_parking vam_sip_test
maximum number of ports	digits (-1 for no limit)
number_of_burst_ports	digits (-1 for no limit)
acct_port_limit	digits

Example File with Parameters and Values



	A	B	C	D	E	F
1	account_name	account_description	account_misc	percent_to_record	recording_enabled	recorder_state
2	sample	sample account imported from a csv file	sample account miscellaneous information	25	1	0

2. Save the file as a <*filename*>*.csv* file (for example, *AccountB.csv*).
3. Login to the ISR Dashboard.
4. Click **Admin** in the main menu (or **Edit System Configurations** on the Home page).
5. Click **Manage Accounts**. The Accounts page displays.



6. Click **Import**. The following dialog box displays.

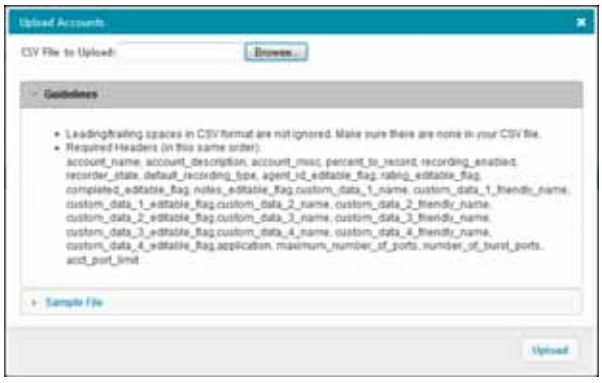
7. **CSV File to Upload—**Enter the name of the account CSV file you want to import into the ISR database. Valid values are alpha-numeric characters. For example, *Account1.csv*.

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

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

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

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



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

4 Managing Routes

Introduction

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

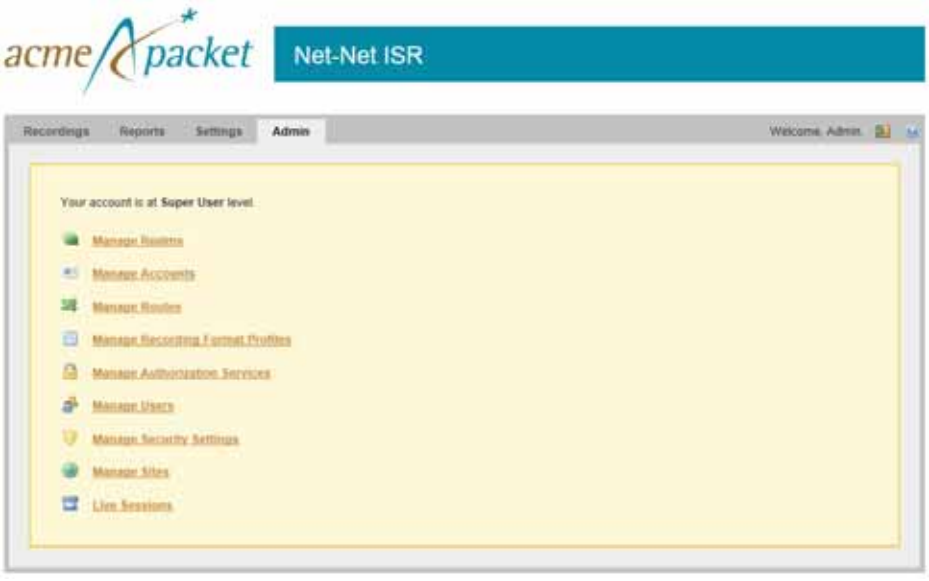
Manage Routes

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

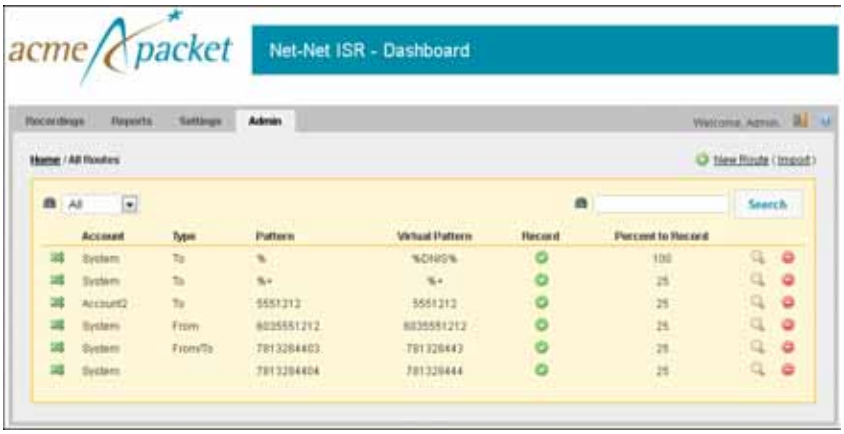
A route on the ISR defines the parameters to evaluate and invoke recording, as well as the recording rules to apply for all calls received by the ISR. You can set a specific account to have one route or multiple routes, depending on the subscriber's business requirements.

Note:

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



Routes Page



The following table describes the columns 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.
Virtual Pattern	Specifies the destination where the calls matching the route pattern are forwarded once recording rules have been evaluated.
Record	Identifies whether or not recording is enabled or disabled on the account. Recording is enabled. Recording is disabled.
Percent to Record	Percentage of calls that are allowed to be recorded on this route for this account. Valid values are 0% to 100%.
	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 **New Route** link on the Routes page. When adding a new route to an account, by default, the parameters on the Route page are defined from the focused account's Account page details. For example, if you are adding a route to Account A (which already exists with details configured), by default, the new route takes on the configured details from Account A.

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

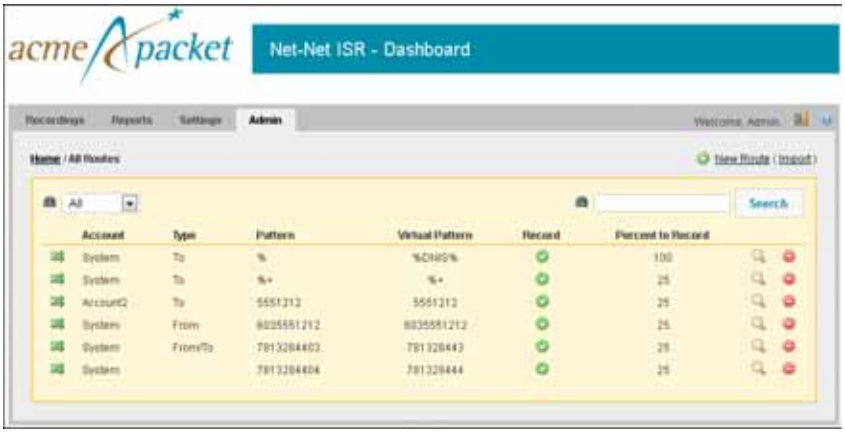
For more information about importing route information into the ISR database, see Chapter2, Importing a Route CSV File.

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

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

To add a route:

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



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

4. **Account**—Select the account name to associate with this new route. Valid values are dependent on the accounts currently configured in the ISR database, and the User's permission level. The default is **System**.

Note: Once a route is added and assigned to an account, it cannot be reassigned to other accounts. If you attempt to reassign a route to another account, the following message displays:

"*Another route with this pattern already exists.*"

5. **Route Type**—Select the type of route to use for this account. This field is used to compare with the value in the "Route Pattern" field. Valid values are:
   - **From** - The incoming call's From SIP URI is compared with the value in the "Route Pattern" field and must match.
   - **To** (default) - The incoming call's To SIP URI is compared with the value in the "Route Pattern" field and must match.
   - **From/To** - The incoming call's From and To SIP URIs are compared with the value in the "Route Pattern" field and both must match.
6. **Route Pattern**—Specify the route pattern to use for this account. This field is based on the "Route Type" selected in step 5 (the SIP URI that triggers this rule set). Use the route pattern value to match an incoming call's From, To or From/To value, and apply the appropriate rules of the route and account. For examples of route patterns, see Examples of Route Patterns.
7. **Virtual Route Pattern**—Clicking this field automatically updates the field with the value from the **Route Pattern** field. To change this value, specify the virtual route pattern to use for the current route. This value specifies the destination where the calls matching the route pattern are forwarded once recording rules have been evaluated. The Virtual Route Pattern is used in conjunction with the Session Agent defined in *Managing Sites*. A full SIP URI can be provided to override this value. Valid values for this field are alpha-numeric characters. For examples of virtual route patterns, see Examples of Route Patterns.

   Note: Use the **Virtual Route Pattern** field for application types of **Default Pass-Through** and **Record and Save** routes only.
8. **Route Label**—Enter a name to assign to this route. The route label replaces the "To" value for display so customers can switch the called number from the number given by their service provider, to one more familiar to the users. Valid values are alpha-numeric characters. The Route Label overrides the "From" value in the recordings view.
9. **Route Priority**—Select a priority to assign to this route. Routes with a higher priority number are matched before routes with a lower priority number. Valid values are **1** through **9**. Default is **5**.
10. Click **Create**. The new route displays on the Routes page.

Examples of Route Patterns

SIP INVITES arrive with the following information:

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

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

Example 1. You want to set up recording rules for calls that come in on a specific 800 number for your billing department, which are answered by a queue at extension 4334.

Since you are evaluating the address the call is sent TO. You need to know what To value your 800 number maps to in your telephony environment. Often, the To is the last 4 digits of the 800 number. To 1234 is the number used in the following example that the 800 number maps to.

a. Select the Account for which this route applies.

b. Select Route Type of **To**.

c. Set Route Pattern as **1234**.

d. Set Virtual Route Pattern to **4334**.

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

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

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

a. Select the Account for which this route applies.

b. Select Route Type of **From**.

c. Set Route Pattern as **3335551234**.

d. Set Virtual Route Pattern to **5445** (high priority queue).

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

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

a. Select the Account for which this route applies.

b. Select Route Type of **From/To**

c. Set Route Pattern as **8664441234/9988.**

d. Set Virtual Route Pattern to **5445** (high priority queue). To override the outbound Session Agent, use sip:5445@10.85.122.15:5060 which sends these calls out their own Session Agent.

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

a. Select the Account for which this route applies.

b. Select Route Type of **To**.

c. Set Route Pattern as **%**.

The % (wild card) indicates matching of all To values on the incoming calls. Any incoming call that matches a To uses the associated route to the call destination using the Virtual Route Pattern of **%To**.

Note: Wild card routes are typically set to a low priority in order to allow other routes with the same route type to be matched.

Configuring/ Editing Details of a Route

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

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

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

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

Edit General Route Information

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

To edit the general route information:

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

3. **Route Type**—Edit the type of route to use for this account. This field is used to compare with the value in the **Route Pattern** field. Valid values are:
   - **From** - The incoming call's From SIP URI is compared with the value in the "Route Pattern" field and must match.
   - **To** (default) - The incoming call's To SIP URI is compared with the value in the "Route Pattern" field and must match.
   - **From/To** - The incoming call's From and To SIP URIs are compared with the value in the "Route Pattern" field and both must match.
4. **Route Pattern**—Edit the route pattern to use for this account. This field is based on the "Route Type" selected in step 5 (the SIP URI that triggers this rule set). Use the route pattern value to match an incoming call's From, To or From/To value, and apply the appropriate rules of the route and account. For examples of route patterns, see Examples of Route Patterns.
5. **Virtual Pattern**—Clicking in this field automatically updates the field with the value from the **Route Pattern** field. To change this value, specify the virtual route pattern to use for the current route. This value specifies the destination where the calls matching the route pattern are forwarded once recording rules have been evaluated. The Virtual Route Pattern is used in conjunction with the Session Agent

defined in *Manage Sites*. A full SIP URI can be provided to override this value. Valid values for this field are alpha-numeric characters. For examples of virtual route patterns, see Examples of Route Patterns.

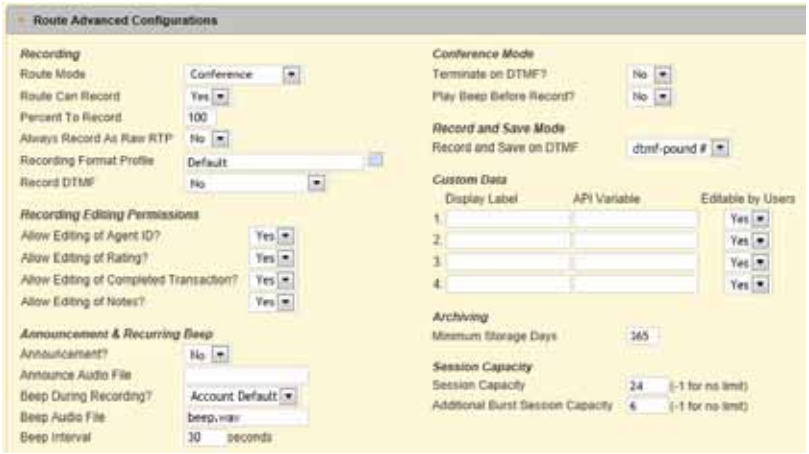
Note: Use the **Virtual Pattern** field for application types of **Default Pass-Through** and **Record and Save** routes only.

6. **Route Label**—Edit the name of this route. The route label replaces the "To" value for display so customers can switch the called number from the number given by their service provider, to one more familiar to the users. Valid values are alpha-numeric characters. The Route Label overrides the "From" value in the recordings view.
7. **Route Priority**—Edit the priority for this route. Routes with a higher priority number are matched before routes with a lower priority number. Valid values are **1** through **9**. Default is **5**.
8. Click **Update** to save the changes.

Route Advanced Configurations

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

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



Recording

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

Recording Editing Permissions

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

Announcement and Recurring Beep

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

Conference Mode

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

Record and Save Mode

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

Custom Data

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

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

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

To set custom data defaults:

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

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

IF	THEN
you are a Super User or Account Administrator	you CAN set/change the "**This Account's Routes will**:" field for all accounts. you CAN specify/change the "**Display Label**" and "**API Variable**" for all accounts.
you are a Tenant Administrator	you CANNOT set/change the "**This Account's Routes will**:" field for your own accounts you CAN specify/change the "**Display Label**" and "**API Variable**" for your own accounts.

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

3. **API Variable**—(optional) Enter the variable that the API uses to identify the "Display Label" field. The API variable must match the name passed in the API. For example, if the Display Label is "Billing", enter the API variable as **billing**. If the Display Label is "Account Number", enter the API variable as **accountnumber**. Valid values are alpha-numeric characters.
4. **Editable by Users** —(optional) Select whether or not to allow the Display Label and the API Variable to be edited by users. To prevent the field from being edited by other users, select "No." Valid values are:
   - Yes - Allows the Display Label/API Variable fields to be edited.
   - No (default) - Prevents the Display Label/API Variable fields from being edited.
5. (optional) For the remaining **Display Label** fields and **API Variable** fields, repeat steps 2, 3, and 4. You can specify up to 4 display labels and API variables.

Capacity

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

Archiving

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

To set the minimum number days to store recordings:

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

Upgrade to Route Group

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

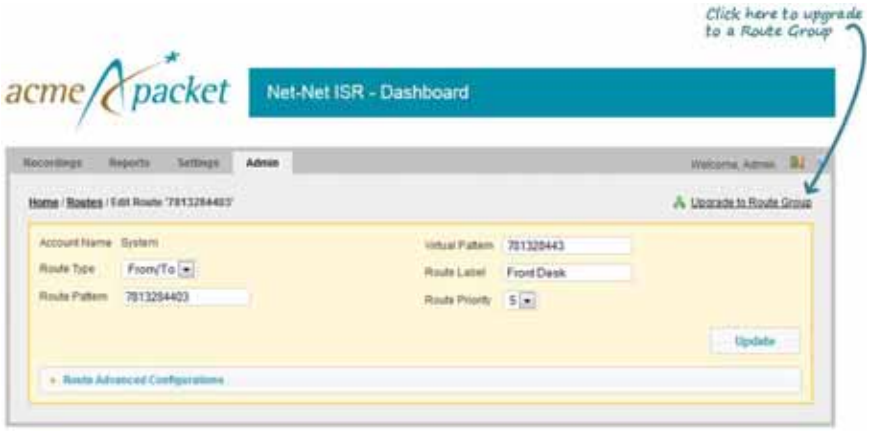
To set up a Route Group, you must have a Master Route previously created with the desired parameters (recording percentage, file formats, announcements, custom data fields, etc.). To create a Master Route, see Adding a Route.

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

To add a route to a Route Group:

1. Make sure you have a Master Route configured for an account.
2. On the Admin page, click **Manage Routes**. The Routes page displays.

3. Select a route from the list to add to a Route Group, and click the Details icon. The following dialog box displays.

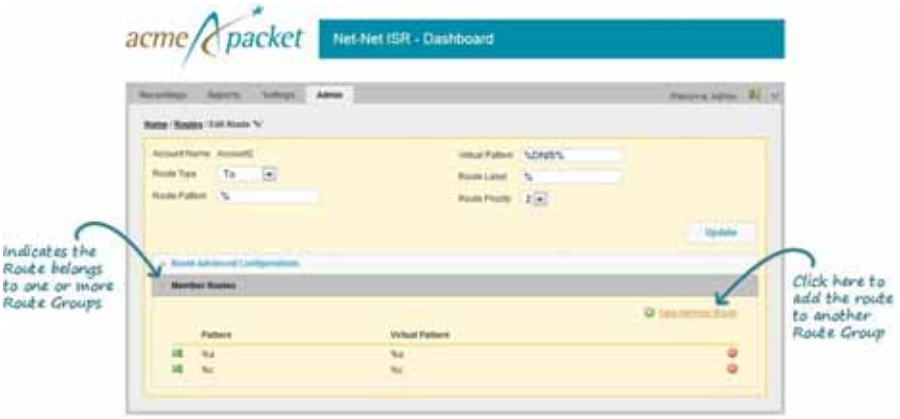


4. Click U**pgrade to Route Group**. The following dialog box displays.

5. **Pattern**—Specify a route pattern to use for this route. This field is based on the "Route Type" currently set for the Master Route. Use the route pattern value to match an incoming call's From, To or From/To and apply the appropriate rules of the route and account.This member is added to the Route Group. Valid values are alpha-numeric characters. For examples of route patterns, see Examples of Route Patterns.
6. **Virtual Pattern**—Specify the value of the destination where the calls matching the route pattern are forwarded once recording rules have been evaluated. This value can be a To number. If you defined a Session Agent at *Manage Sites*, a full SIP URI can override this number. Valid values for this field are alpha-numeric characters. For example of route patterns, see Examples of Route Patterns.

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

7. Click **Create** to add the Route to the Route Group. The Routes page displays. A Member Routes tab displays at the bottom of the Routes page.



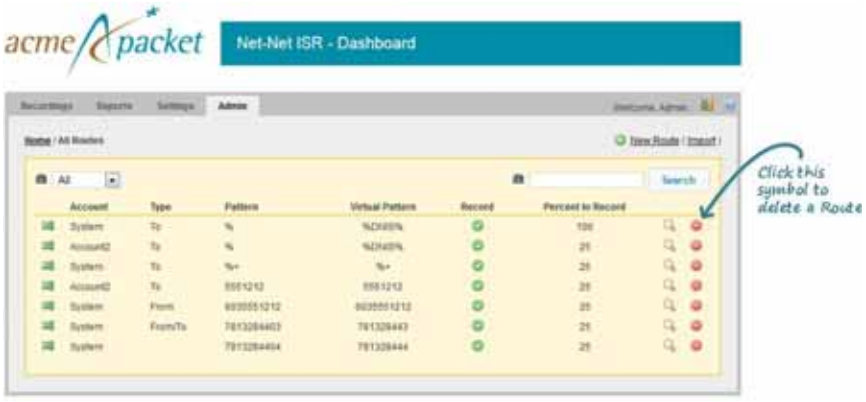
8. Add the current route to additional Route Groups if required by clicking **New Member Route** and repeat Steps 5, 6, and 7.

Deleting a Route

You can delete routes in the ISR Dashboard as required.

To delete a route:

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



The following message and prompt displays.

"*By deleting this route you will delete any associated webservice appliance and data.*

Are you sure you want to delete this route?"

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

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

Managing Recording Format Profiles

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

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

There are four Recording Format Profiles:

- Best Quality
- Default
- Small
- Smallest

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

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

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

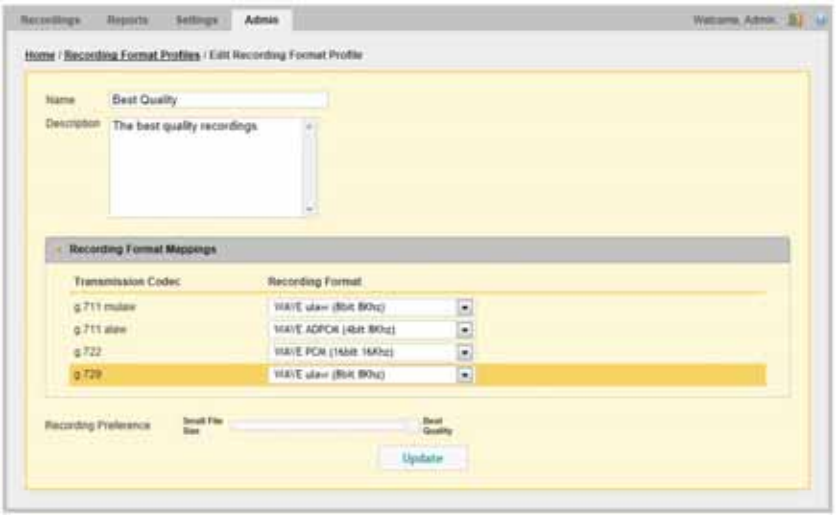
Within a recording format profile, you can also configure recording format mappings. This allows you to select a recording format for each of the four supported transmission codecs, g.711 mulaw, g.711 alaw, g.722, and g.729.

To edit a recording format profile:

1. After logging into the ISR Dashboard, click **Edit System Configurations** or click **Admin** in the top menu bar.
2. Click **Manage Recording Format Profiles**.

   A list of all four recording format profiles displays.
3. Click the recording format profile you want to edit.

The Edit Recording Format Profile page appears.



4. **Name**—(*Optional*) Enter a name for this recording format profile.
5. **Description**—(*Optional*) Enter a brief description of this recording format profile.
6. **Recording Preference**—(*Optional*) Drag the slide-bar to the appropriate space between Small File Size and Best Quality based on the recording preference for this recording format profile.

To configure Recording Format Mappings:

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

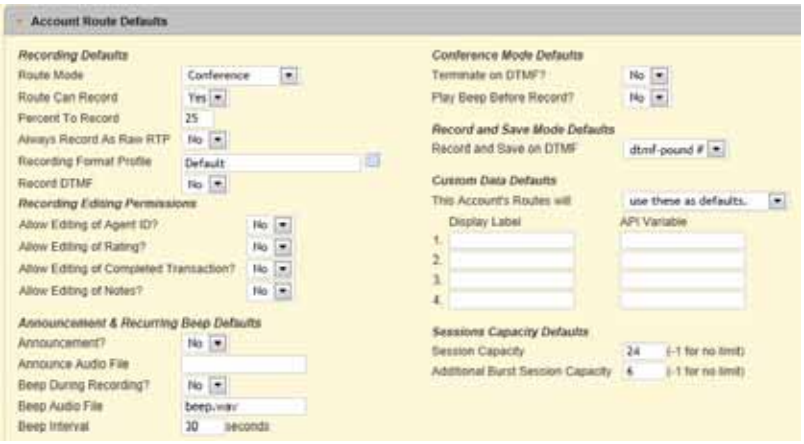
2. Beside each Transmission Codec, select a Recording Format from the drop-down list.
3. Click **Update**.

Applying Recording Format Profiles to Accounts

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

   A list of all accounts configured on the ISR displays.

3. Click the account on which you are applying a recording format profile.Click **Account Route Defaults**.

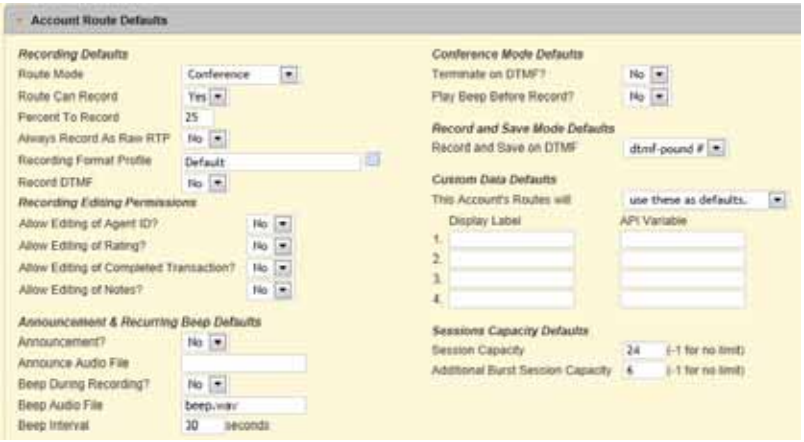


4. **Always Record as Raw RTP**—Select **Yes** when multiple transmission codecs are present in a session. If set to **No** with multiple transmission codecs present in a session, the ISR will not record the call properly.
5. **Recording Format Profile**—Select the recording format profile you want to assign to this account. The default value is **Use System Account's Profile**.
6. Click **Update**.

Applying Recording Format Profiles to Routes

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

   A list of all routes configured on the ISR displays.
3. Click the route on which you are applying a recording format profile.
4. Click **Route Advanced Configurations**.



5. **Always Record as Raw RTP**—Select **Yes** when multiple transmission codecs are present in a session. If set to **No** with multiple transmission codecs present in a session, the ISR will not record the call properly.
6. **Recording Format Profile**—Select the codec profile you want to assign to this account. The default value is **default**.
7. Click **Update**.

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.

To import route information from a CSV file:

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

   Notes:

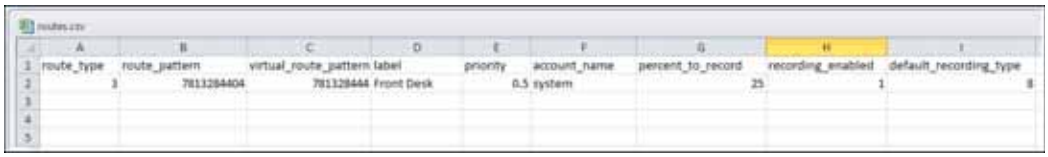
   - Boolean (yes/no) values must be entered using 0 (yes or enabled) and/or 1 (false or disabled).
   - All parameters must be entered with no spaces (use underscores instead of spaces).

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

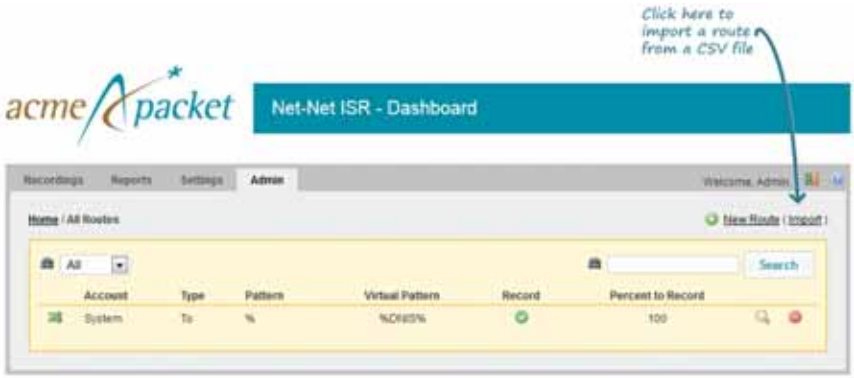
Parameter Heading	Valid Values
route_type	0 To 1 From 3 From/To
route_pattern	alpha-numeric characters
virtual_route_pattern	alpha-numeric characters
label	alpha-numeric characters
priority	1 to 9
account_name	alpha-numeric characters
percent_to_record	0 to 100
recording_enabled	0 | 1
default_recording_type	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
custom_data_1_name	alpha-numeric characters
custom_data_1_friendly_name	alpha-numeric characters

custom_data_1_editable_flag	0 | 1
custom_data_2_name	alpha-numeric characters
custom_data_2_friendly_name	alpha-numeric characters
custom_data_2_editable_flag	0 | 1
custom_data_3_name	alpha-numeric characters
custom_data_3_friendly_name	alpha-numeric characters
custom_data_3_editable_flag	0 | 1
custom_data_4_name	alpha-numeric characters
custom_data_4_friendly_name	alpha-numeric characters
custom_data_4_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

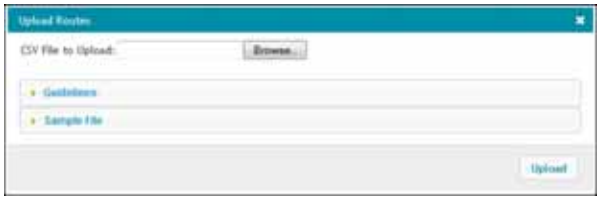
Example File with Parameters and Values



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



6. Click **Import**. The following dialog box displays.



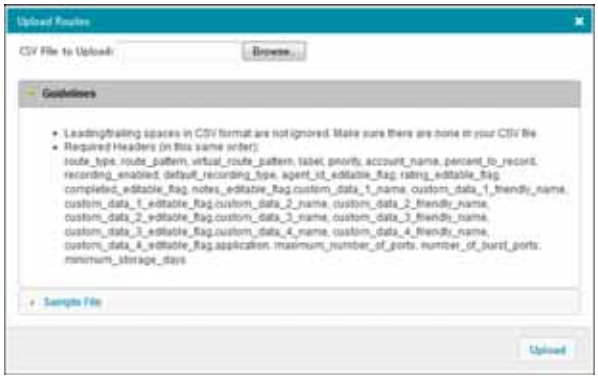
7. **CSV File to Upload—**Enter the name of the route CSV file you want to import into the ISR database. Valid values are alpha-numeric characters. For example, *Route1.csv*.

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

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

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

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



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

5 Managing Authorization Services

Introduction

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

Manage Authorization Services

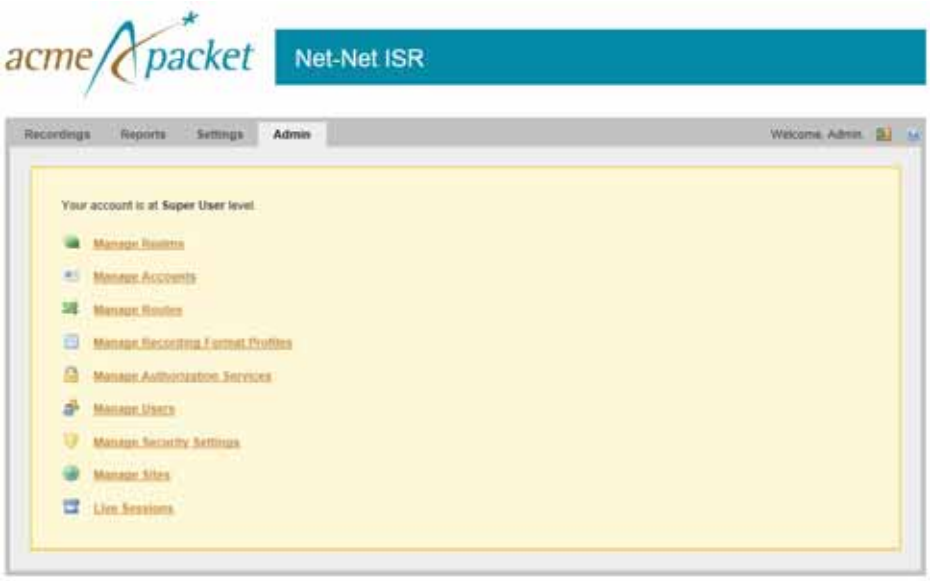
Use **Manage Authorization Services** on the Admin Menu of the ISR Dashboard to manage 3rd party servers in the ISR network.

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

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

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

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



Authorization Services Page

The following table describes the columns on the Routes page.

Column	Description
Name	Name of the Authorization Service.
Service URL	Specifies the Uniform Resource Locator (URL) of the Authorization Service. This is the URL associated with the Authorization Service.
Status	Identifies the current status of the Authorization Service on the ISR. Values can be: Authorization Service is enabled. 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 dependant on your access privileges (Super Users and Account Administrators only).

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

To add an Authorization Service:

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

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

4. **Name**—Enter the name of the Authorization Service (3rd party server). Valid values are alpha-numeric characters.
5. **Service**—Enter the Uniform Resource Locator (URL) of the Authorization Service (3rd party server). Valid values are alpha-numeric characters, and must be entered in a typical URL format. For example, *http://ews.xdp.broadsoft.com/webservice/services/ProvisioningService?wsdl*
6. **Enabled**—Select whether or not to enable the Authorization Service (3rd party server) in the ISR network. Valid values are:
   - Yes (default) - Enable the Authorization Service (3rd party server) to be used in the ISR network.
   - No - Prevents the Authorization Service (3rd party server) from being used in the ISR network.
7. **SRC Type**—Select the Authorization Service (3rd party server) currently deployed in your ISR network. Valid values depend on the type of Session Recording Client (SRC) you are using in your ISR network. Default value is “default” which uses any SRC type having the URL specified for the “Service” parameter.

8. Click **Create**. The new Authorization Service displays on the Authorization Services page.

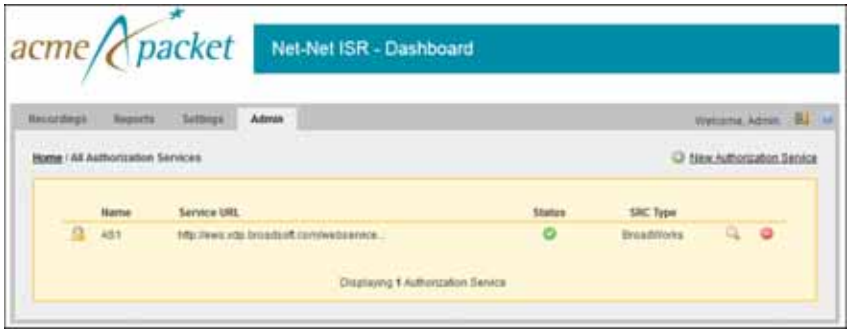
Editing an Authorization Service

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

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

To edit an Authorization Service:

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



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

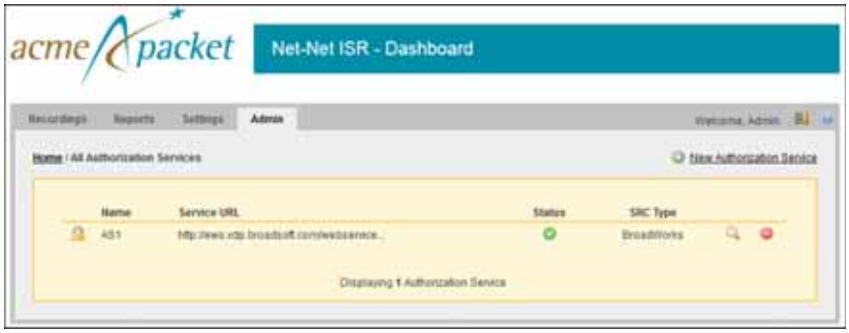
You can delete an Authorization Service(s) (3rd party server) from the ISR database as required.

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

To delete an Authorization Service:

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

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



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.

6 Managing Users

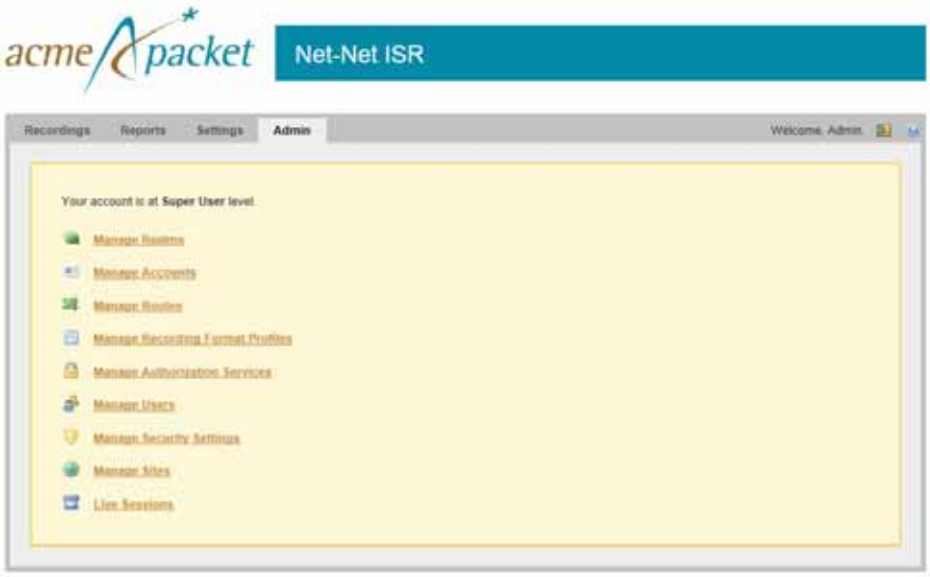
Introduction

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

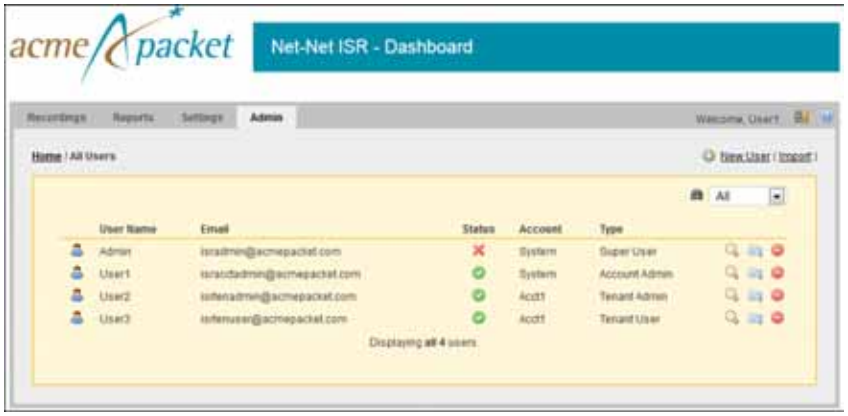
Manage Users

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

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



Users Page



The following table describes the columns 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.)>*
Status	Indicates the current status of the User. Status can be: Status is active. User can log into the ISR Dashboard. Status is inactive. User cannot log into the ISR Dashboard. 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).
	Displays profile details about the User and allows you to edit the details.
	Displays details about the actions of the user in the ISR Dashboard. Information includes: • Time - Time of the action. • Action - Description of the action. • Object - Object that was used during the action. • IP Address - IP address that was accessed during the action.
	Deletes the User profile.

User Access Levels

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

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

	USER TYPE				
DASHBOARD FEATURE	Super User	Account Administrator	Tenant Administrator	Tenant User	Remote Archiver User
View/Play Recordings	X	X	Own Recordings only	Own Recordings only	X
Generate Reports	X	X	Reports for own Accts only	Reports for own Accts only	X
Edit Dashboard Settings	X	X	X	X	X
Manage Realms	X	X	-	-	
Manage Accounts	X	X	Own Accts only	-	X
Manage Routes	X	X	Routes for own Accts only	-	X
Manage Authorization Services	X	X	-	-	X
Manage Users	X	X	Users for own Accts only	-	X
Manage Sites	X	View only	-	-	X
View Live Sessions	X	X	-	-	X

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

Adding a User

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

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

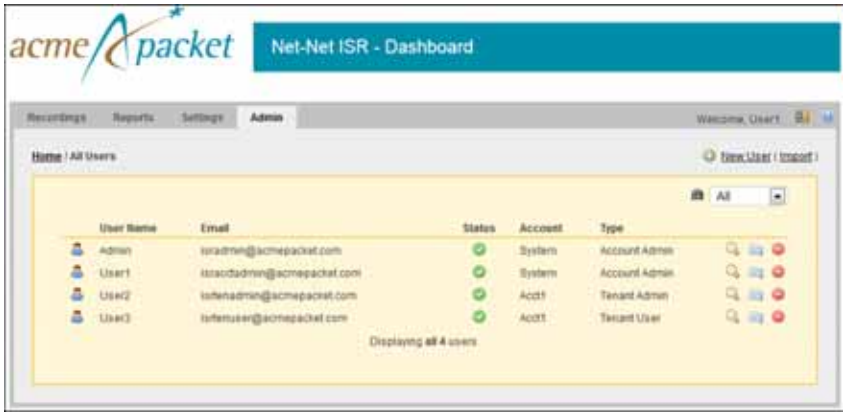
Note: You can create a User profile using any application that can save to a comma separated value (CSV) file (i.e., Microsoft® Excel, Notepad®, etc.). Using the ISR Dashboard, you can then import the User profile information from the file (<*filename*>.*csv*) to the ISR database.

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

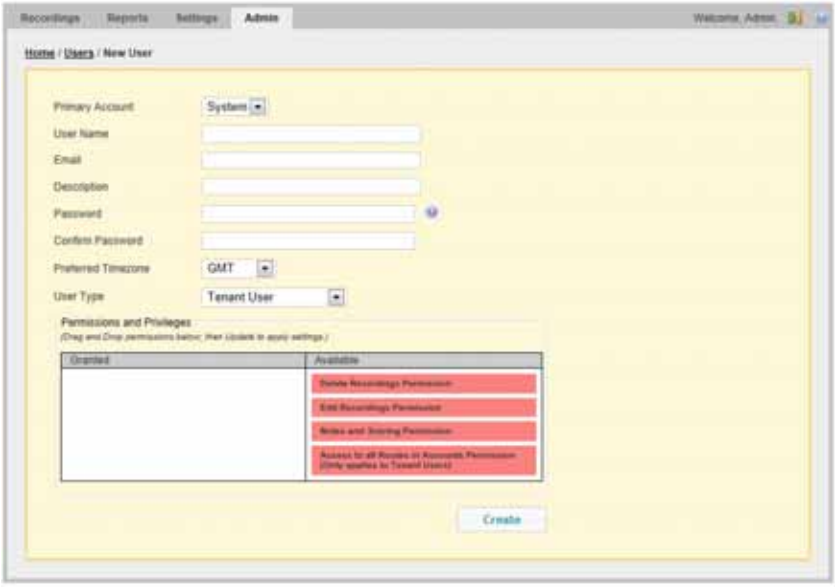
To add a user:

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

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



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



4. **Primary Account**—Select the primary account to assign to this User. Valid values are dependant on the accounts currently configured in the ISR, and the permission level of the User. Default is “System.”
5. **User Name**—Enter a name for the user. Valid values are alpha-numeric characters.
6. **Email**—Enter the user’s email address. This is the value the User enters in the “Email” field on the login page. Valid values are alpha-numeric characters, and is usually a domain name in the format:

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

   For example, smith@acmepacket.com.
7. **Description**—(optional) Enter a description for the user. Valid values are alpha-numeric characters.
8. **Password**—Enter a password for the user to specify when logging into the ISR Dashboard. By default, the password must contain letters and numbers, have at least one uppercase letter, and be at least 8 characters long. Valid values are alpha-numeric characters.

Note: When the user logs in using the assigned password, the Dashboard prompts the user to change it for security purposes.

9. **Confirm Password**—Re-enter the password from Step 8 to verify you entered the password correctly.
10. **Preferred Time Zone**—Select the time zone associated with the location of the user. This value is an offset of Greenwich Mean Time (GMT). The following table provides the valid values and default for this field.

Time Zone Table

Time Zone	Location
GMT-12 (default)	**IDLW - International Date Line West**
GMT-11	**NT - Nome**
GMT-10	**AHST - Alaska-Hawaii Standard** **CAT - Central Alaska** **HST - Hawaii Standard**
GMT-9	**YST - Yukon Standard**
GMT-8	**PST - Pacific Standard** Los Angeles, CA, USA
GMT-7	**MST - Mountain Standard**
GMT-6	**CST - Central Standard** Mexico City, Mexico Saskatchewan, Canada
GMT-5	**EST - Eastern Standard** Bogota Lima, Peru New York, NY, USA
GMT-4	**AST - Atlantic Standard** Caracas La Paz
GMT-3	Brasilia, Brazil Buenos Aires, Argentina Georgetown, Guyana
GMT-2	**AT - Azores**
GMT-1	**WAT - West Africa** Azores, Cape Verde Islands
GMT	London, England Dublin, Ireland Edinburgh, Scotland Lisbon, Portugal Reykjavik, Iceland Casablanca, Morocco
GMT+1	**CET - Central European** Paris, France Berlin, Germany Amsterdam, The Netherlands Brussels, Belgium Vienna, Austria Madrid, Spain Rome, Italy Bern, Switzerland Stockholm, Sweden Oslo, Norway

Time Zone	Location
GMT+2	**EET - Eastern European** Athens, Greece Helsinki, Finland Istanbul, Turkey Jerusalem, Israel Harare, Zimbabwe
GMT+3	**BT - Baghdad** Kuwait Nairobi, Kenya Riyadh, Saudi Arabia Moscow, Russia
GMT+4	Abu Dhabi, UAE
GMT+5	Kazakhstan (western-Aqtau) Maldives (Male) Pakistan (Islamabad, Karachi) Russia Tajikistan (Dushanbe) Turkmenistan (Ashkhabat) Uzbekistan (Tashkent) India (New Delhi, Calcutta) Sri Lanka (Colombo) Nepal (Katmandu)
GMT+6	Bangladesh Bhutan Kazakhstan Kyrgyzstan Sri Lanka (formerly Ceylon)
GMT+7	Cambodia Christmas Island Indonesia Lao Thailand Vietnam
GMT+8	**CCT - China Coast**
GMT+9	**JST - Japan Standard**
GMT+10	**GST - Guam Standard**
GMT+11	Solomon Islands
GMT+12	**IDLE - International Date Line East** **NZST - New Zealand Standard** Wellington, New Zealand Fiji Marshall Islands

11. **User Type**—Select the user access level from the drop-down list to assign to this user. Valid values are

- Super User
- Account Admin
- Tenant Admin
- Tenant User
- Remote Archiver User

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

User Type	Available User Type Values
Superuser	Superuser Account Admin Tenant Admin Tenant User
Account Administrator	Account Admin Tenant Admin Tenant User
Tenant Administrator	Tenant Admin Tenant User
Tenant User	N/A
Remote Archiver User	N/A

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

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

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

User Type	Available Permission and Privileges
Superuser	A Superuser can assign these permissions to an Account Admin, Tenant Admin, and Tenant User: • Delete Recordings Permission • Edit Recordings Permission • Notes and Scoring Permission • Access to all Routes in Accounts Permission (Only applies to Tenant Users)
Account Administrator	An Account Admin can assign these permissions to a Tenant Admin and a Tenant User: • Delete Recordings Permission • Edit Recordings Permission • Notes and Scoring Permission • Access to all Routes in Accounts Permission (Only applies to Tenant Users)
Tenant Administrator	An Tenant Admin can assign these permissions to a Tenant User: • Delete Recordings Permission • Edit Recordings Permission • Notes and Scoring Permission • Access to all Routes in Accounts Permission (Only applies to Tenant Users)

User Type	Available Permission and Privileges
Tenant User	N/A
Remote Archiver User	N/A

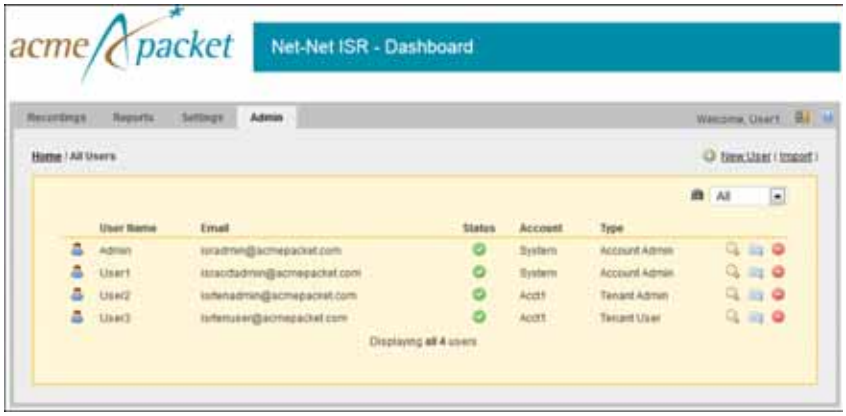
13. Click **Create** to add the new User to the Users page.

Editing a User Profile

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

To edit a User profile:

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



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

   "*Successfully saved*".

Showing User Details

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

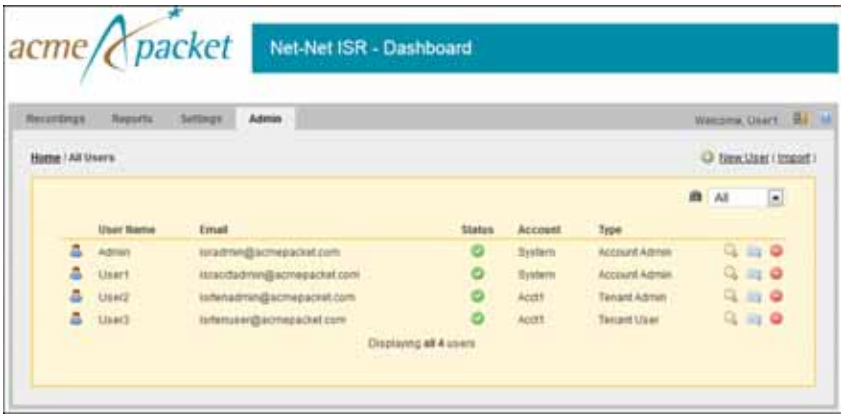
- Date and time (based on time zone) that the User performed an action.
- Specific action that the User performed.
- Object (User email ID) of the User that was logged in when the action was performed.
- IP address of where the action was performed by the User.

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

To display the User Audit Trail:

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

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



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.

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

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

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

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

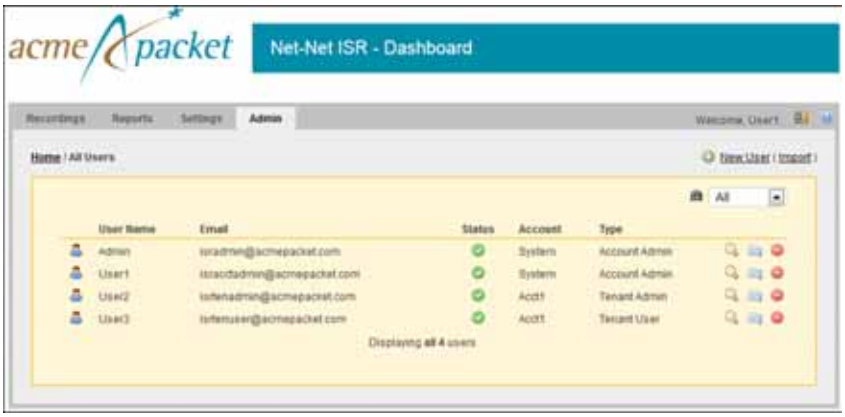
Deleting a User

You can delete users from the ISR database as required.

To delete a User:

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

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



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

   "*Are you sure you want to delete this user?*"

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

Managing User Dashboard Security Settings

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

To Configure Dashboard Security Settings:

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

3. **Users Password Expires in**—Specify the number of days after which users' passwords expire. The default value is **90**.
4. **User Lockout Duration**—Specify the number of minutes a user must wait before attempting to log in again after reaching the User Max Failed Logins Before Lockout value. The default value is **30**.
5. **User Max Failed Logins Before Lockout**—Specify the number of failed login attempts allowed before the ISR locks a user out.
6. **Show Forgotten Password Page?**—Specify whether or not a user can view a Forgotten Password Page. The default value is **no**.
7. Click **Update**.

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.

To import a user profile from a CSV file:

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

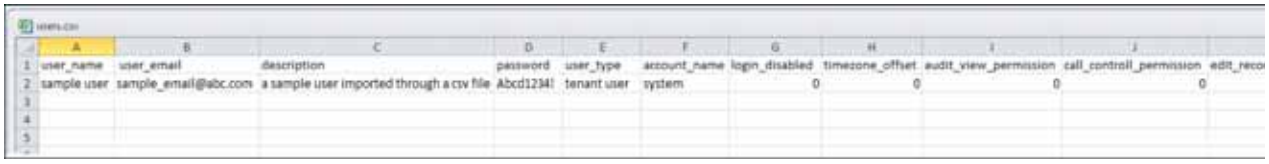
   Notes:

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

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

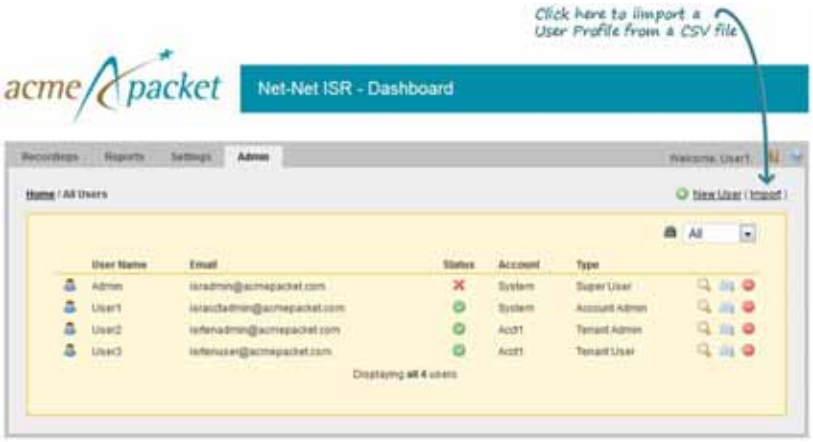
Parameter Heading	Valid Values
user_name	alpha-numeric characters
user_email	Usually a domain name in the format *<username>@<host server>.<domain name system (.com, .org, .net, .edu, etc)>*. For example: sample_email@abc.com
description	alpha-numeric characters
password	alpha-numeric characters
user_type	Superuser Account Admin Tenant Admin Tenant User
account_name	alpha-numeric characters
login_disabled	0 | 1
timezone_offset	0 | 1
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	
1	user_name	user_email	description	password	user_type	account_name	login_disabled	timezone_offset	audit_view_permission	call_controll_permission	edit_reco
2	sample user	sample_email@abc.com	a sample user imported through a csv file	Abcd1234!	tenant user	system	0	0	0	0	
3											
4											
5											

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



6. Click **Import**. The following dialog box displays.

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

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

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

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

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

Click on **Sample File**, then click **users.csv** to download an example of a route CSV file you can use as a guideline.

7 Managing Sites

Introduction

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

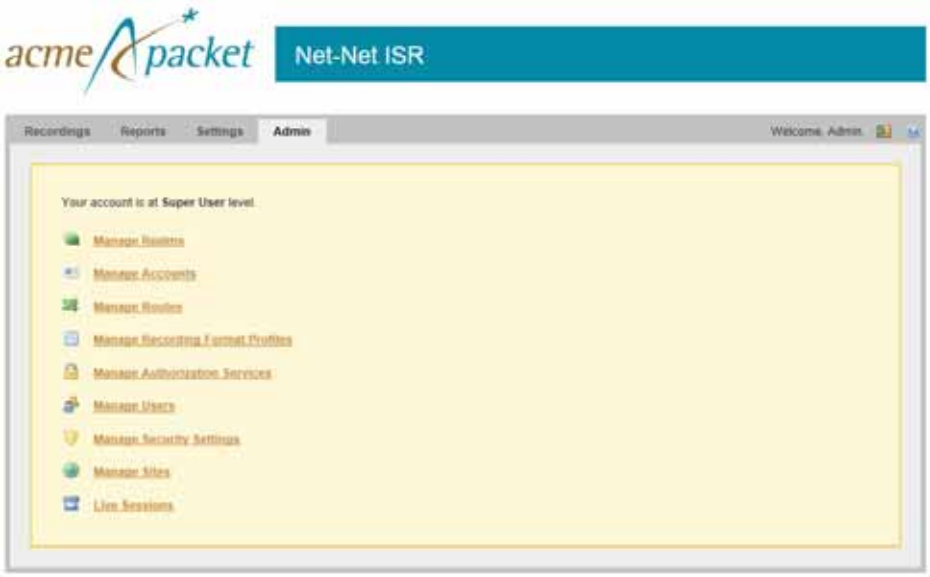
Manage Sites

Use the **Manage Sites** on the Admin Menu of the ISR Dashboard to manage ISR sites in your network. A site is a physical location, a group of recording servers, or a single ISR.

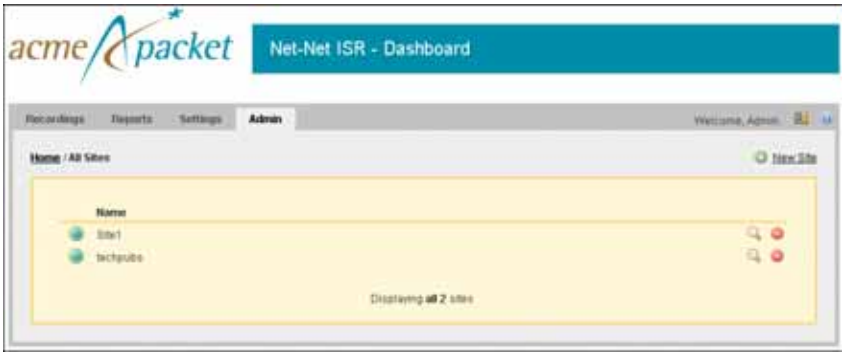
Managing sites includes adding, editing, and deleting sites that contain configurations for the following components:.

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).
Session Agent	Allows you to edit or delete information about the current telephony Session Agent(s), or add a new Session Agent associated with a site. A Session Agent connects to the IP PBX and is used to transfer calls to agents or to the PSTN. The Session Agent configuration displays the Session Agent name, IP Address, type of Session Agent (primary or failover), and the status of Session Agent (active or disabled). It also displays information about the last event that occurred on the Session Agent.
Web Appliance	Allows you to edit or delete information about an Appliance, or add a new Appliance associated with all current sites configured for the ISR. An Appliance allows the ISR to connect to a Web Service to push call recording data to a remote storage area. The Web Appliance configuration displays the route(s) for which the Appliance is associated, the URL that connects the ISR to the Web Service, the maximum connections allowed by the ISR for connecting to the Web Service, the maximum failures allowed per call data record (CDR) by the ISR, whether or not the recording is deleted after the push (enabled or disabled), and the state of the Appliance (active or paused).

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 columns 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

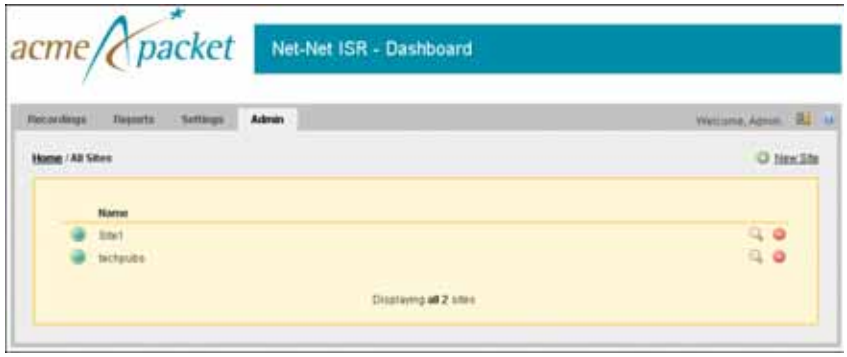
Superusers can add a Site to the ISR using the **New Site** link on the Manage Sites page. Once the Site is created and saved to the ISR database, you must configure the following applicable components for the Site:

- RSS (required)
- RSS Location (required)

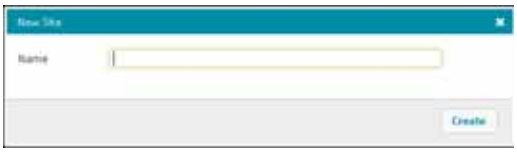
- Archiver (optional)
- Session Agent (optional)
- Web Appliance (optional)

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 **Manage Sites**. The Manage Sites page displays.



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



4. **Name**—Enter a name for the Site. Valid values are alpha-numeric characters.
5. Click **Create**. The Site name displays on the Sites page.

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

Managing an RSS

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

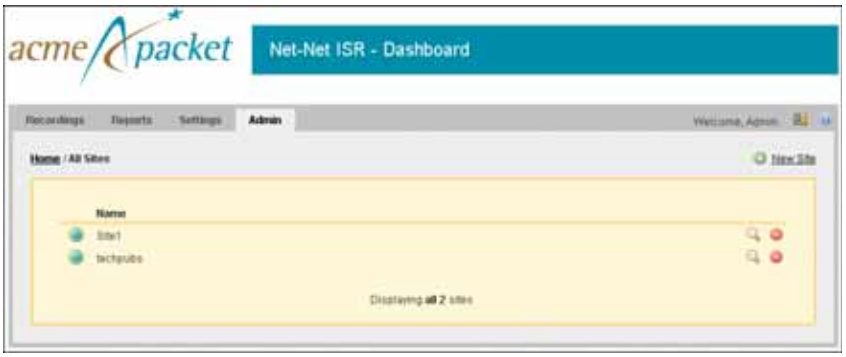
Important: It is recommended that you contact your Technical Support representative before adding or changing an RSS configuration.

Adding an RSS

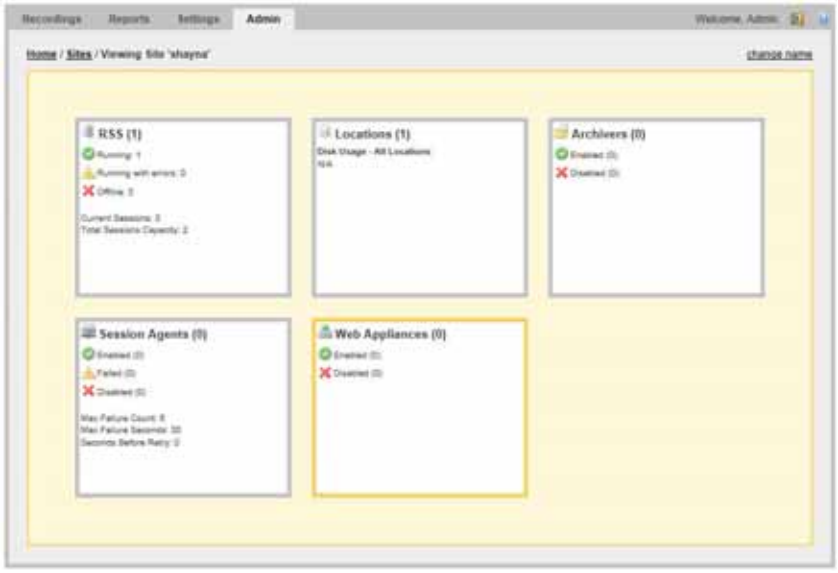
After adding a Site to the ISR, you must add an RSS to the Site's configuration.

To add an RSS to a Site:

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



The following page displays.



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

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

RSS Information	Description
Running	Total number of RSSs currently running on this Site.
Offline	Total number or RSSs currently offline on this Site.
Running with errors	Total number of RSSs running with errors on this Site.
Current Sessions	Total number of ports currently being used on the RSSs on this Site.
Total Sessions Capacity	Total number of licensed ports on the RSSs on this Site.

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

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

4. **Name**—Enter a name that describes the RSS you are adding. Valid values are alpha-numeric characters.
5. **IP Address**—Enter the IP address (in dotted decimal format) for which the RSS is listening for traffic.

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

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

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

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

The following table identifies each column on the RSS page.

Column	Description
RSS	Name of the RSS.
IP Address	IP Address of the RSS in dotted decimal format (0.0.0.0).
SIP Traffic Port	SIP Port number on the RSS that is currently accepting SIP traffic.

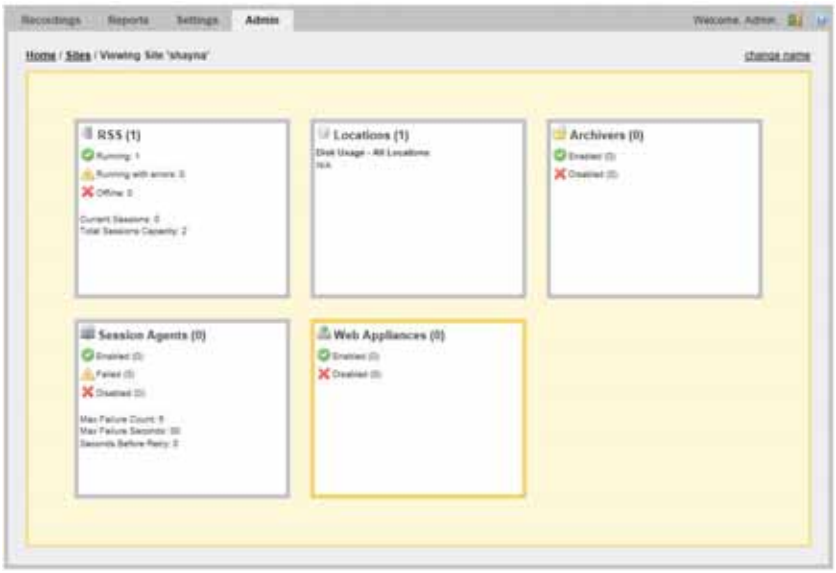
Column	Description
Status	Identifies the current status of the RSS. Status can be: RSS is running. RSS is offline. RSS is running with errors.
Uptime	Amount of time in days that the RSS has been up and running successfully.
Current Sessions	Number of ports currently being used on the RSS.
Sessions Capacity	Total number of licensed ports on the RSS.
	Displays details of the RSS and allows you to configure or edit the details.
	Deletes the RSS from the ISR database.

Editing an RSS

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

To configure the RSS:

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



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

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

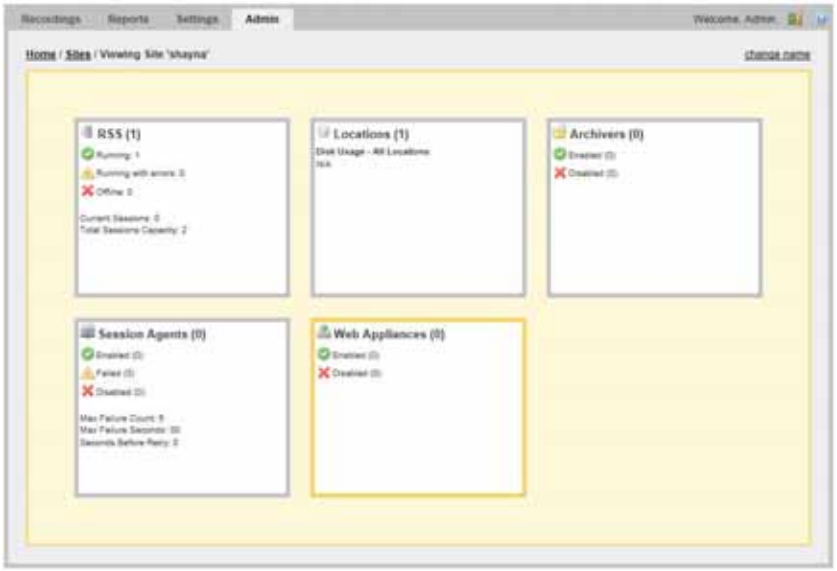
4. Edit the parameters for the RSS as applicable using the procedures defined in Adding an RSS, starting at Step 4.
5. When you are finished editing the RSS configuration, click **Update**. The changes are saved to the ISR database. The RSS page displays.

Deleting an RSS

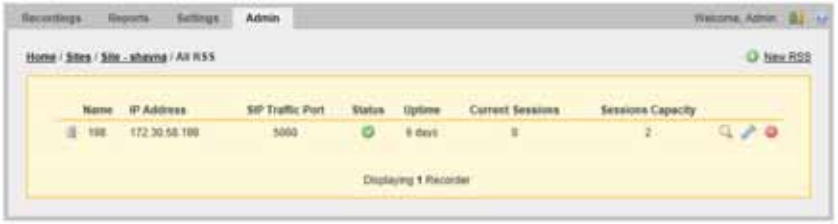
You can delete an RSS from a Site if required.

To delete an RSS:

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



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



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

   "*Are you sure you want to delete this RSS?*"

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

Warning: Once you delete an RSS, it cannot be recovered.

RSS Handling of a 302 Response via the ISR

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

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

Managing an RSS Location

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

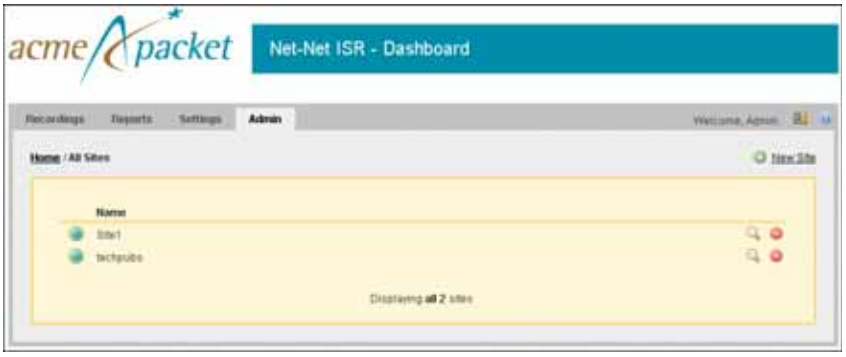
Adding a Location

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

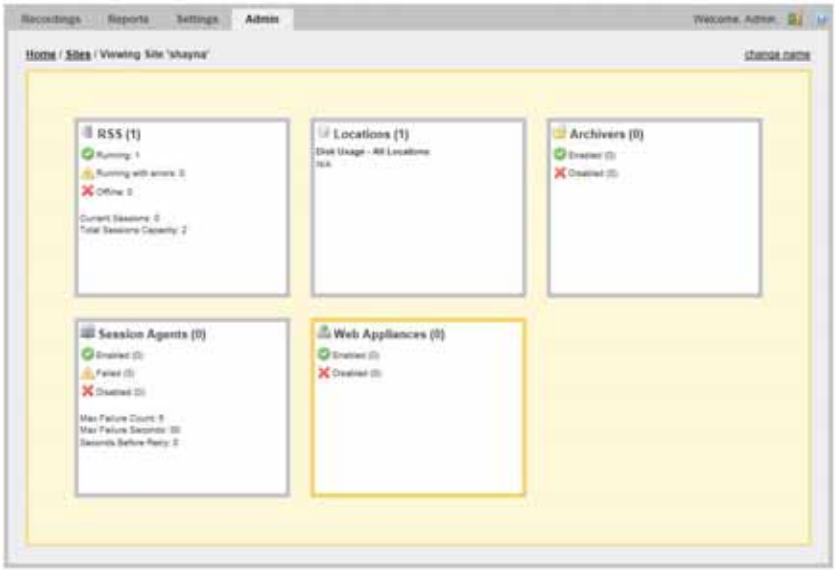
Note: A single configured Archiver (on the RSS) can move recordings to only one destination location. If you need recordings to go to other destination locations, you must configure an Archiver for each of those locations. For more information about configuring an Archiver, see Managing Archivers.

To add a new RSS Location:

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



The following page displays.



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

Location Information	Description
Disk Usage- All Locations	Indicates the percentage of storage disk used by the RSSs in all locations. Valid values are 0% to 100%.

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

The following table identifies each column on the Location page.

Column	Description
Name	Name of the RSS Location.
Recordings Directory	Specifies the directory path on the RSS where the recordings are stored before they are forwarded to the database on the Control and Index Server (CIS).
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 source directory location. Valid values are 0% to 100%.
	Displays details of the RSS Location and allows you to edit the details.
	Deletes the RSS Location from the ISR database.

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

4. **Name**—Enter a name that describes the Location you are adding. Valid values are alpha-numeric characters. For example, RSS1 (1.1.1.1) Primary.
5. **Recordings Directory**—Enter the directory path to where the Archiver stores the recordings on the RSS (destination directory). Valid values are alpha-numeric characters. For example, */cxc_common/ISR/Recordings.*
6. **URL**—Enter the URL that identifies the Web location for accessing the recordings via a browser. For example, *http://location1.foo.com/Recordings*.
7. **Global**—Select whether or not this Location may be used in Archival configurations on all Sites. Valid values are:
   - Yes - This Location may be used in all Sites.
   - No (default) - This Location configuration may apply to this Site only.

Recording Converter

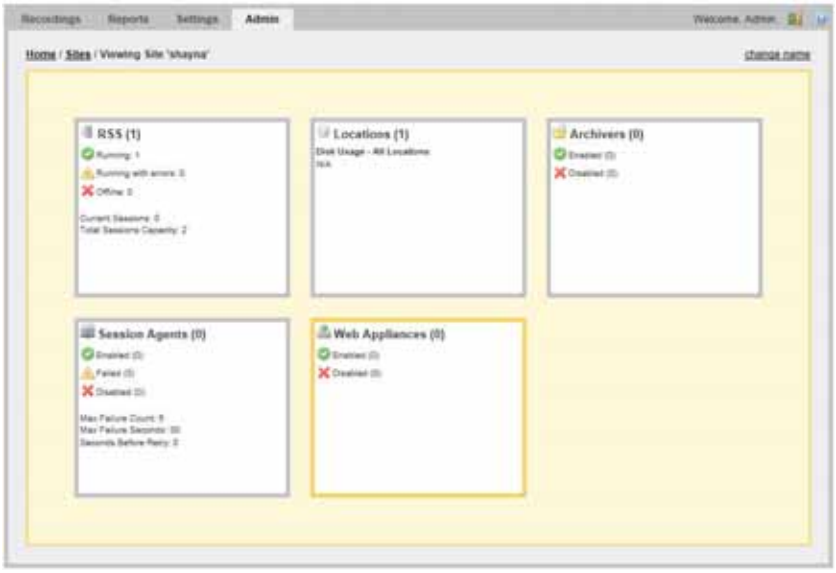
8. **IP Address**—Enter the IP address (in dotted decimal format) of the G.729 media converter (RMC). The RMC media converter converts incoming G.729 recordings from ".rpdd" formatted files to ".wav" formatted files, for playback by the ISR Dashboard. It allows the ISR to accept calls using a G.729 codec. For example, 172.453.45.6.
9. **Port**—Enter the port number of the RMC media converter that receives the G.729 media. Default is **8890**.
10. Click **Create**. The new RSS Location displays on the Location page.

Editing a Location

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

To edit the Location of an RSS:

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



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

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

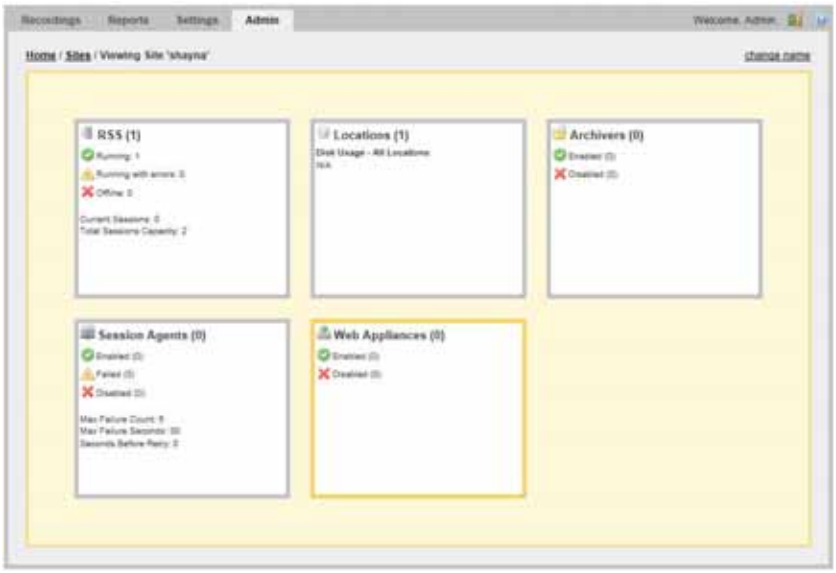
4. Edit the parameters for the RSS Location as applicable using the procedures defined in Adding a Location, starting at Step 4.
5. When you are finished editing the RSS Location, click **Update**. The changes are saved to the ISR database and display on the Location page.

Deleting a Location

You can delete an RSS Location if required.

To delete an RSS Location:

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



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

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

   "*Are you sure you want to delete this Location?*"

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

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

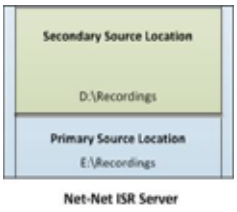
Managing Archivers

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

When you first install the ISR, you specify a Primary location for where the Archiver actively writes the recordings in real time. This can be a partition on the ISR server (RSS) or on another drive or server on the network. (The primary source location in the illustration below is *E:\Recordings on the RSS*).

You can also specify a secondary (failover) source location for the recordings. In the event that the primary location is inaccessible (i.e., it is full, or it can't be reached on the network, etc.), the ISR begins writing the recordings to the secondary location in real time. (The secondary source location in the illustration below is *D:\Recordings*).

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

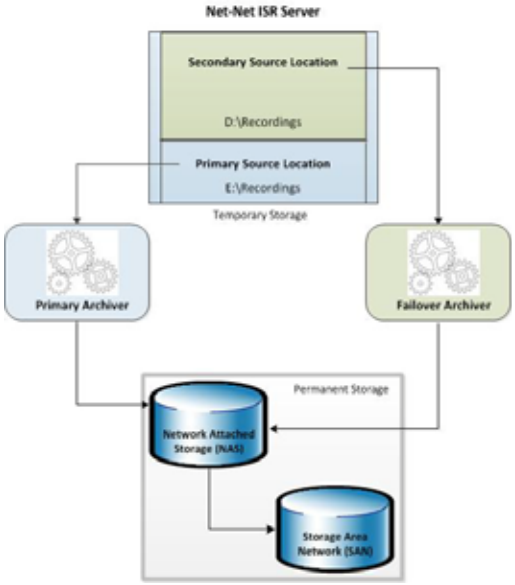


Note: Oracle recommends that you specify a secondary location for your recordings in the event the primary is inaccessible for any reason. For more information about setting up your secondary (failover) location, see the *Interactive Session Recorder Installation Guide*.

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

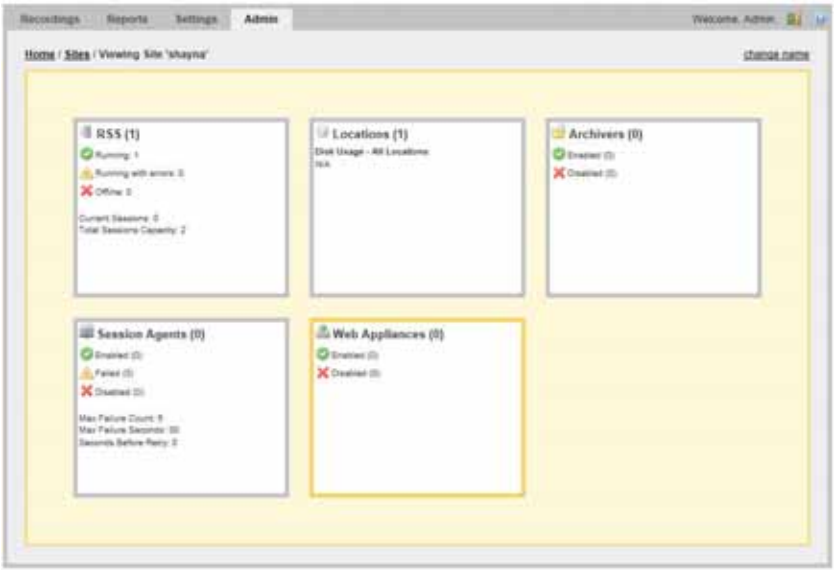
On the ISR, you can configure a Primary and Secondary (Failover) Archiver to move recordings from the primary and secondary locations, to more permanent storage devices as required. The Primary Archiver moves recordings from the primary location (source location) to the NAS or (destination location).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

The following illustration shows the use of the Primary and Failover Archiver in a network.



Note: A single configured Archiver can move recordings to only one destination location. If you need recordings to go to other destination locations, you must configure an Archiver for each of those locations.

The **Archivers** box on the Viewing Sites page displays the current status of the Archiver.



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

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

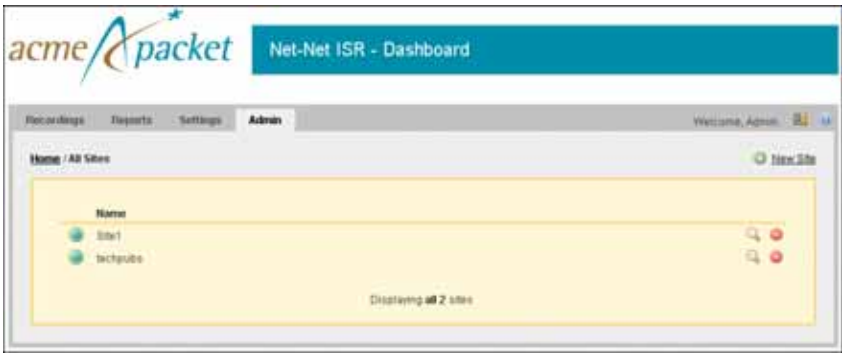
Clicking on the **Archiver** box on the Viewing Sites page allows you to add a new Archiver to the site, edit the configuration of an existing Archiver, or delete an Archiver if required.

Adding an Archiver

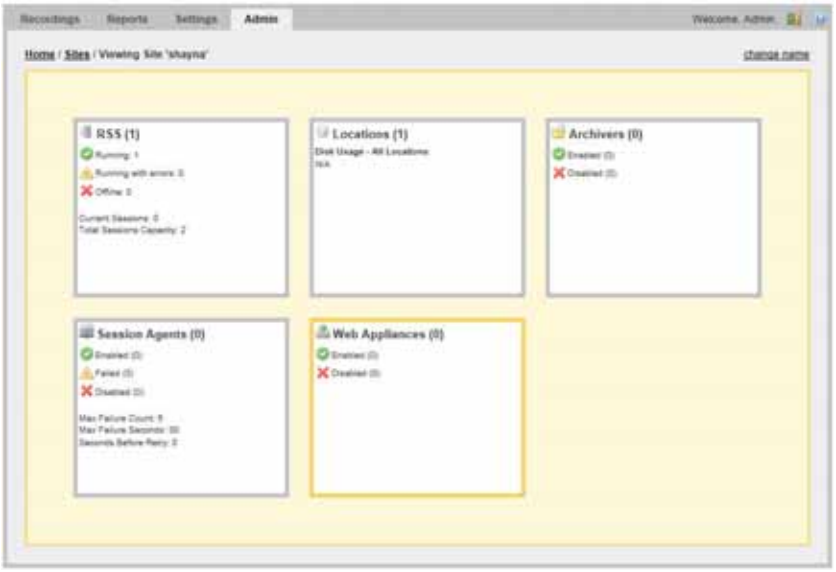
You can add an Archiver to a Site if required.

To add an Archiver:

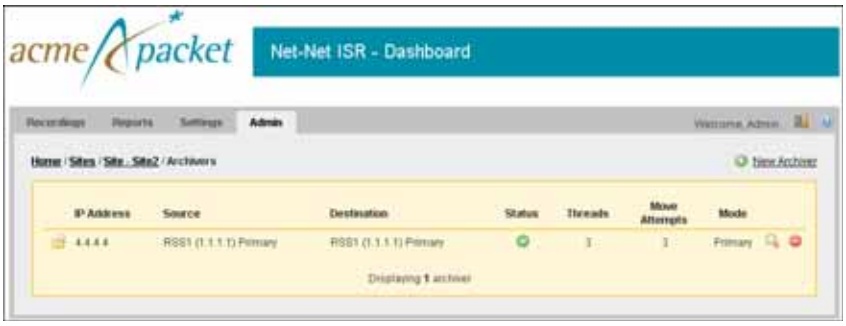
1. From the Sites page, choose a Site and click the Details icon.



The following page displays.



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

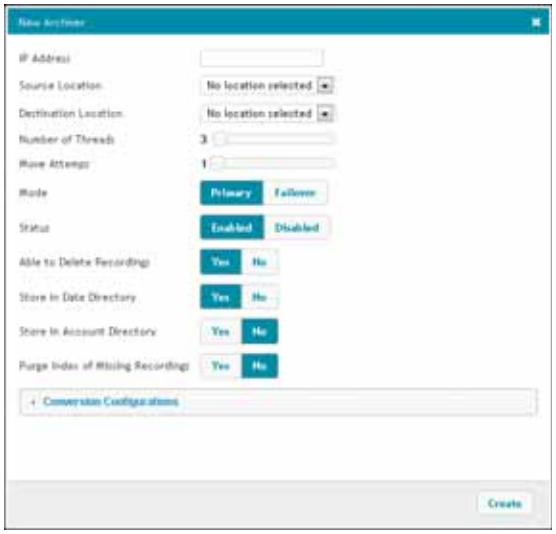


The following table identifies each column on the Archivers page.

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

Column	Description
Threads	Specifies the number of simultaneous recordings that an Archiver can move at one time.
Move Attempts	Specifies the number of attempts that the Archiver makes when moving recordings from the local disk to the storage device(s). If the Archiver fails to move the recording files from the source location to the destination location the first time, it repeats the attempts to move the files the number of times you set for this field. When all attempts are exhausted, and the Archiver still cannot move the recordings, a message displays stating that the Archiver has failed. If the Archiver is successful in moving the files, a message displays stating that the Archiver was successful.
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.

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



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

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

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

6. **Destination Location**—Select the location of the storage devices (NAS, SAN, etc.) for which the Archiver moves the recordings for storage. This is the Universal

Naming Convention (UNC) path of the destination location. When the Archiver moves the recording files to the destination location, it creates the appropriate subdirectories in this path to sort by machine, date, and time. By default, this field displays the destination location installed in your ISR network during the installation of the Archiver.

7. **Number of Threads**—Select the number of simultaneous recordings that an Archiver can move at one time. Valid values are **1** through **90**. Default is **3**.
8. **Move Attempts**—Select the number of attempts that the Archiver makes when moving recordings from the local disk to the storage device(s). If the Archiver fails to move the recording files from the source location to the destination location the first time, it repeats the attempts to move the files the number of times you set for this field. When all attempts are exhausted, and the Archiver still cannot move the recordings, a message displays stating that the Archiver has failed. If the Archiver is successful in moving the files, a message displays stating that the Archiver was successful. Valid values for this field are **1** through **10**. Default is **1**.
9. **Mode**—Select whether this Archiver is the Primary or the Failover Archiver. The Primary Archiver moves all recordings from the Primary Source Location to the destination location. The Failover Archiver moves all recordings from the Secondary Source Location to the destination location. Valid values are:
    - **Primary** (default) - This Archiver moves files from Primary Source Location.
    - **Failover** - This Archiver moves files from Secondary Source Location.
10. **Status**—Select whether the Archiver is enabled (active) for moving recording files, or temporarily disabled (paused). Valid values are:
    - **Enabled** (default) - Archiver is active and monitors when recording files are ready to be archived.
    - **Disabled** - Archiver is temporarily disabled and does not move recording files.
11. **Able to Delete Recordings**—Select whether or not this Archiver has permission to delete recordings and metadata stored longer than specified in Route/Account configurations. Valid values are:
    - **Yes** (default) - Archiver deletes files older than specified in Route/Account configurations.
    - **No** - Archiver does not delete files, regardless of the date specified in Route/Account configurations.
12. **Store in Date Directory**—Select whether or not the Archiver stores the recording files in a folder identified by the current date. Valid values are:
    - **Yes** (default) - Archiver stores recordings in a folder by date.
    - **No** - Archiver does not store recordings in a folder by date.
13. **Store in Account Directory**—Select whether or not the Archiver stores the recording files in a folder identified by the associated account on the local disk. Valid values are:
    - **Yes** - Archiver stores recordings in a folder by account.
    - **No** (default) - Archiver does not store recordings in a folder by account.
14. **Purge Index of Missing Recordings**—Select whether or not the Archiver attempts to remove recording files with no audio, from the main recording table, and send them to a “problem” table that can be reviewed at a later time. Enabling this feature prevents a user from viewing recording files with no audio, when they perform a search. However, an Administrator can view the “problem” table if required, for troubleshooting purposes. If this feature is disabled, the Archiver keeps the recording

file with no audio in the main recording table and moves on to the next record in the table. Valid values are:

- **Yes** - Archiver moves recordings with no audio from the main recording table to a "problem" table. Users cannot view these recordings. Administrators can view the "problem" table.
- **No** (default) - Archiver keeps recordings with no audio in the main recording table. Users can view these recordings.

Conversion Configurations

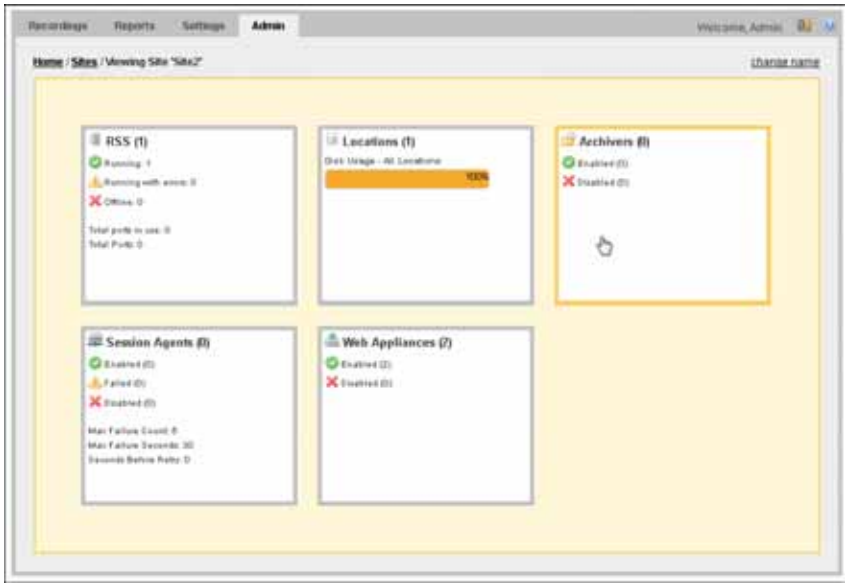
15. **Mode**—Select whether all G.729 recordings are converted, a percentage of recordings are converted, or no recordings are converted. Valid values are:
    - **Disabled** (default) - The RMC media converter does not convert incoming G.729 recordings from *.rpdd* format to *.wav* format.
    - **Convert All** - The RMC media converter converts all incoming G.729 recordings from *.rpdd* format to *.wav* format.
    - **Convert by Percentage** - The RMC media converter converts only a percentage of all incoming G.729 recordings from *.rpdd* format to *.wav* format, based on the value entered for the "**Percent of Recordings to Convert**" parameter.
16. **Percent of Recordings to Convert**—Select a number to indicate the percentage of incoming recordings to be converted by the RMC media converter. The "Mode" field must be set to "Convert by Percentage" in order to set the percentage value. Valid values are **0** to **100**. Default is **100** percent.
17. **Convert All Recordings in Last Archiver Destination**—Select whether or not the RMC media converter converts all of the last G.729 recordings stored in the Archiver from *.rpdd* format to *.wav* format. Valid values are:
    - **Yes** (default) - The RMC media converter converts all of the last G.729 recordings stored in the Archiver from *.rpdd* format to *.wav* format.
    - **No** - The RMC media converter DOES NOT convert all of the last G.729 recordings stored in the Archiver from *.rpdd* format to *.wav* format.
18. Click <**Create**>. The new Archiver displays on the Archivers page.

Editing an Archiver

You can edit an Archiver configuration if required.

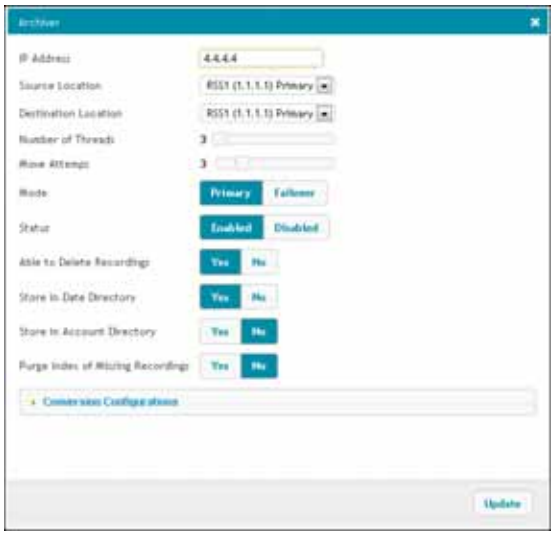
To edit an Archiver:

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



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

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



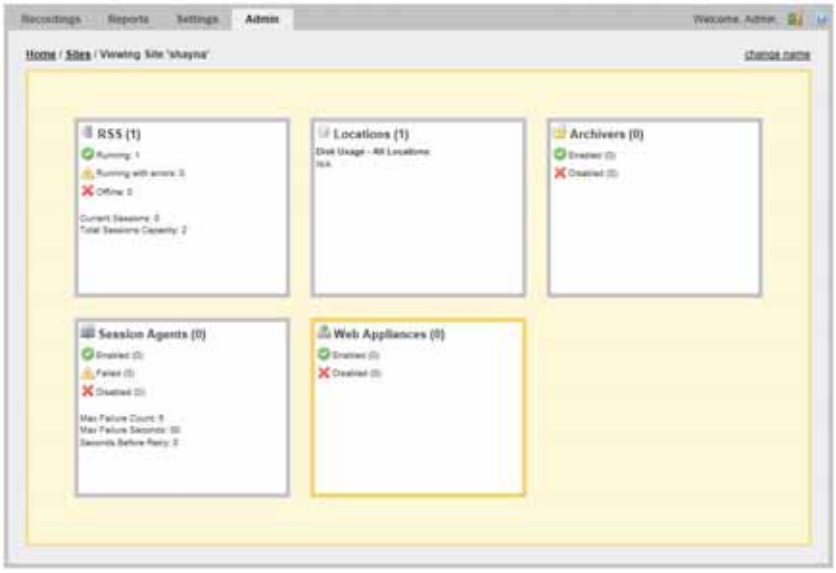
4. Edit the parameters for the Archiver as applicable using the procedures defined in Adding an Archiver, starting at Step 4.
5. When you are finished editing the Archiver, click **Update**. The changes are saved to the ISR database and display on the Archivers page.

Deleting an Archiver

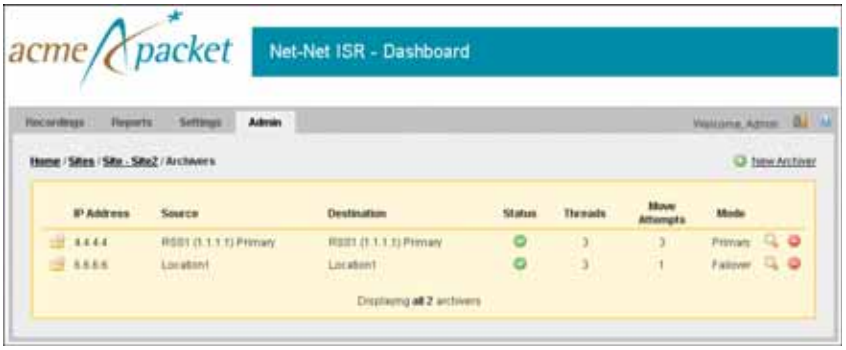
You can delete an Archiver if required.

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 **Archiver** component. The following page displays.



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

   "*Are you sure you want to delete this Archiver?*"

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

Warning: Once you delete an Archiver, it cannot be recovered.

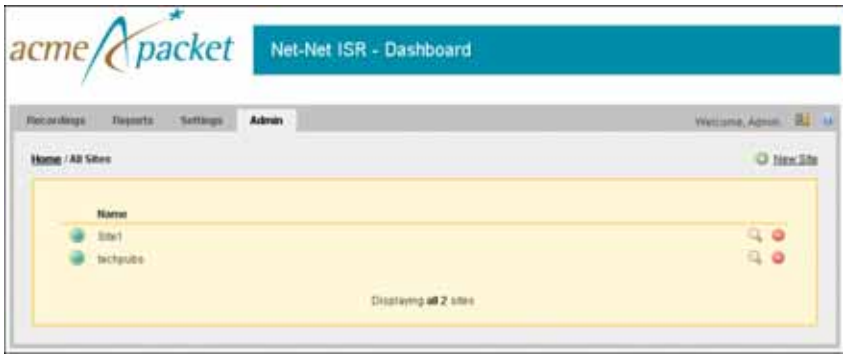
Managing Session Agents

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

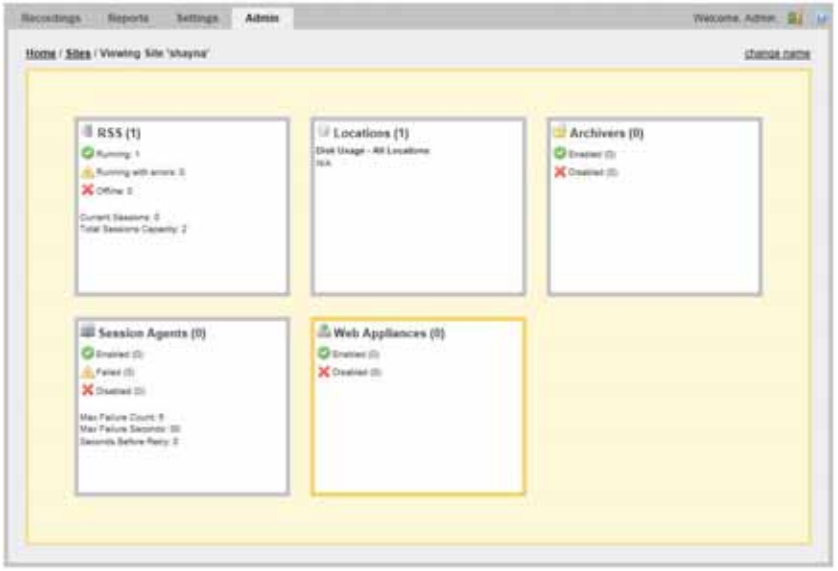
Adding a Session Agent

To add a Session Agent:

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



The following page displays.

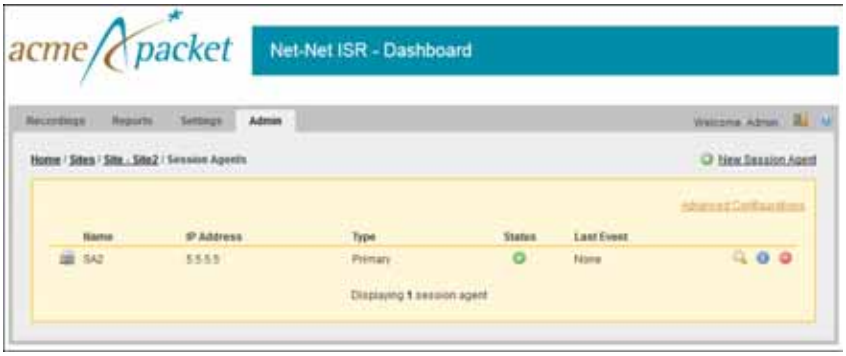


The following table describes the information that displays in the Session Agents component box.

Archivers Information	Description
Enabled	Total number of Session Agents enabled on this Site.
Failed	Total number of failed Session Agents on this Site.

Archivers Information	Description
Disabled	Total number of Session Agents disabled on this Site.
Max Failure Count	Total number of failures endured by all Session Agents for this Site before they are disabled.
Max Failure Seconds	Length of time, in seconds, for which the Session Agents for this Site can have failures before they are disabled.
Seconds Before Retry	Length of time, in seconds, that the Session Agents for this Site wait to retry a connection after a failed attempt has occurred.

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



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

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

3. Click **New Session Agent**. The following dialog box displays.

4. **Name**—Enter a name for the new Session Agent. Valid values are alpha-numeric characters. For example, SA2.
5. **IP Address**—Enter the IP address (in dotted decimal format), for the new Session Agent. Value must be entered in the format 0.0.0.0. For example, 123.243.3.5.
6. **Type**—Select the type to associated with this Session Agent you are adding. Valid values are:
   - **Primary** - The site uses this Session Agent as the Primary Session Agent to transfer calls to an agent or to the PSTN. By default, the Primary Session Agent is disabled if there are more than 5 failures in 30 seconds. If this occurs, the Session Agent is disabled for 5 minutes.
   - **Failover** - The site uses this Session Agent as the secondary (or failover) Session Agent to transfer calls to an agent or to the PSTN. The site uses this Session Agent ONLY if the primary Session Agent is inactive or has failed.

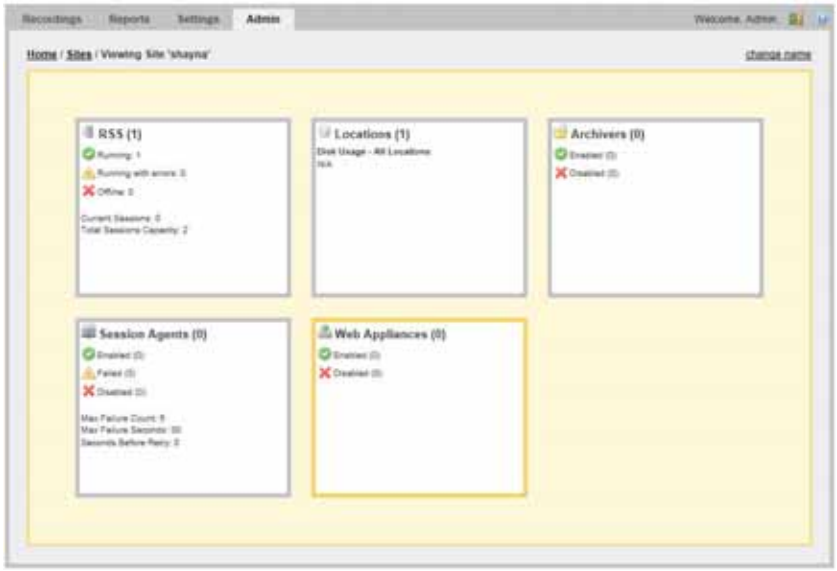
   Note: You can define multiple Primary Session Agents. The ISR load balances calls across all Primary Session Agents.
7. Click **Create**. The new Session Agent displays on the Session Agent page.

Editing a Session Agent

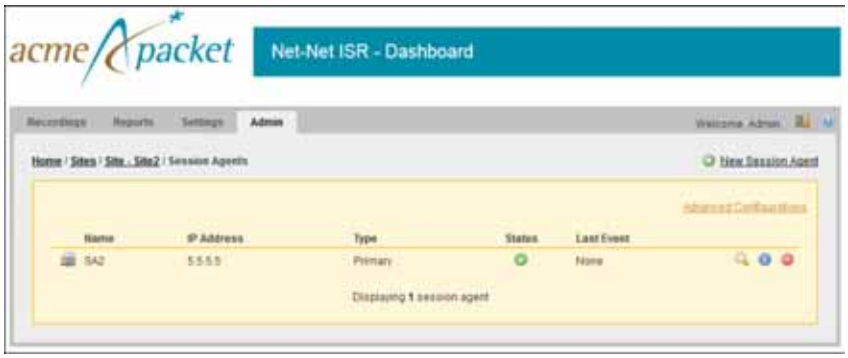
You can edit an existing Session Agent configuration if required.

To edit a Session Agent:

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



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



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

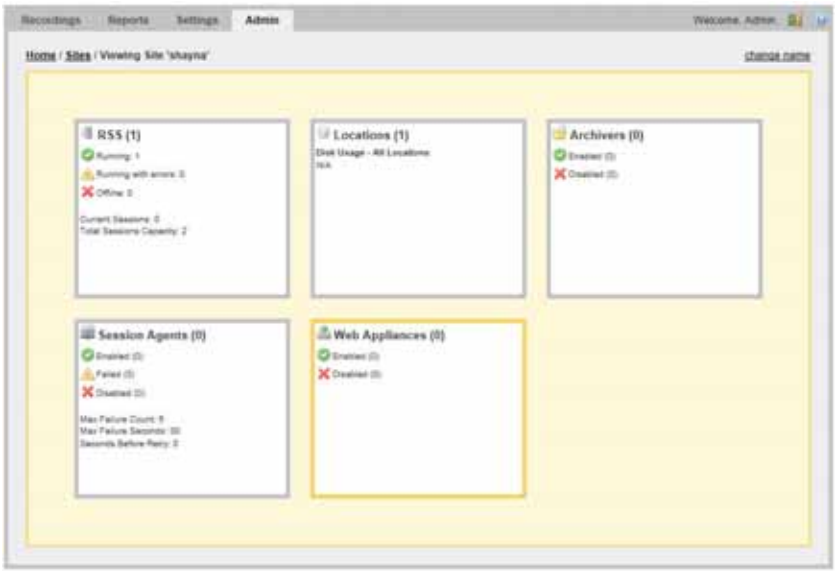
4. Edit the parameters for the Session Agent as applicable using the procedures defined in Adding a Session Agent, starting at Step 4.
5. **Status**—Select whether or not to enable the Session Agent for the current Site. Valid values are:
   - **Enabled** - Enable this Session Agent for the current Site.
   - **Disabled** - Disable this Session Agent for the current Site.
6. When you are finished editing the Session Agent, click <**Update**>. The changes are saved to the ISR database and display on the Session Agents page.

Deleting a Session Agent

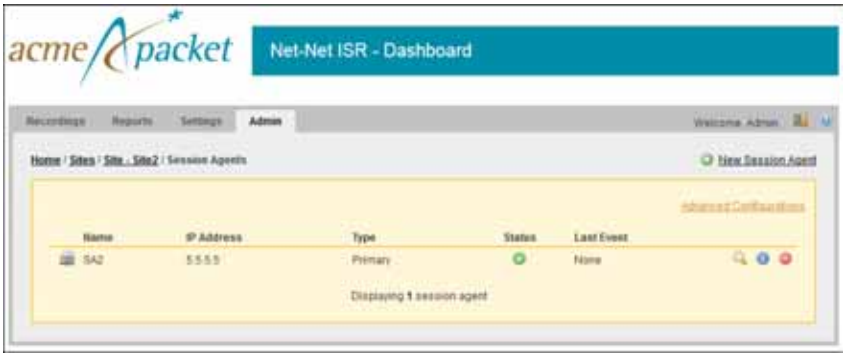
You can delete a Session Agent if required.

To delete a Session Agent:

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



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



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

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

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

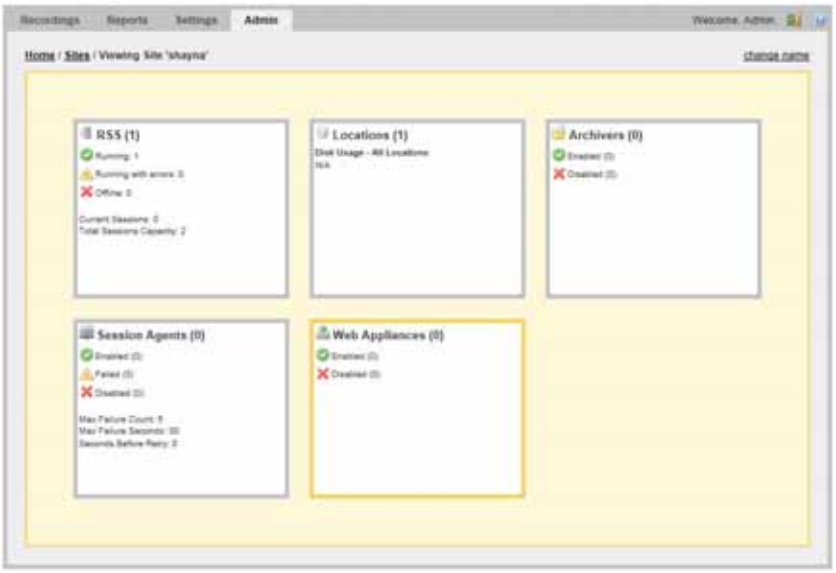
Warning: Once you delete a Session Agent, it cannot be recovered.

Display Events for a Session Agent

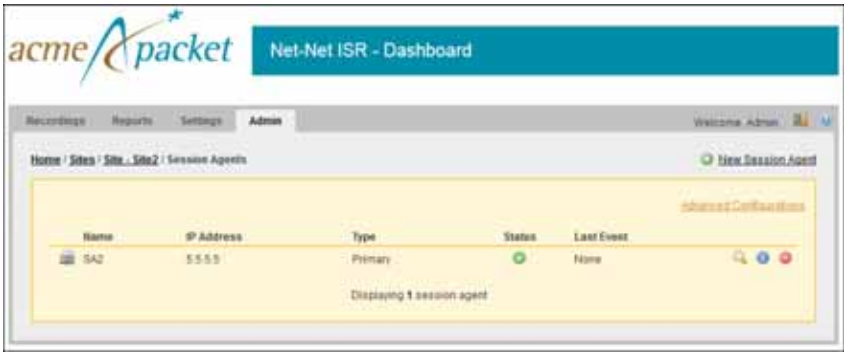
You can display the events that occur for each Session Agent by clicking the Events icon. Events include information on the date, time, time zone, and User of the event. If no events have occurred for the Session Agent, a message, "*There are no Events for this Session Agent*" displays.

To display events for a Session Agent:

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



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



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

   The Event list is read-only.

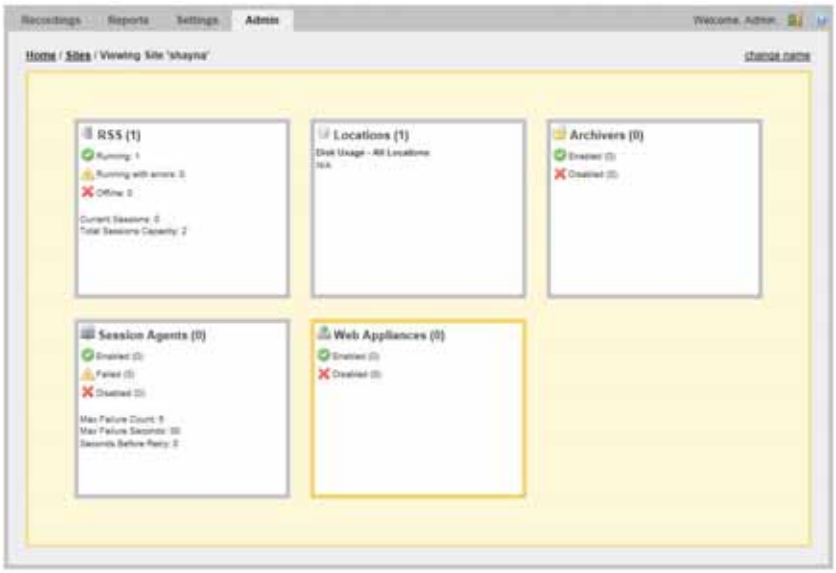
4. Click **X** in the upper-right corner to close the Events box.

Advanced Configuration for Session Agents (Site-wide)

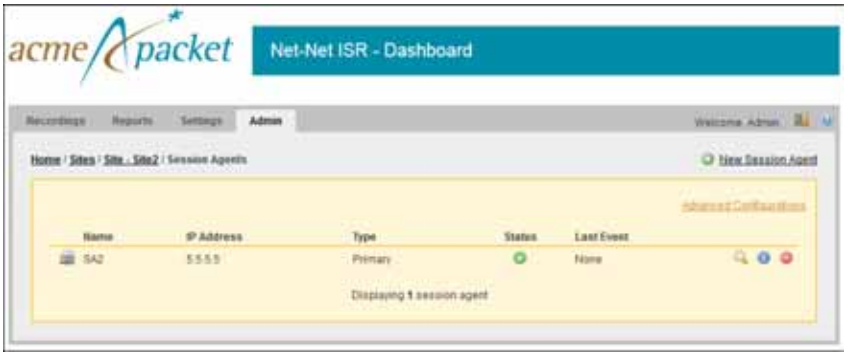
You can configure specific advanced configuration parameters that apply to all Session Agents for a single Site.

To configure advanced parameters for Session Agents:

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



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



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

4. **Max Failure Count**—Select the number of failures that the Session Agent endures before it is disabled. Valid values are **1** through **100**. Default is **5**.
5. **Max Failure Seconds**—Specify the length of time, in seconds, for which the Session Agent can have failures before it is disabled. Valid values are **1** through **300** seconds (5 minutes). Default is **30** seconds.
6. **Seconds Before Retry**—Specify the length of time, in seconds, that the Session Agent waits to retry a connection after a failed attempt has occurred. Valid values are **0** through **300** seconds (5 minutes). Default is **0** seconds.
7. Click **Update**. The settings apply to all the Session Agents for the current Site. The following message displays in the dialog box:

   "*Updated successfully*".

Managing Web Appliances

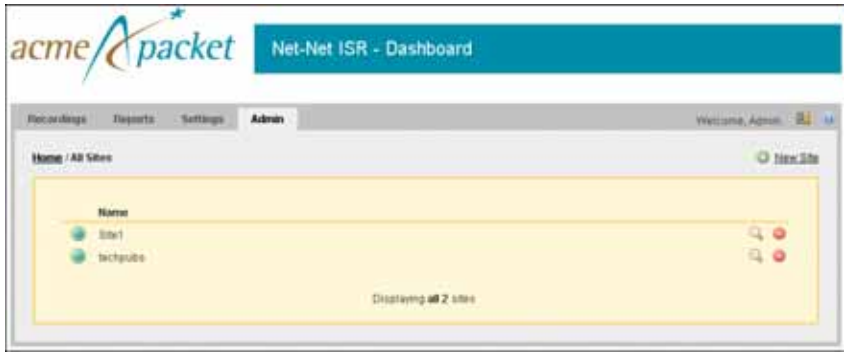
A Web Appliance allows the ISR to connect to a Web Service to push call recording data to a remote storage area. The **Web Appliances** page allows you to edit or delete information about an Appliance, or add a new Appliance associated with a Site configured for the ISR. This page displays the route(s)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

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

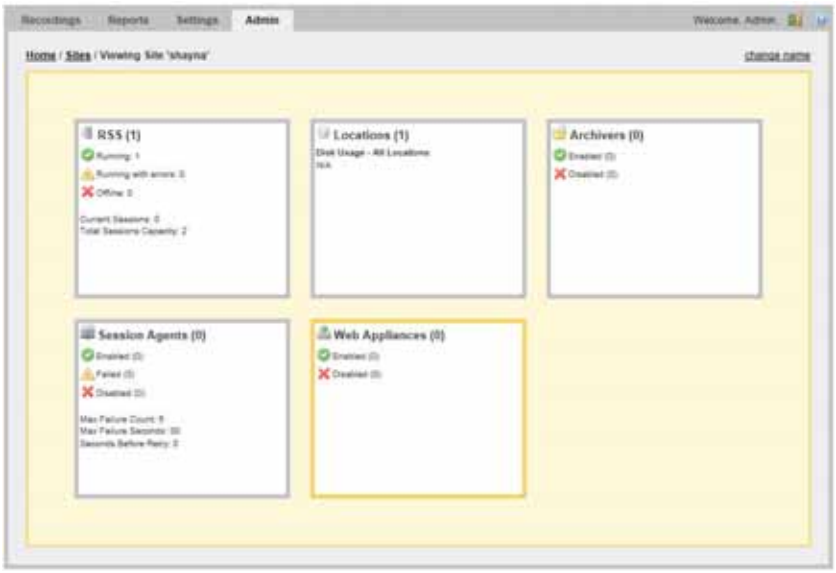
Adding a Web Appliance

To add a Web Appliance:

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



The following page displays.



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

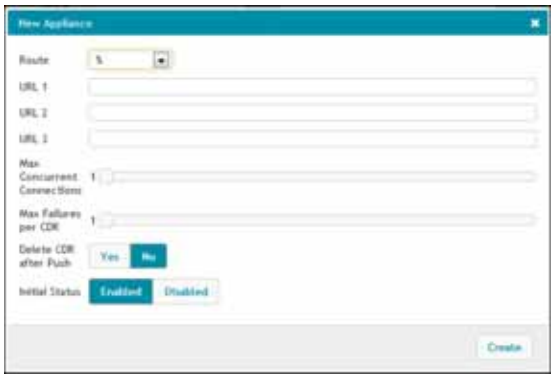
Archivers Information	Description
Enabled	Total number of Web Appliances enabled on this Site.
Disabled	Total number of Web Appliances disabled on this Site.

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

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

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

3. Click **New Web Appliance**. The following dialog box displays.



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

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

   Note: A domain name may have a secure connection using "https" as well.

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

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

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

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

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

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

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

10. **Delete CDR after Push**—Select whether or not the ISR deletes the call recording detail record after the Web Service has completed pushing the data to the ISR.

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

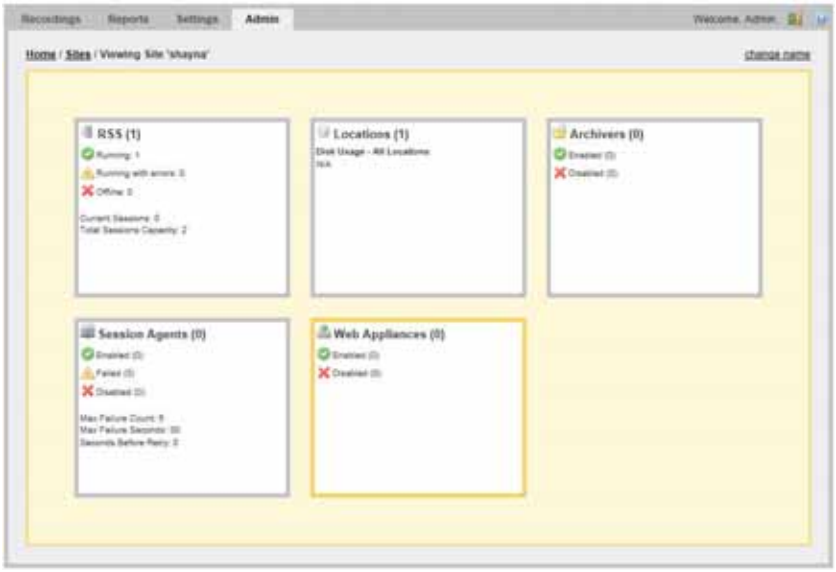
11. **Initial Status**—Select whether or not the Web Appliance is available to connect to the ISR. Valid values are:
    - **Enabled** (default) - Indicates the Web Service is available to the ISR for connection.
    - **Disabled** - Indicates the Web Service availability is not currently available to the ISR for connection.
12. Click **Create**. The new Web Appliance displays on the Web Appliance page.

Editing a Web Appliance

You can edit an existing Web Appliance configuration if required.

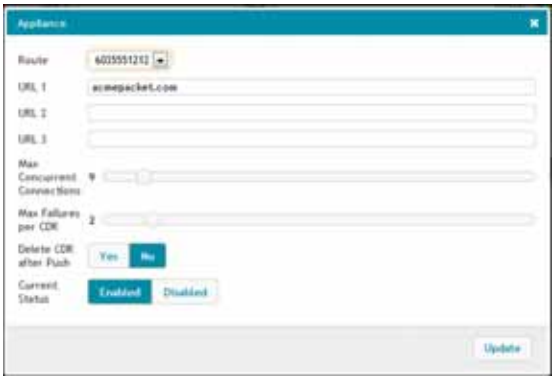
To edit a Web Appliance:

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



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

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



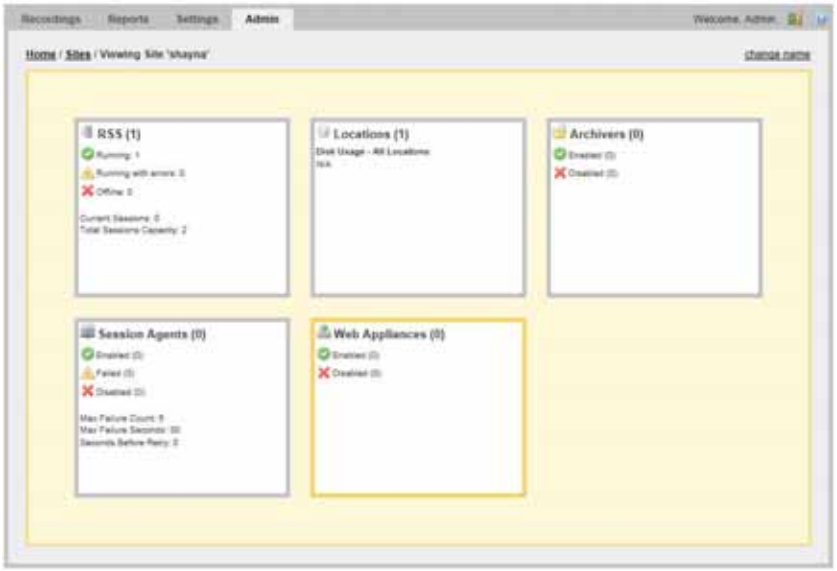
4. Edit the parameters for the Web Appliance as applicable using the procedures defined in Adding a Web Appliance, starting at Step 4.
5. **Current Status**—Select whether or not to enable the Web Appliance for the current Site. Valid values are:
   - **Enabled** - Enable this Web Appliance for the current Site.
   - **Disabled** - Disable this Web Appliance for the current Site.
6. When you are finished editing the Web appliance, click **Update**. The changes are saved to the ISR database and display on the Web Appliances page.

Deleting a Web Appliance

You can delete a Web Appliance if required.

To delete a Web Appliance:

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



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

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

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

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

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

---

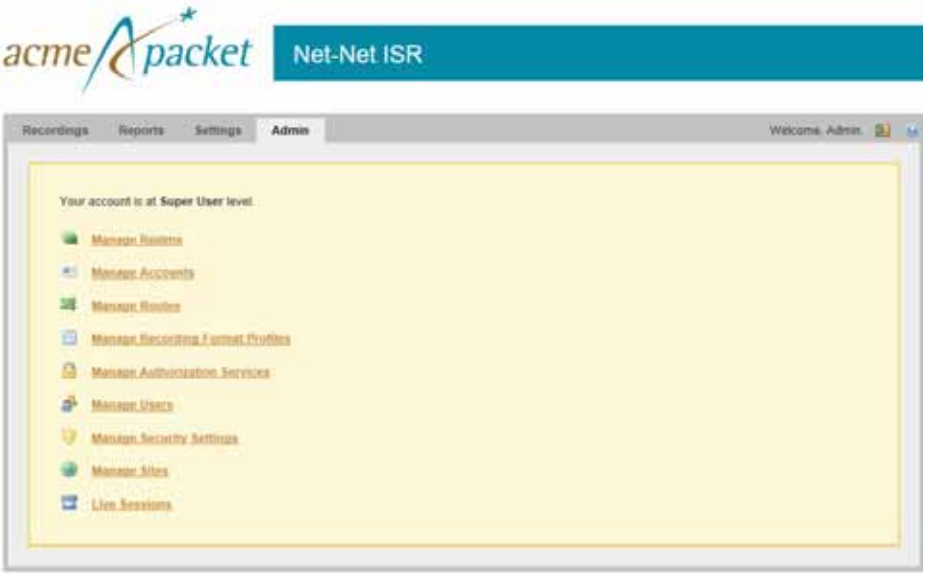
8 Viewing Live Sessions

Introduction

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

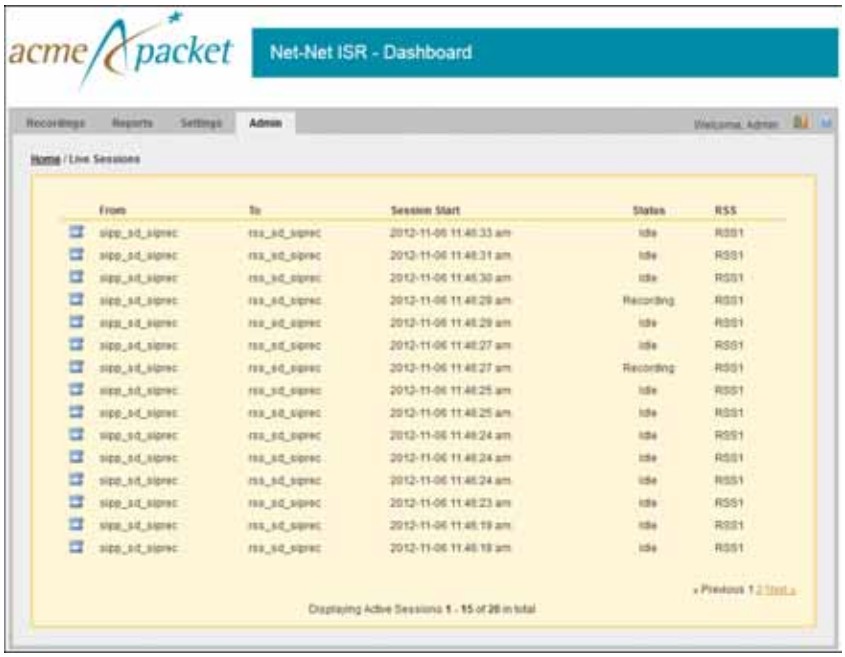
Manage Live Sessions

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



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

Lives Sessions Page



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

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 GMT time when the active session began.
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.

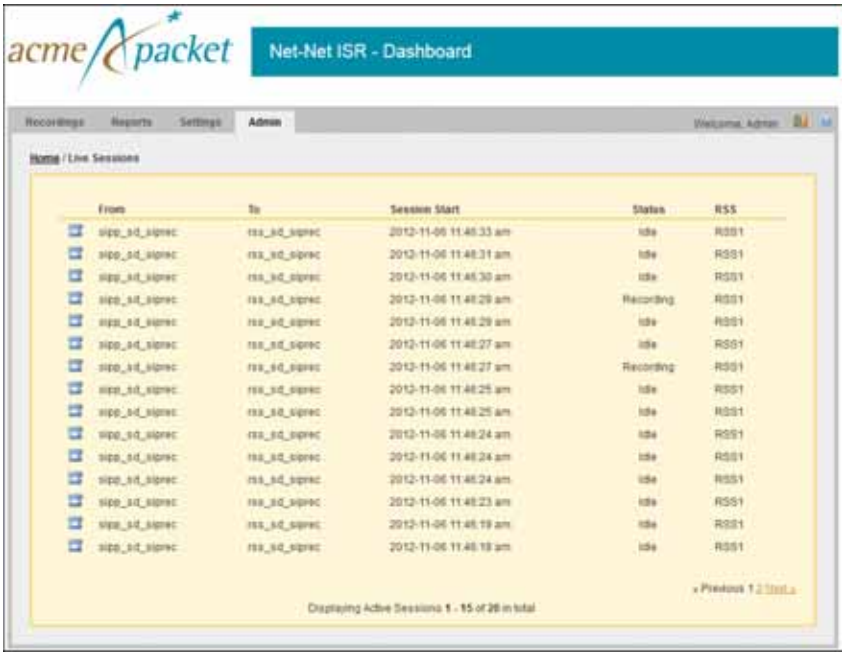
If more than 15 calls display on a single page, click the **Next** and **Previous** links to navigate between pages of the Live Sessions list.

Viewing Live Sessions

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

To view the Live Sessions:

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



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

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

9 Managing Recordings

Introduction

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

Manage Recordings

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

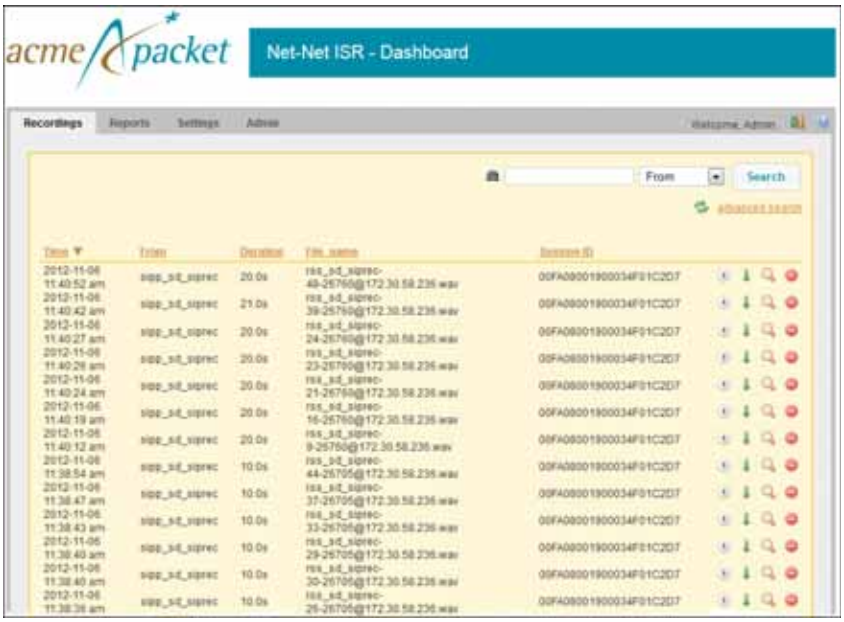
> **Note:** Recordings that display are dependant on the level of user currently logged into the ISR Dashboard.

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

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

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

Recordings Page



The following table describes each column on the Recordings page.

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

Playing a Recording

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

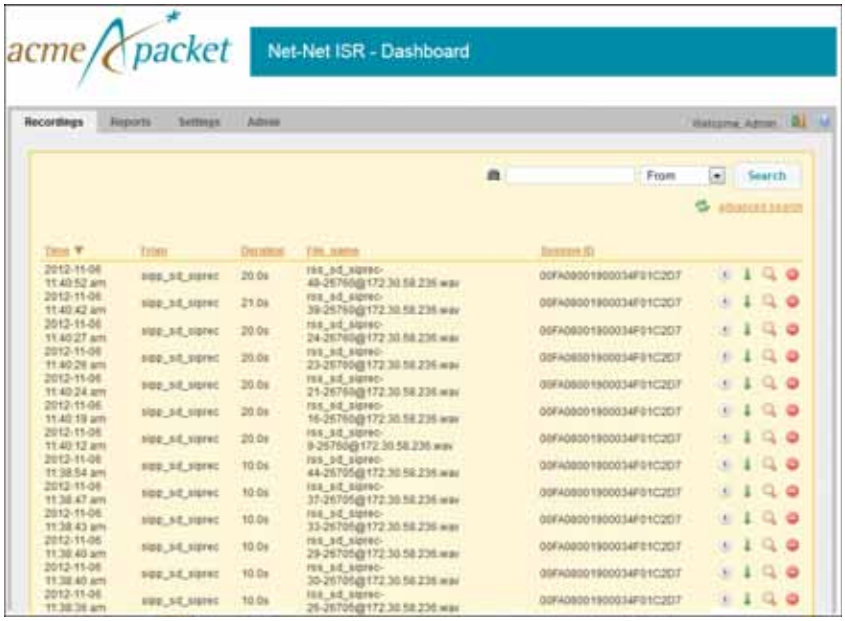
> **Note:** The recording's metadata is saved in the ISR database.

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

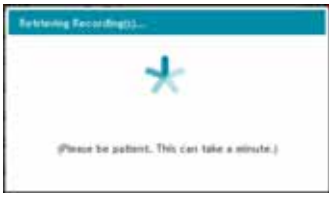
> **Note:** Before playing recordings, make sure you have a media application that plays audio files with a "*.wav*" format. For more information about the software requirements and recommendations for playing recordings, see Requirements/Recommendations.

To play a recording:

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



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



> **Note:** To find a specific recording, perform a search using the **Advanced Search** link in the upper-right corner of the page. For more information, see Search Tools.

The Recordings page refreshes depending on the value set at *Settings->Refresh Rate (seconds)*. Default is every 30 seconds. For more information about setting the Refresh rate, see Dashboard Settings.

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

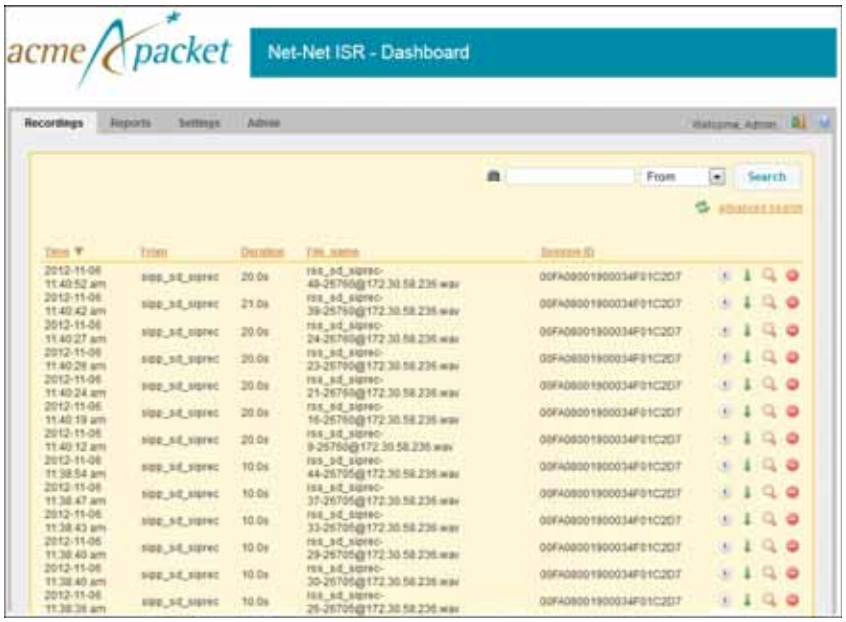
Viewing and Editing Details of a Recording

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

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

To play a recording from the details page:

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



2. Choose a recording and click the Details icon. The following dialog box displays.

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

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

To play the recording, click the recording file name.

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

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

Recording Details

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

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

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

- Write notes about the call session.
- Transcribe the conversation that took place in the call session.

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

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

To display and specify details:

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

Recording: 'rss_sd_siprec-1-16414@172.30.58.237.wav'
Account Name: System
Session ID: 00FA00001900034F01C2D7
From: sipp_sd_siprec
To: rss_sd_siprec
Duration: 10.0s
Start Time: 2012-12-11 10:13:28 pm

2. Click **Details**. The following information displays.

RSS: RSS_1 (172.30.58.222)
RSS Ingress Call ID: 1-16414@172.30.58.237
Complete Transaction: No
Hours: 0.0

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

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

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

> **Note:** The **Custom Data Fields 1** through **4** must be enabled for editing. For more information about entering values and enabling the Custom Data Fields, see Custom Data.

4. **Complete Transaction**—Select whether or not the call session is completed for this recording. For example, if a caller calls into a Technical Support Center for problems with his PC, the call is recorded. If the problem was not resolved on the initial call session, the reviewer can select "No" for the Complete Transaction field, indicating that the problem was not resolved on this call. Valid values are:

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

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

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

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

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

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

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

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

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

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

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

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

Archiving Recordings Permanently

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

You can also flag a recording to remain archived permanently.

To flag a recording to never expire:

1. After logging into the ISR Dashboard, click **Find Recordings** or click **Recordings** in the top menu bar.
2. Choose the recording you want to flag and click the Details icon.

The Recording's detail page displays.

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

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

Recording Session Metadata

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

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

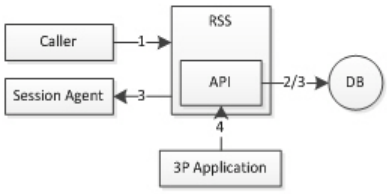
The value of this unique ID is stored in the lookup tables with the session data on the CIS for recording control, and can be viewed in the meta-data details of a recording and used as a means of searching for a recording.

The fields in the SIP Header for this feature are:

- **ingress_callid** - RSS uses the call-id in the SIP Header of the initial INVITE to populate this field.
- **egress_callid** - RSS initiates a second call leg (egress) for pass-through (or Record & Save) configurations and uses the new call leg's call-id to populate this field. (When the RSS is acting as a B2BUA).
- **isr_ucid** - RSS matches the X-ISR-UCID to the SIP Header, then populates this field.

  Note: The ingress_callid is always populated. The egress_callid may not be populated for calls with only one participant. The isr_ucid is only populated for calls where the X-ISR-UCID SIP header is present in the ingress INVITE.

The following illustration shows the call flow using the call control unique ID on the NN-ISR.



1. The ISR receives a SIP INVITE with optional X-ISR-UCID header.
2. The VMG_CHANNEL_LOOKUP table is updated with the ingress_callid and isr_ucid.

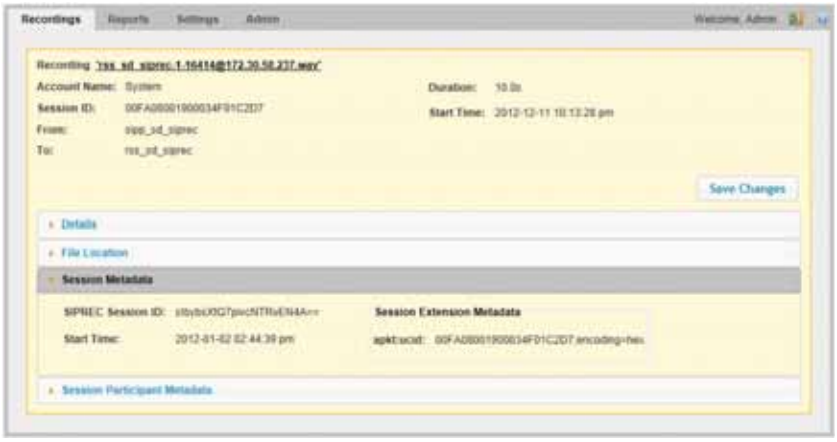
3. The ISR sends an INVITE to the Session Agent and updates the egress_ucid if applicable.
4. Recording control is now possible from a third-party application using either the isr_ucid, ingress_ucid, or the egress_ucid.

You can configure the X-ISR-UCID header field using the standard RSS configuration file, *vmgConfig.xml*. This allows you to customize the SIP header field without having to make changes to your application. For more information on configuring X-ISR-UCID in the vmgConfig.xml file, see the *Interactive Session Recorder Installation Guide*.

To view Session Metadata:

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

2. Click **Session Metadata**. The following information displays.



The **SIPREC Session ID** field displays the SIP Recording Session ID assigned to the call recording session at the time the call was received by the RSS.

The **Start Time** field displays the date and GMT time the call recording session began. The date and time are based on the time zone configured for the Account.

The **Session Extension Metadata** displays the Unique Caller ID (ucid) assigned by the ISR and indicates the ID of the incoming call.

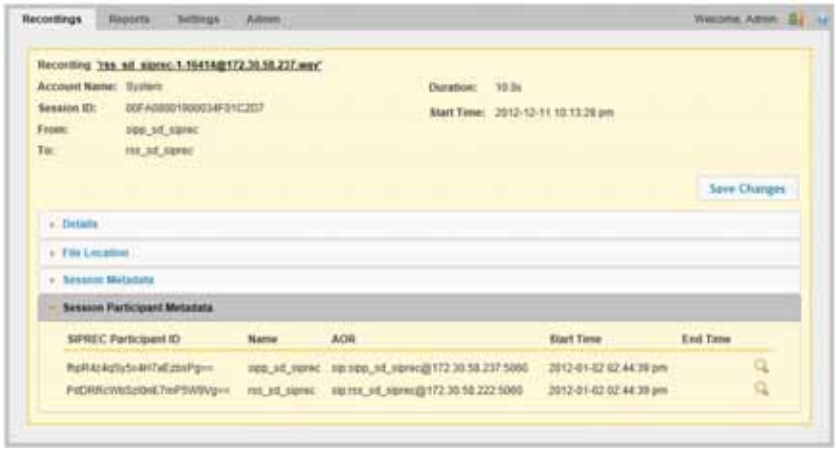
Recording Session Participant Metadata

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

To view Session Participant Metadata:

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

2. Click **Session Participant Metadata**. The following information displays.



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

Column Heading	Description
SIPREC Participant ID	Specifies the ID of the incoming caller who is the SIPREC participant on the recording.
Name	Specifies the From SIP URI name. This is the URI from where the call session was coming.
AOR	Specifies the address of record (AOR) associated with the call that was recorded.
Start Time	Specifies the date and GMT time when the active session recording began.
End Time	Specifies the date and GMT time when the active session recording ended.
	Displays additional metadata information about the participant if it exists.

3. Choose a SIPREC Participant ID and click the Details icon to display additional metadata information about the participant. The following box displays.

Information in this box can include metadata for:

- apkt:ucid
- extTrackingID
- ServiceProviderID
- userID
- groupID
- callID
- callingPartyNumber
- calledPartyNumber
- newExtTrackingID
- apkt:in-realm
- apkt:P-Asserted-Identity
- apkt:Diversion
- apkt:request-uri

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

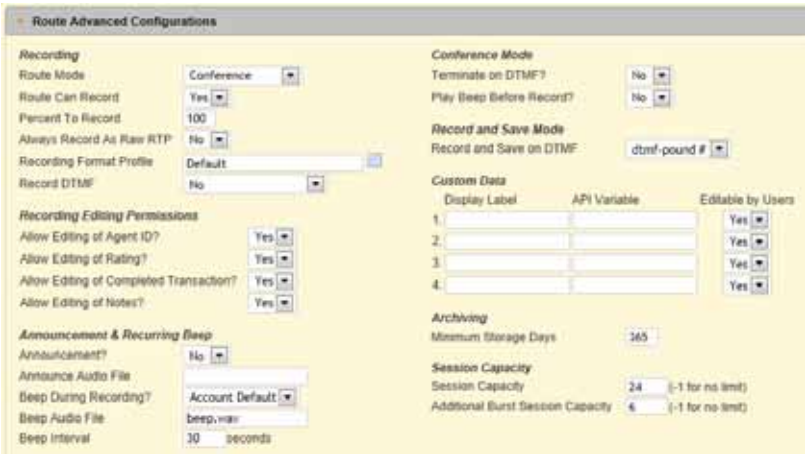
Displaying DTMF Data in Recording's Details

You can configure the ISR to display DTMF details within a call's recording details for digits transmitted via RFC 2833 and SIP INFO. The **DTMF Logging** parameter has been created which allows you to specify whether or not to display DTMF details on either a per-route or per-account basis.

To enable the ISR to display DTMF details for a particular route:

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

   A list of all routes configured on the ISR displays.
3. Click the route on which you are enabling DTMF details.
4. Click **Route Advanced Configuration**.

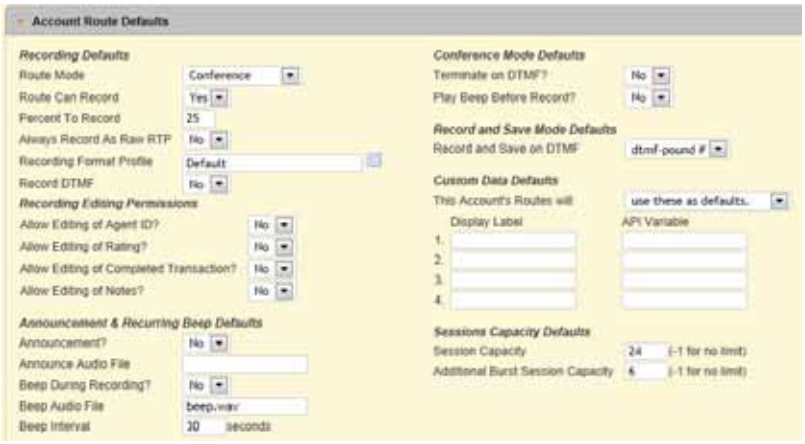


5. **Record DTMF**—Select whether or not to display DTMF details. Valid values are:
   - Use account or system default—This route defaults to its account's behavior. This is the default value.
   - No—No DTMF details appear in the recording details.
   - Yes—DTMF details appear in the recording details.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

To enable the ISR to display DTMF details for a particular account:

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

   A list of all accounts configured on the ISR displays.
3. Click the account on which you are enabling DTMF details.
4. Click **Account Route Defaults**.



5. **Record DTMF**—Select whether or not to display DTMF details. Valid values are:
   - No—No DTMF details appear in the recording details. This is the default value.
   - Yes—DTMF details appear in the recording details.
6. Click **Update**.

To view DTMF data in recording details:

1. After logging into the ISR Dashboard, click **Find Recordings** or click **Recordings** in the top menu bar.
2. Choose the recording you want to view and click the Details icon.

   The Recording's detail page displays.

3. Click **DTMF Events**. The DTMF data appears.

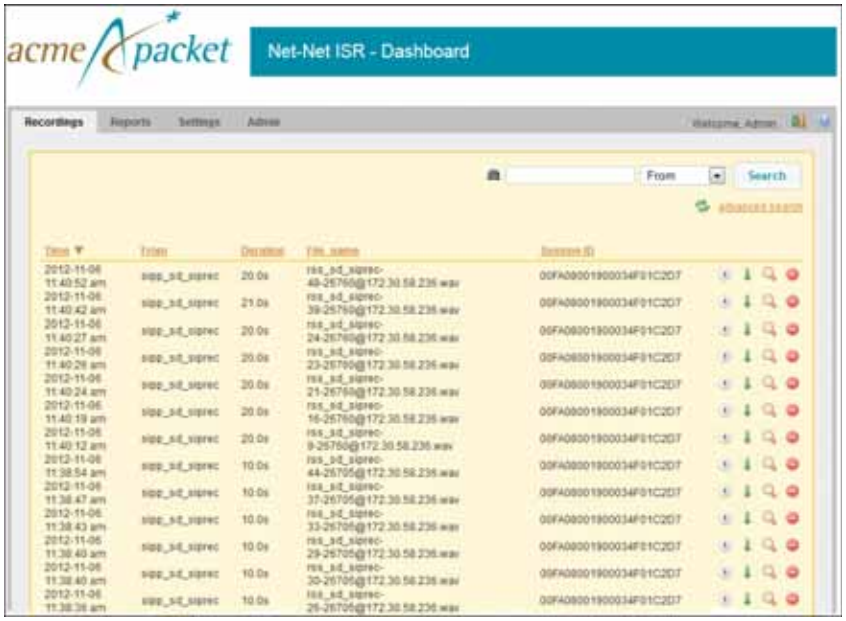
You can zoom in on a particular area of the DTMF Events graph by highlighting the section you want to view. To get back to the original graphical view, click **Reset zoom**.

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.

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

---

10 Managing Reports

Introduction

The ISR allows you to generate call usage and billing statistical reports using date and route filters. This chapter describes the type of reports you can generate and filters you can use to generate the reports.

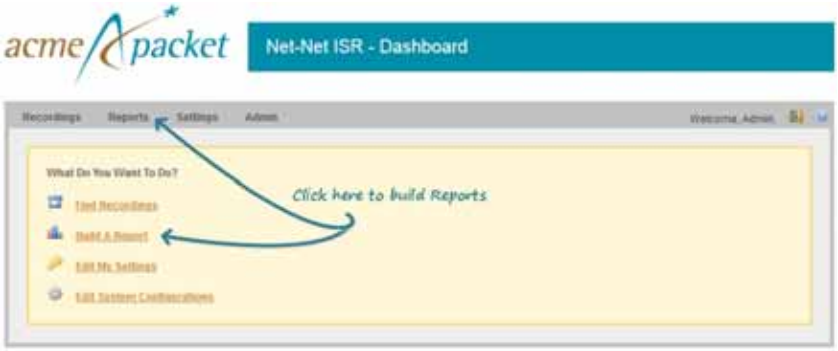
Manage Reports

The ISR provides the following types of reports you can generate:

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

You can run these reports for the current month or the previous month, or specify a date range.

You can access the Reports from the Home page by clicking **Build A Report** (or by clicking **Reports** on the top menu bar).



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.

To generate a Usage Report:

1. After logging into the ISR Dashboard, click **Build a Report** on the Home Page (or **Reports** on the main menu bar). The Reports page displays.

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

To generate a report by month:

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

To generate a report by range:

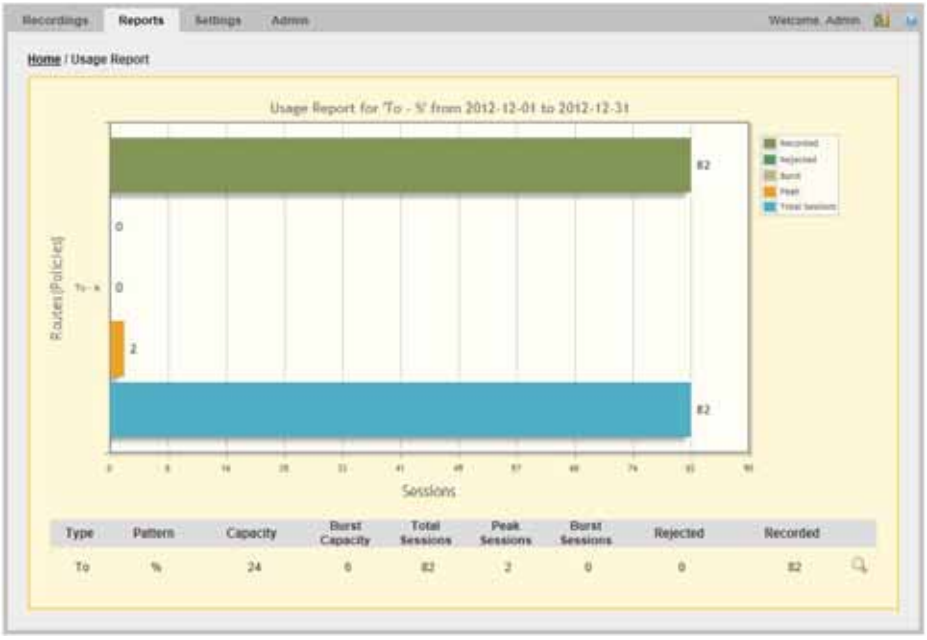
5. Select **By Range**. The “From Date” and “To Date” fields display.
6. **From Date**—Click the cursor in the text box or click the Calender icon to display the calendar.
7. Click the date from where you want to begin to include the report data. Use the arrow keys in the calendar to change months.
8. **To Date**—Click the cursor in the text box or click the Calender icon to display the calendar.
9. Click the date from where you want to end the inclusion of the report data. Use the arrow keys in the calendar to change months.

To select a route:

10. **Select Route**—Select a route or routes to include in the report. Valid values are dependant on the routes currently configured in the ISR database.

    Note: To select multiple routes, click on a route in the selection box, press and hold the <**Ctrl**> key, and select additional routes.

11. Click **Usage Reports**. The **Generate Report** button displays.
12. Click **Generate Repor**t to generate the Usage Report. The following report displays.



The Usage Report displays the information in bar graph format at the top of the page, and in data format at the bottom of the page.

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

Usage Report Bar Graph Descriptions

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

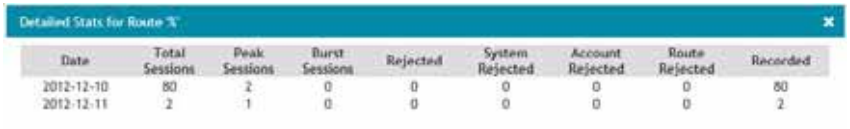
The following table describes each column in the data format section of the report.

Usage Report Data Format Descriptions

Column	Description
Route	Route(s) included in this Usage Report.
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.

Column	Description
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.

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



Billing Reports

Billing Reports show information about calls that use the routes configured on your ISR. Billing Reports include:

- Route used for calls
- Number of sessions provisioned on the route
- Number of provisioned burst sessions on the route
- Total number of calls initiated using the route
- Number of calls made during peak time on the route
- Number of calls that used burst sessions on the route
- Number of calls rejected on the route

You can filter the call data by month or by date range, and select a single or multiple routes to display in the report. You can use this information for billing purposes as required.

To generate a Billing Report:

1. After logging into the ISR Dashboard, click **Build a Report** on the Home Page (or **Reports** on the main menu bar). The Reports page displays.

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

To generate a report by month:

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

To generate a report by range:

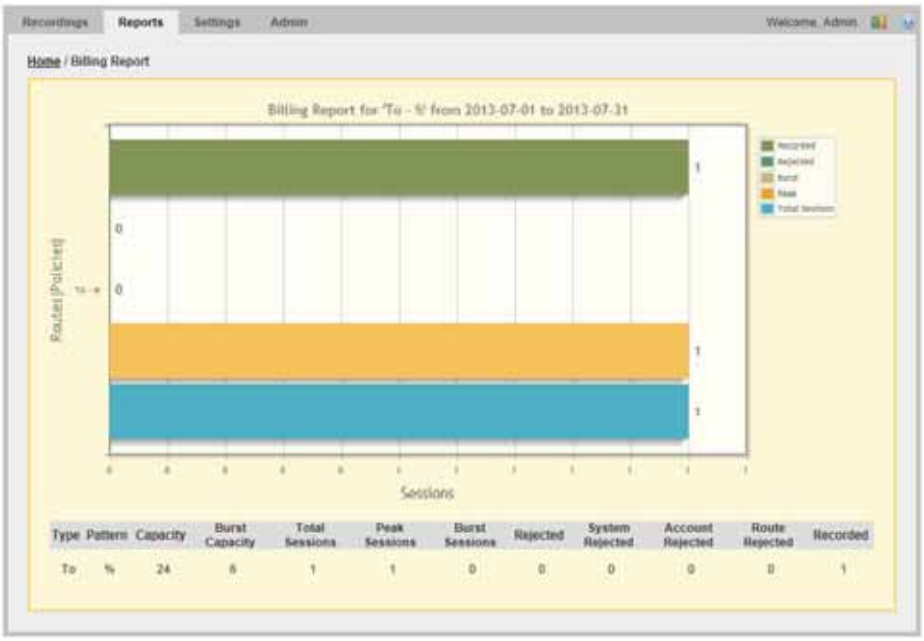
5. Select **By Range**. The “From Date” and “To Date” fields display.
6. **From Date**—Click the cursor in the text box or click the Calender icon to display the calendar.
7. Click the date from where you want to begin to include the report data. Use the arrow keys in the calendar to change months.
8. **To Date**—Click the cursor in the text box or click the Calender icon to display the calendar.
9. Click the date from where you want to end the inclusion of the report data. Use the arrow keys in the calendar to change months.

To select a route:

10. **Select Route**—Select a route or routes to include in the report. Valid values are dependant on the routes currently configured in the ISR database.

    Note: To select multiple routes, click on a route in the selection box, press and hold the <**Ctrl**> key, and select additional routes.

11. Click **Billing Reports**. The **Generate Report** button displays.
12. Click **Generate Repor**t to generate the Billing Report. The following report displays.



The Billing Report displays the information in bar graph format at the top of the page, and in data format at the bottom of the page.

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

Billing Report Bar Graph Descriptions

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

Column	Description
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.

11 Remote Archival Webservice

Introduction

Remote Archival allows customers of hosted call recording providers to pull their recordings to a premise location. Utilizing a secure connection between the premise and service provider applications, a Remote Archival client connects to the Remote Archival Webservice and retrieves all recordings for a single account configured on the host platform.

The Remote Archival process includes:

1. Moving recording files to a remote file system. The files may be optionally deleted from the source RSS/NAS/SAN after the client confirms a successful delivery.
2. Moving recording metadata for the configured account, including the standard recording data from the recordings table, SIPREC metadata, and ISR custom fields, to a remote store. The data may be optionally deleted from the source index after a successful push.

To enable the Remote Archival Webservice, you must configure at least one Remote Archival user and at least one account. This user's username and password are required in the client requests.

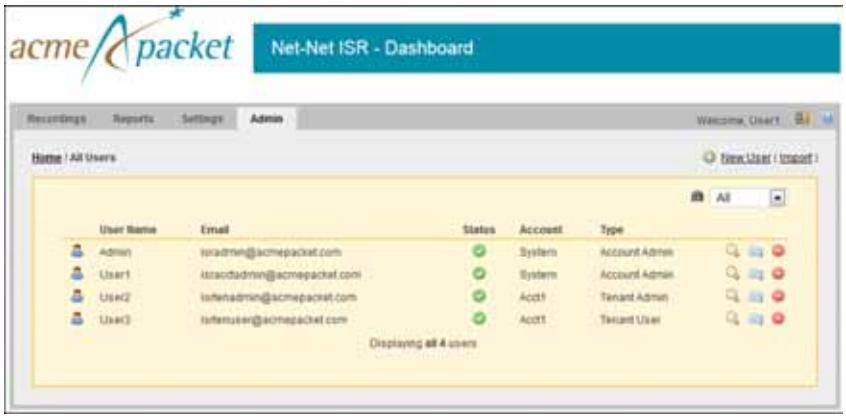
Configuring Remote Archival Users

Remote Archival users are configured under the ISR Dashboard's Manage Users link.

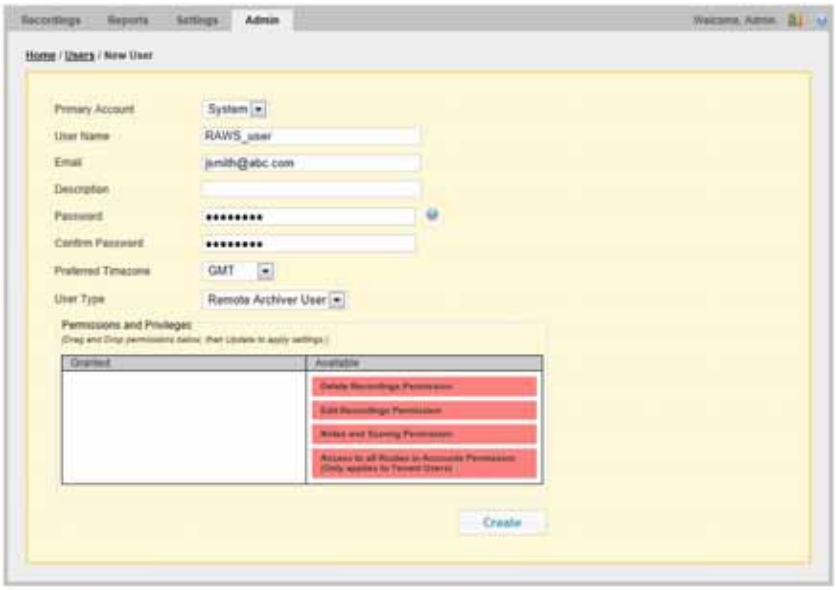
Note: A Remote Archival user is specific to the Remote Archival Webservice only and cannot log into the ISR Dashboard.

To configure a Remote Archival user:

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



3. Click **New User**. The New User page appears.



4. **Primary Account**—Select the primary account to assign to this Remote Archival user. Valid values are dependant on the accounts currently configured in the ISR. The default value is **System**.

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

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

   <username>@<host server>.<DNS (*.com, .org., .net., .edu*)*>*

   For example, jsmith@abc.com.

7. **Password**—Enter a password for the user to specify when logging into the Remote Archival Webservice. By default, the password must contain letters and numbers, have at least one uppercase letter, and be at least 8 characters long. Valid values are alpha-numeric and special characters.

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

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

Time Zone Table

Time Zone	Location
GMT-12 (default)	**IDLW - International Date Line West**
GMT-11	**NT - Nome**
GMT-10	**AHST - Alaska-Hawaii Standard** **CAT - Central Alaska** **HST - Hawaii Standard**
GMT-9	**YST - Yukon Standard**

Time Zone	Location
GMT-8	**PST - Pacific Standard** Los Angeles, CA, USA
GMT-7	**MST - Mountain Standard**
GMT-6	**CST - Central Standard** Mexico City, Mexico Saskatchewan, Canada
GMT-5	**EST - Eastern Standard** Bogota Lima, Peru New York, NY, USA
GMT-4	**AST - Atlantic Standard** Caracas La Paz
GMT-3	Brasilia, Brazil Buenos Aires, Argentina Georgetown, Guyana
GMT-2	**AT - Azores**
GMT-1	**WAT - West Africa** Azores, Cape Verde Islands
GMT	London, England Dublin, Ireland Edinburgh, Scotland Lisbon, Portugal Reykjavik, Iceland Casablanca, Morocco
GMT+1	**CET - Central European** Paris, France Berlin, Germany Amsterdam, The Netherlands Brussels, Belgium Vienna, Austria Madrid, Spain Rome, Italy Bern, Switzerland Stockholm, Sweden Oslo, Norway
GMT+2	**EET - Eastern European** Athens, Greece Helsinki, Finland Istanbul, Turkey Jerusalem, Israel Harare, Zimbabwe
GMT+3	**BT - Baghdad** Kuwait Nairobi, Kenya Riyadh, Saudi Arabia Moscow, Russia
GMT+4	Abu Dhabi, UAE

Time Zone	Location
GMT+5	Kazakhstan (western-Aqtau) Maldives (Male) Pakistan (Islamabad, Karachi) Russia Tajikistan (Dushanbe) Turkmenistan (Ashkhabat) Uzbekistan (Tashkent) India (New Delhi, Calcutta) Sri Lanka (Colombo) Nepal (Katmandu)
GMT+6	Bangladesh Bhutan Kazakhstan Kyrgyzstan Sri Lanka (formerly Ceylon)
GMT+7	Cambodia Christmas Island Indonesia Lao Thailand Vietnam
GMT+8	**CCT - China Coast**
GMT+9	**JST - Japan Standard**
GMT+10	**GST - Guam Standard**
GMT+11	Solomon Islands
GMT+12	**IDLE - International Date Line East** **NZST - New Zealand Standard** Wellington, New Zealand Fiji Marshall Islands

10. **User Type**—Select **Remote Archiver User** from the drop-down list.
11. Click **Create**.

Configuring Remote Archival Accounts

In addition to creating a Remote Archival-specific user to enable the Remote Archival Webservice, you must also configure it within the user's associated account.

To enable Remote Archival on an account:

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

3. Either select an existing account on which to enable Remote Archival or click **New Account**.

   Note: If you are creating a new account, configure it as you would any account. For more information on configuring accounts, see Chapter 3, Managing Realms/Accounts.

4. Click **Account Remote Archiver Server**.

5. **Client IP Address**—Enter the Remote Archival client's IP address.
6. **Remove Recordings**—When set to **On**, the associated metadata is deleted from the Index after the client confirms a successful delivery. Valid values are **On** and **Off**. The default setting is **Off**.
7. **Max Allowed Attempts**—The maximum number of unsuccessful downloads of an ISR recording until the recording is marked as failed and ignored in future Remote Archival "getList" requests. The default setting is **3**.
8. Click **Update**.

   Note: Remote Archival Webservice logging information can be found on the rWebservice host's /cxc_common/ISR/RemoteArchival/RemoteArchivalWebservice.log file.

Running the Remote Archival Client

The Remote Archival client is an application created specifically for developer testing purposes.

To run the Remote Archival client in a Windows environment:

1. Verify Java Version 5 or greater is installed on the Remote Archival client host.
2. Unzip the file "Remote Archival Client Development-Only Version <*number*>.zip to the install directory.
3. From a command line, change to the install directory and, depending on the operating system, execute **run.bat** or **run.sh** and hit <*Enter*>.
4. Follow the usage information provided in the response.

12 Securing the ISR

Introduction

This chapter describes how to configure security on the ISR.

SSL-Enabling the ISR Dashboard

You can enable serving pages with SSL to force SSL cookies. In the ISR, by default cookies are not forced through the Secure Sockets Layer (SSL).

To force the SSL cookies, you may need to generate a certificate and you must enable serving of pages in SSL.

To enable serving pages with SSL to force SSL cookies:

1. Enable SSL in nginx by editing the nginx configuration file (/opt/nginx/conf/nginx.conf) and edit the following SSL config lines to the following (edit paths and remove the '#' sign).

   ```
   # listen 443;
   # ssl on;
   # ssl_certificate /opt/nginx/conf/<pem_keystore_file>;
   # ssl_certificate_key /opt/nginx/conf/<pem_keystore_file>;
   # keepalive_timeout 60;
   ```

2. Add the following line below **keepalive_timeout 60;**:

   ```
   ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
   ```

3. Confirm the location of the SSL certificate and key currently being used.
4. Save the changes in the editor:
5. Enable secure cookies in the ISR Dashboard:
   - Edit /var/www/dashboard/current/config/initializers/session_store.rb
   - Inside of "actionController::Base.session = {.....}', add the new line

   ```
   :secure => true
   ```

   Note: You must add a comma to the end of the line for this to work properly.

   - Restart nginx by entering the command:

   ```
   service nginx restart
   ```

6. Edit the following line in the iptables configuration file (/etc/sysconfig/iptables) to open port 443:

   Change From:

   ```
   -A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
   ```

   Change To:

   ```
   -A INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
   ```

7. Restart the iptables service by executing the following command:

   ```
   service iptables restart
   ```

8. After the restart, confirm access of the application using HTTPS in a browser.

Generating a PEM Format Keystore

Generate a PEM format keystore if needed.

Note: Oracle recommends creating the keystore using Java 7.

1. The following is an example command.

```
>"C:\Program Files\Java\jre7\bin\keytool" -genkeypair -alias
<alias_of_choice> -keyalg RSA -ext san=ip:<dashboard_ip> -keystore
"<keystore_path>"
```

2. Using the keystore created by keytool, create the PKCS12 file with the following command:

```
keytool -v -importkeystore -srckeystore <keystore_path> -srcalias
<alias_of_choice> -destkeystore <pkcs12_keystore_path> -deststoretype
PKCS12
```

Once the PKCS12-formatted keystore has been successfully created, copy the PKCS12 keystore file to the ISR Dashboard host. From the Dashboard host, execute the following:

3. Using openssl, create the PEM format keystore by following this example command:

```
# openssl pkcs12 -in <pkcs12_keystore_file> -out
<keystore_filename>.pem
```

4. Once the .pem keystore is available, copy the file to the */opt/nginx/conf* directory.

SSL-Enabling the Remote Archival Webservice

You can configure the Remote Archival Webservice to handle HTTP requests over SSL.

To enable SSL on the Remote Archival Webservice:

1. Create a key on server. To do this, on the rWebservice host, generate the keystore by executing the following command (and follow the instructions).

```
/opt/jdk1.6.0_24/bin/keytool -genkey -alias <alias of choice> -keyalg RSA
-keystore /cxc_common/ISR/RemoteArchival/server.keystore
```

2. Import the certificate into the client's trustore. To do this, on the Remote Archival Webservice host export the certificate by executing the following command (and follow the instructions).

```
/opt/jdk1.6.0_24/bin/keytool -export -keystore
/cxc_common/ISR/RemoteArchival/server.keystore -alias <alias chosen>
-file /cxc_common/ISR/RemoteArchival/raws.crt
```

Transfer the newly-created file, raws.crt, from the rWebservice host to the Remote Archival Client host.

If the Remote Archival Client is a Java-based application, execute the following command (and follow the instructions).

```
/opt/jdk1.6.0_24/bin/keytool -import -alias <alias chosen> -file
/cxc_common/ISR/raws2.crt -keystore
/opt/jdk1.6.0_24/jre/lib/security/cacerts
```

Note: The password for the keystore is required and, by default, is "changeit". To change the password, execute the following command:

```
keytool -storepasswd -new <new_storepass> -keystore <JAVA_HOME>
/jre/lib/security/cacert
```

3. Edit and verify the RA Client's run.sh or run.bat files so that the -k parameter matches the keystore path.

Note: Some troubleshooting tips on the keystore:

- Exception:org.apache.axis2.AxisFault:java.lang.RuntimeException:Unexpected error: java.security.InvalidAlgorithmParameterException: the trustAnchors parameter cannot be left empty.
  - Your client keystore path is not valid.

- org.apache.axis2.AxisFault:sun.security.validator.ValidatorException:PKIX path building failed:sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certificate path to requested target.
    - Your keystore path is valid, but the keystore has not been updated with the RA WS exported certificate.

4. Configure the Remote Archival Webservice for SSL-only requests. To do this edit /opt/jboss/standalone/configuration/standalone.xml.

   Within the section marked by the following tag:

   ```
   <subsystem xmlns=”urn:jboss:domain:web:1.1” default-virtual-server=”default-host” native=”false”>
   ```

   add:

   ```
   <connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https" secure="true">
   <ssl name="ssl" key-alias="<alias chosen>" password="<key password>" certificate-key-file="/cxc_common/ISR/RemoteArchival/server.keystore" protocol=”TLSv1,TLSv1.1,TLSv1.2”/>
   </connector>
   ```

   Note:<*key_password*> refers to the password provided during the instructions to generate, export, and import the key.

   For JBoss to stop listening on port 8080, remove (or comment) the following lines in standalone xml:

   ```
   <connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="http"/>
   ```

5. Modify the Linux firewall to allow port 8443 instead of 8080 by editing:

   ```
   /etc/sysconfig/iptables
   ```

   Change the following line:

   ```
   -A INPUT -m state --state NEW -m tcp - tcp --dport 8080 -j ACCEPT
   ```

   To:

   ```
   -a INPUT -m state --state NEW -m tcp -p tcp --dport 8443 -j ACCEPT
   ```

   Restart the iptables service with the following command:

   ```
   service iptables restart
   ```

   Restart Jboss with the following command:

   ```
   service jboss restart
   ```

6. Modify the ISR API connection parameter for the RAWS to use HTTPS. To do this edit /opt/jboss/standalone/deployments/RemoteArchival.war/WEB-INF/web.xml. Find the section for baseApiUrl and change the param-value.

   Change the following line:

   ```
   http://<localhost>:8080/IsrApi/rest/
   ```

   To:

   ```
   https://<localhost>:8443/IsrApi/rest/
   ```

   It should now look like the following:

   ```
   <context-param>
                  <param-name>baseApiUrl</param-name>
                <param-value>https://localhost:8443/IsrApi/rest/</param-value>
            </context-param>
   ```

7. To confirm the new configuration, point a web browser to the Remote Archival Webservice JBoss root URL at:

   `https://<RA Webservice IP>:8443/IsrApi/`

   and confirm that it is accessible.

Adding User Accounts on the RSS

After the RSS has been installed, by default it has no configured users or authorization at the login. Once you have at least one user configured, authorization is limited to configured users only.

To configure users and authorization you must create a permissions group, create a user, and then assign the user to the appropriate permissions group.

The following is an example of configuring users and authorization via the CLI.

```
NN-ISR>config access
config access>config permissions basic
Creating 'permissions basic'
config permissions basic>exit
Do you want to commit your changes before you exit (y or n)? y
Do you want to update the startup configuration (y or n)? y
NN-ISR>config access
config access>config users
Creating 'users'
config users>config user testuser
Creating 'user testuser'
config user testuser>set password
password: ******************
confirm: ******************
config user testuser>set permissions access\permissions basic
config user testuser>exit
Do you want to update the startup configuration (y or n)? y
NN-ISR>
```

SSL-Enabling the RSS ISR API

You can configure the RSS ISR API to handle HTTP requests over SSL.

To enable SSL on the RSS ISR API:

1. Create a key on the RSS. To do this, on the RSS host, generate the keystore by executing the following commands (and follow the instructions).

   ```
   mkdir /home/jboss
   keytool -genkey -alias <alias of choice> -keyalg RSA -keystore
   /home/jboss/.keystore
   ```

2. Configure the RSS for SSL (or to allow SSL-only requests), edit /usr/local/jboss-7.1.1/standalone/configuration/standalone.xml.

   Within the section marked by the following tab:

   ```
   <subsystem xmins=”urn:jboss:domain:web:1.1” default-virtual-
   server=”default-host” native=”false”>
   ```

   Add:

   ```
   <connector name="https" protocol="HTTP/1.1" scheme="https" socket-
   binding="https" secure="true">
   <ssl name="ssl" key-alias="<alias chosen>" password="<keystore
   password>" certificate-key-file="/home/jboss/.keystore"
   protocol="TLSv1,TLSv1.1,TLSv1.2"/>
   ```

```
</connector>
```

Note: The <*keystore_password*> and <*alias_chosen*> values refer to the password provided and alias chosen in the instructions to generate the key in step 1.

3. Remove (or comment) the following lines in standalone xml for JBoss to stop listening on port 9000.

```
<connector name="http" protocol="HTTP/1.1" scheme="http" socket-
binding="http"/>
```

4. Restart JBoss with the following command from the Linux CLI:

```
/etc/init.d/jboss restart
```

5. Confirm the configuration by pointing a browser to the RSS JBoss root URL:

```
https://<RSS IP>:8443/IsrApi/
```

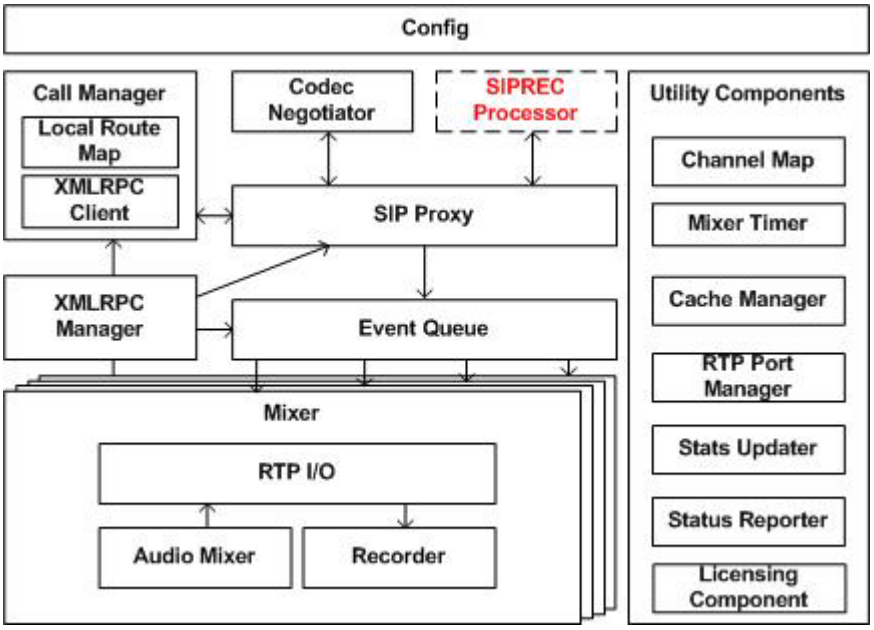
A ISR Software Diagrams and Call Setup Sequence

Overview

This appendix contains a high-level, software architecture diagram of the ISR platform along with a set of ladder diagrams describing interaction of the software components. This is for informational purposes only.

ISR Software Architecture Diagram

The following is a diagram of the ISR software architecture.



Description of Components

The components of the ISR consist of the following:

- RSS - Record Store Server
- CIS - Control Index Server

Each of these components are described if the following paragraphs.

Record Store Server (RSS)

The RSS consists of the following components:

- Call Manager - Using call state, channel and route information Call Manager handles account and platform-related call decisions.
- SIP Agent - Processor for SIP-related events.
- Channel Map - State storage and reference for active call information and available channels.
- Local Route Cache - Binary tree store of route-based information for call and recording decisions. Initializes reflecting the dashboard-driven route_config database table with periodic (configurable) updates mirroring changes in the table.
- Call Stats Updater - Processes call metrics and refreshes call and recording tables with call statistics.
- XML-RPC Server - Accepts and queues remote call and recording commands.
- XML-RPC Agent - Manages API requests and responses via XML-RPC.
- RTP Port Manager - Returns available RTP ports and maintains port status for SIP Agent.
- Event Queue - Prioritizes and stores call and other events
- Cache Manager - Local audio store which makes available audio content such as busy messages and beeps during recording.
- Mixer Channel - RTP support for sending, receiving, buffering, transcoding and mixing audio which contains the following:
  - RTP I/O - RTP input and output stream handling.
  - Audio Mixer - Audio stream processing for injecting platform or route-specific audio.
  - Recorder Thread - Manages audio and file stream processing.
- RSS API - offers ISR remote call and recording services along with resources for route and channel references in ISR database.
- VoiceXML API - VoiceXML resource for ISR API commands.
- RSS API Servlet - Service handles ISR XML-RPC API requests.
- REST API - REST resource for ISR API commands.
- Archiver
- SIPREC - Used to interact between a Session Recording Client (SRC) and a Session Recording Server (SRS).
  - SIP Proxy - SIP user agent. SIP Proxy acts as B2BUA if configured in pass-thru mode and acts as SIP Endpoint for conference mode and call parking mode. The proxy handles SIP signaling and keeps track of call states. It also maps two legs to a call session when acting as B2BUA. Once it receives a new call, the SIP Proxy gets routing and recording decisions from the Call Manager, then submits

an event to Event Queue to be distributed to a Mixer that corresponds to the call channel.

- Codec Negotiator - Responsible for generating supported Codec list for SDP offers and answers to offers.
- SIPREC Processor - This component is responsible for processing SIPREC requests. When the SIP Proxy receives a SIPREC call, judging by multipart bodies, it passes call context and SIPREC Metadata to SIPREC process. The SIPREC Processor then parses the Metadata of the Recording Session (RS) into a structured data object. The SIPREC Processor, in turn, passes the call context back to SIP Proxy with flag set for detailed instructions on SIP signaling. Note: Final SIP action for SIPREC from SIP Proxy, afterward, is also affected by Call Manager.

Control Index Server (CIS)

The CIS consists of the following components:

ISR Database

ISR User Dashboard

ISR Administrator Dashboard

Sequence Diagrams

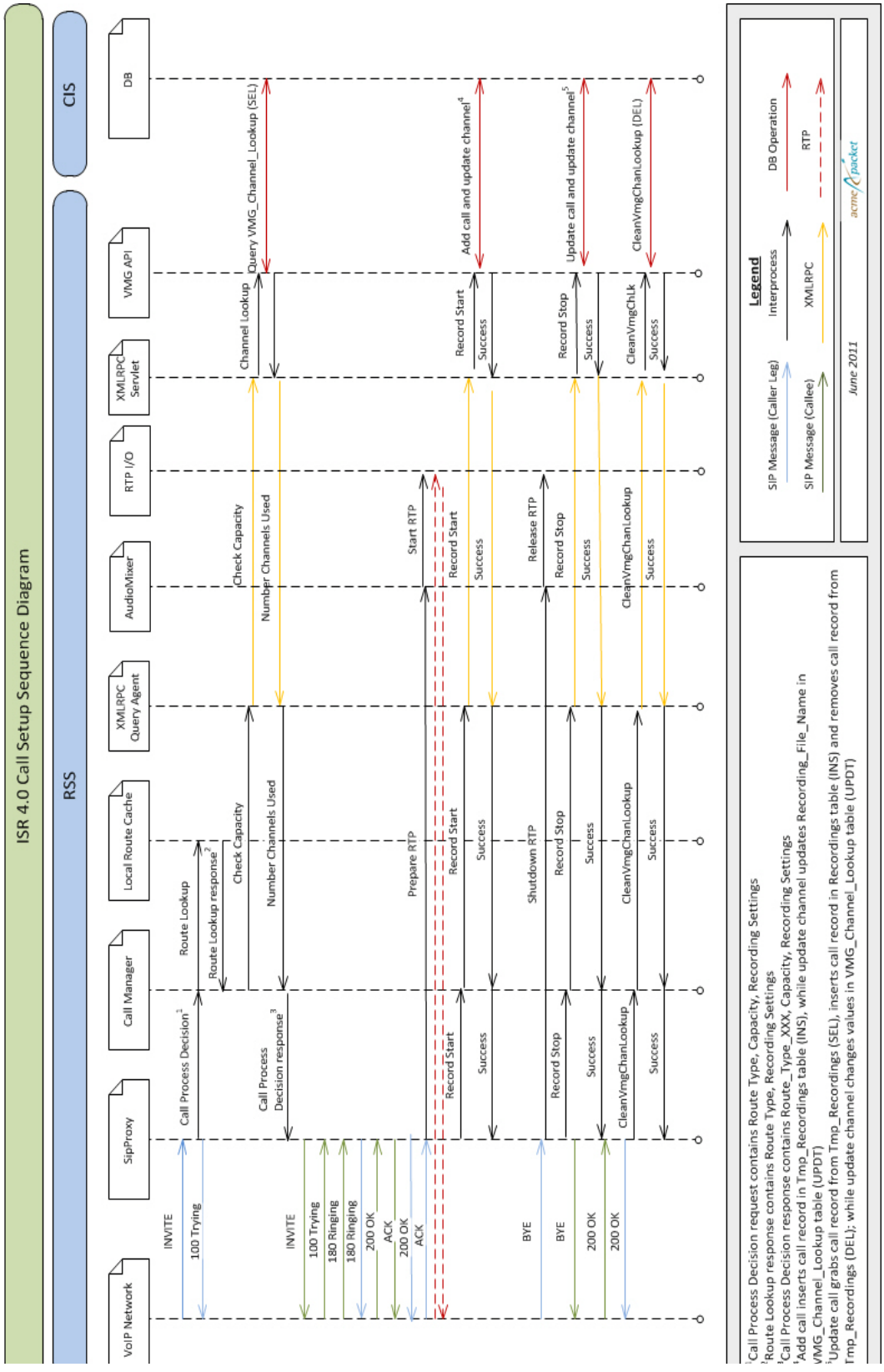
This section provides details about the ISR call setup for a single successful call. This is for informational purposes only.

Non-SIPREC Call

The following sequence diagram applies to the ISR configuration in non-SIPREC, pass-through, interactive voice response (IVR) skip mode. The call applies to a percentage-based recording route.

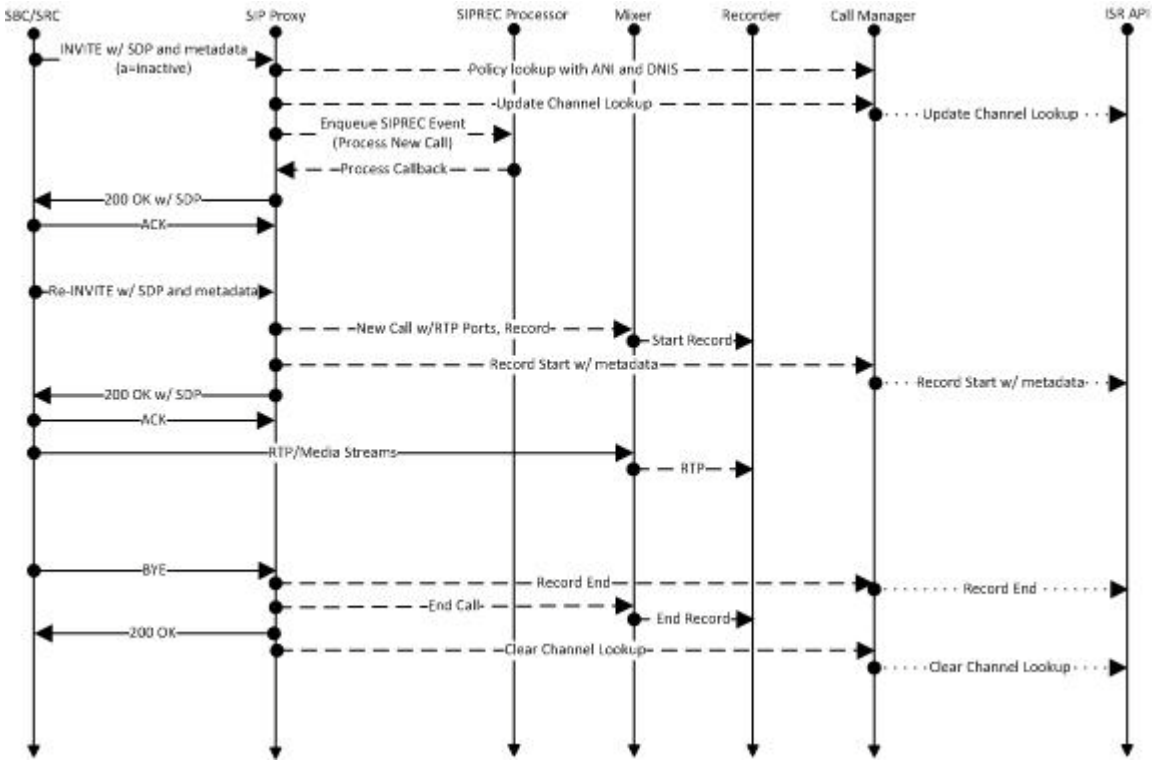
The simple call flow below reflects a single successful call which applies to a route configured for pass-through mode and recording of 100% of calls. The diagram highlights some of the features in the ISR, such as IVR-skip mode. Previously, the ISR architecture required a VoiceXML platform to make routing,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

ISR Call Setup Sequence Diagram



SIPREC Call

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



B ISR RMC

This appendix provides an overview of the ISR Media Converter (RMC) and provides procedures for editing locations that contain raw RTP files that require conversion for playback. It also includes a procedure for installing the RMC license.

About the ISR RMC

The ISR records sessions in several RTP codecs and handles the conversion and playback of most codecs using the RMC. This RMC is automatically installed as part of the RSS installation and runs on its own license. Contact your Oracle sales representative for more information about obtaining the RMC license.

The ISR RMC is a media converter that converts recordings from RTP packet data (".rpdd" formatted files) to Pulse Code Modulation (PCM) wave files (".wav" formatted files), for playback by the ISR Dashboard. It allows the ISR to record calls from multiple codecs, including G.729 and G.722. Consult the ISR Release Notes for a complete list of RTP codecs currently supported on the ISR.

In previous releases, the location configurations through the ISR Dashboard were associated only with archiving - the moving of recorded files and updating of the recording information in the database. Now each location also has a G.729 converter, or RMC, configuration to define which RMC has access to the files at that location. When a user plays a recording that is in raw RTP format (.rpdd formatted file), the dashboard makes a request to the RMC converter set for that file's location. Once the RMC converter is finished transcoding (to .wav format), the browser's media player plays the file.

ISR RMC License

This RMC is automatically installed when performing the RSS installations.

When you have obtained an RMC license for the ISR, you can install the license key to enable the RMC to work in your network.

Obtaining the RMC License Key

Use the following procedure to obtain and install the license key and enable RMC in your network.

To obtain the RMC license key:

1. SSH to your RSS.
2. At the "Login as" prompt, enter "**root**" and press <Enter>.

```
Login as: root
The password prompt displays.
```

3. At the "Password" prompt, enter "**sips**" and press <Enter>.

```
root@<hostname>’s password> sips
The following prompt and message display.
Net-Net ISR
Copyright (c) 2004-2012 Acme Packet Inc.
Username:
```

4. No username is required so press <Enter>.

```
Username: (leave blank)

The password prompt displays.
```

5. No password is required so press <Enter>.

```
Password: (leave blank)
The following message displays followed by the NN-ISR hostname prompt.
"Access granted since there are no configured users."
NN-ISR>
```

6. Enter **ifconfig** and press <Enter> to list the current configuration on the ISR.

```
NN-ISR> ifconfig
eth0      Link encap:Ethernet  HWaddr 3C:4A:92:F5:9B:C4
inet addr:172.30.58.141  Bcast:172.30.255.255  Mask:255.255.0.0
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:184074 errors:0 dropped:0 overruns:0 frame:0
TX packets:34402 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:20765532 (19.8 Mb)  TX bytes:3099950 (2.9 Mb)
Interrupt:30 Memory:f4000000-f4012800
```

7. Make a note of the MAC Address (HWaddr) for the license request.
8. Contact your Oracle sales representative and provide the following SBC information to request an RMC license key:
   - System name
   - Number of ports
   - Production or development license
   - License expiration (Development licenses only)
   - Product name (converter with G.729 for standard ISR RSS hosts)
   - MAC address (from Step 4 and 5)

Installing the RMC License Key

After receiving the RMC license key, you must transfer it to the RSS host's filesystem.

To install the RMC license:

1. Open an FTP client.
2. In the “**Host**” field, enter the RSS management IP address. For example,

```
Host: 172.30.58.16
```

3. In the “**Port**” field, enter **22**. For example,

```
Port: 22
```

4. In the "**Username**" and "**Password**" fields, enter **root** and **sips**, respectively. For example,

```
Username: root
Password: sips
```

   The license file is stored in the */cxc* directory of the RSS. When you connect via FTP (or SSH) you are in the */cxc* directory.

5. Copy the license file from your local machine to the RSS using the FTP application.
6. Using an SSH Client, login to the ISR by entering "**root**" at the "Login as" prompt, and press <Enter>.

```
Login as: root
The password prompt displays.
```

7. At the "Password" prompt, enter "**sips**" and press <Enter>.

```
root@<hostname>'s password> sips
The following prompt and message display.
Net-Net OS-E
Copyright (c) 2004-2012 Acme Packet Inc.
Username:
```

8. No username is required so press <Enter>.

```
Username: (leave blank)
The password prompt displays.
```

9. No password is required so press <Enter>.

```
Password: (leave blank)
The following message displays followed by the NN-ISR hostname prompt.
"Access granted since there are no configured users."
NN-ISR>
```

10. At the "<Hostname>#"prompt, enter "**restart process isr**" and press <Enter>.

```
<NN-ISR> # restart process isr
```

   Note: The "restart process isr" restarts the ISR and allows the RSS to read the new license information immediately.

Testing the RMC Converter

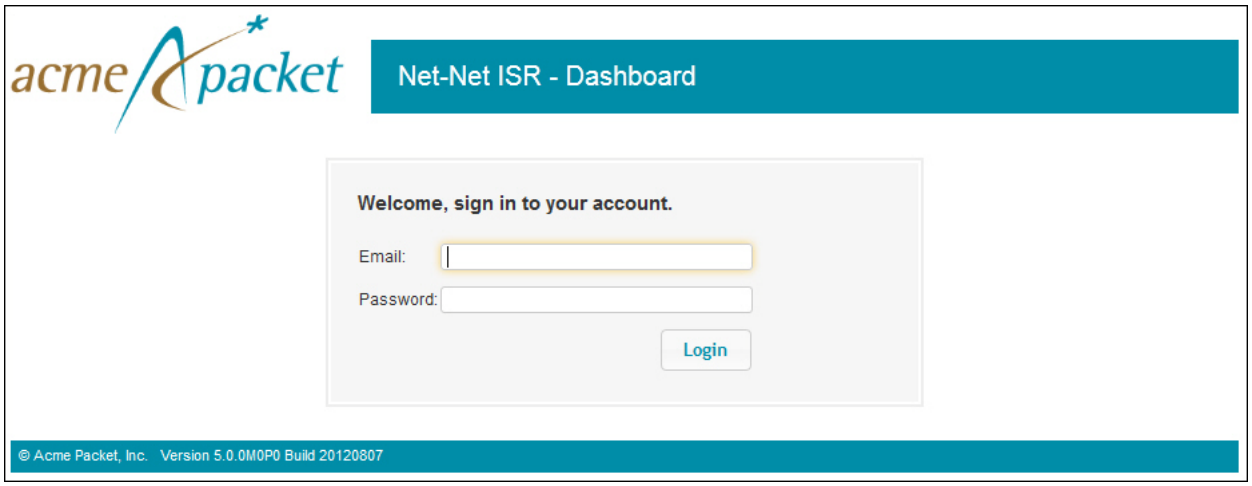
When the RMC license is enabled on the ISR, you can test that it is working properly by playing a G.729 recording through the ISR Dashboard.

To test the RMC converter:

1. Open your Internet Web browser.
2. Enter the IP address of the ISR. For example:

   ```
   http://172.54.66.7
   ```

   The Login page displays.



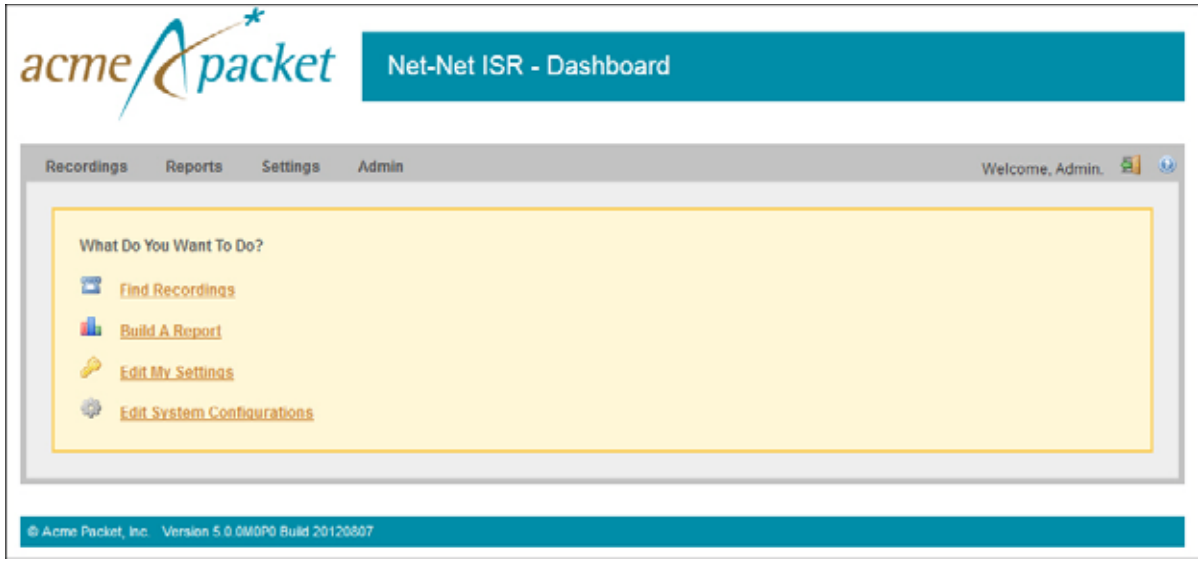
3. Enter your email and password, respectively, in the "**Email**" and "**Password**" fields.

   The default user name and password are:

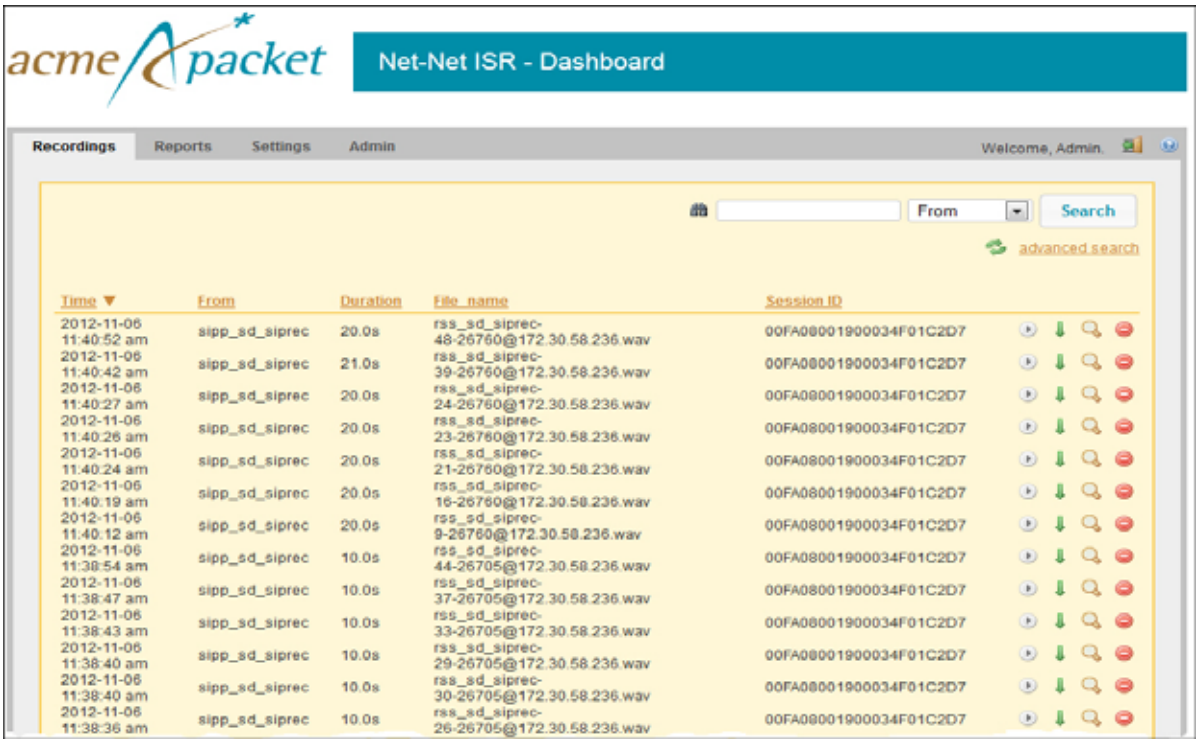
   User name: isradmin@acmepacket.com

   Password: admin123

   The following page displays.



4. From the Main Menu, click **Recordings**. The following page displays.



5. Select a recording that has a file name in the format "**.rpdd**" and then click the .

   The following message displays:

   If the RMC conversion process was successful (message is converted from a ".rpdd" file to a ".wav" file), the recording opens and an audible playback of the recording is heard.

   If the RMC conversion process was unsuccessful, the following message displays:

   Converter logs can be found on the RSS host /cxc_common/ISR/converter for troubleshooting.

Assigning RMC Conversion to Specific Locations

The ISR recordings are stored at locations you specified during the installation process of the CIS and RSS. If you enable the RMC license on your ISR, each location containing files that could require conversion must have an RMC set to handle conversion of the files for playback.

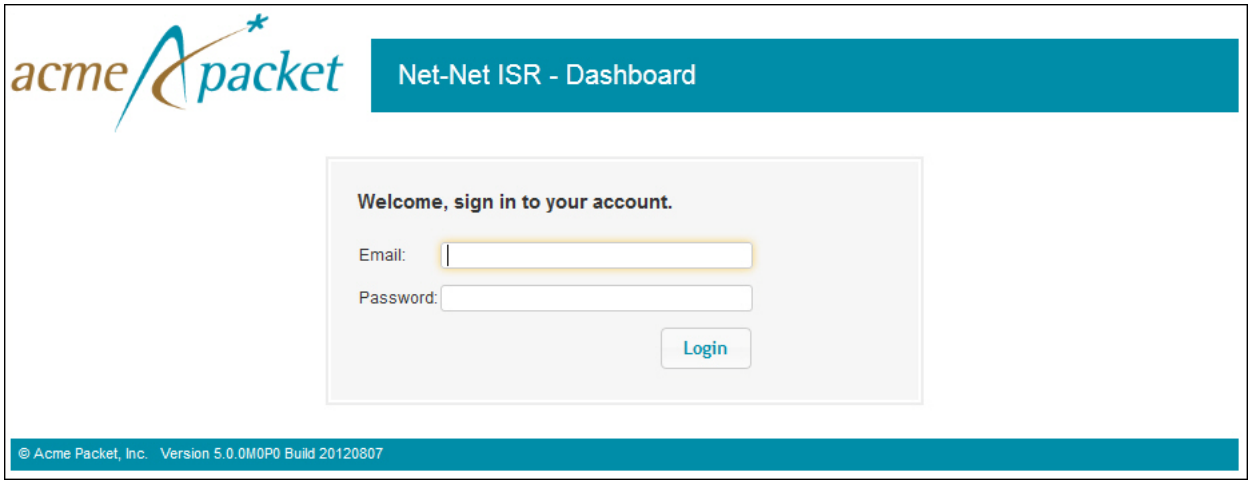
By default, a converter is configured on every location that is created. Some locations, like SANs, do not have a converter installed and should be configured to use an existing converter.

To specify RMC conversion to a specific location:

1. Open your Internet Web browser.
2. Enter the IP address of the ISR. For example:

   `http://172.54.66.7`

   The Login page displays.



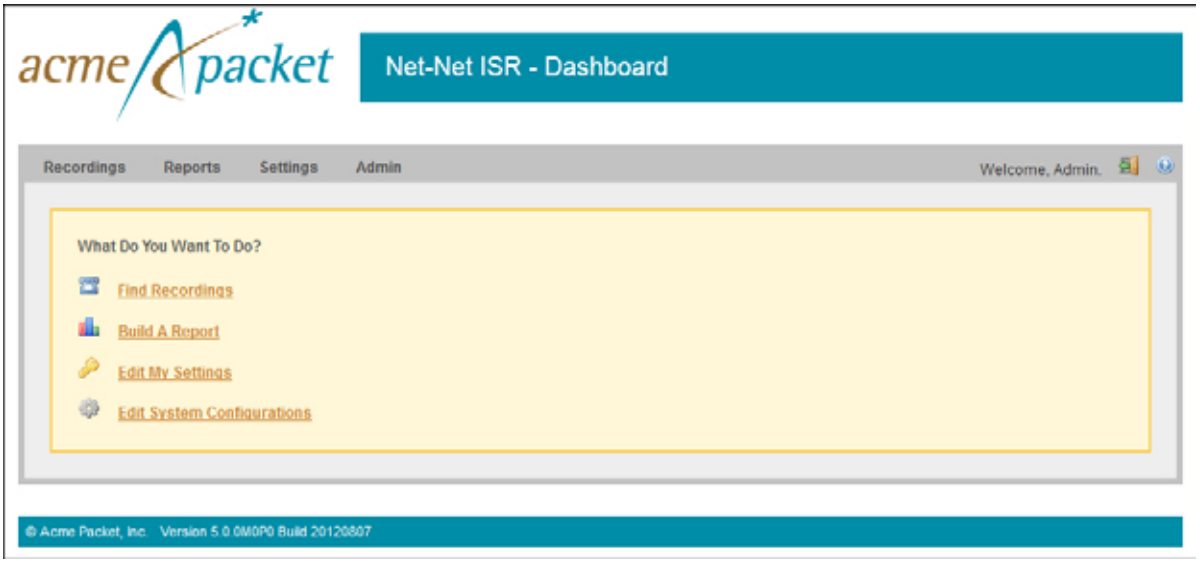
3. Enter your email and password, respectively, in the "**Email**" and "**Password**" fields.

   The default user name and password are:

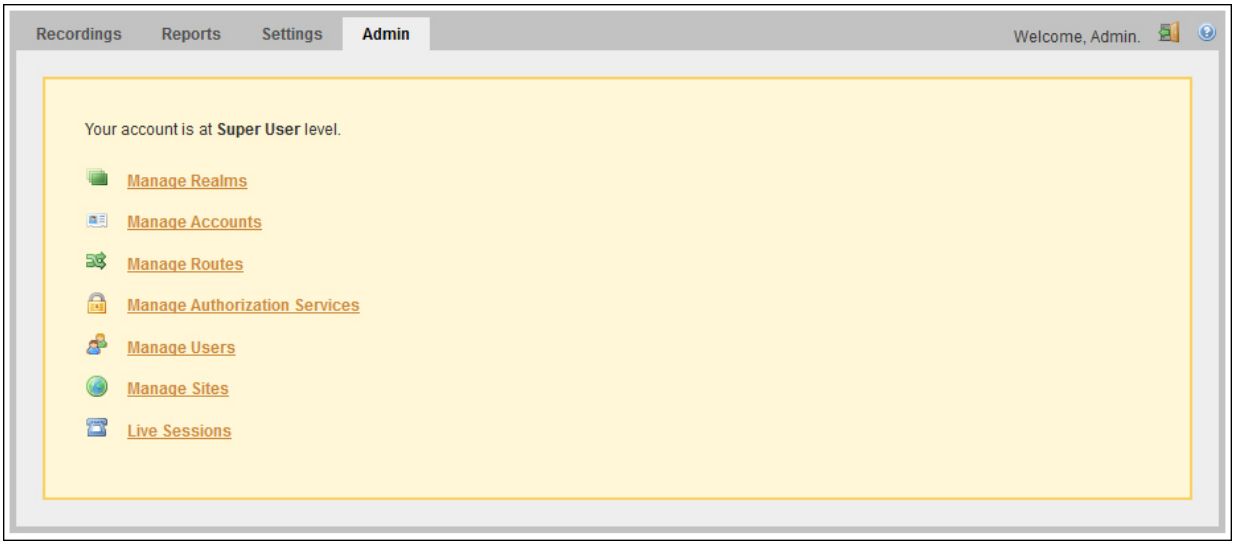
   User name: isradmin@acmepacket.com

   Password: admin123

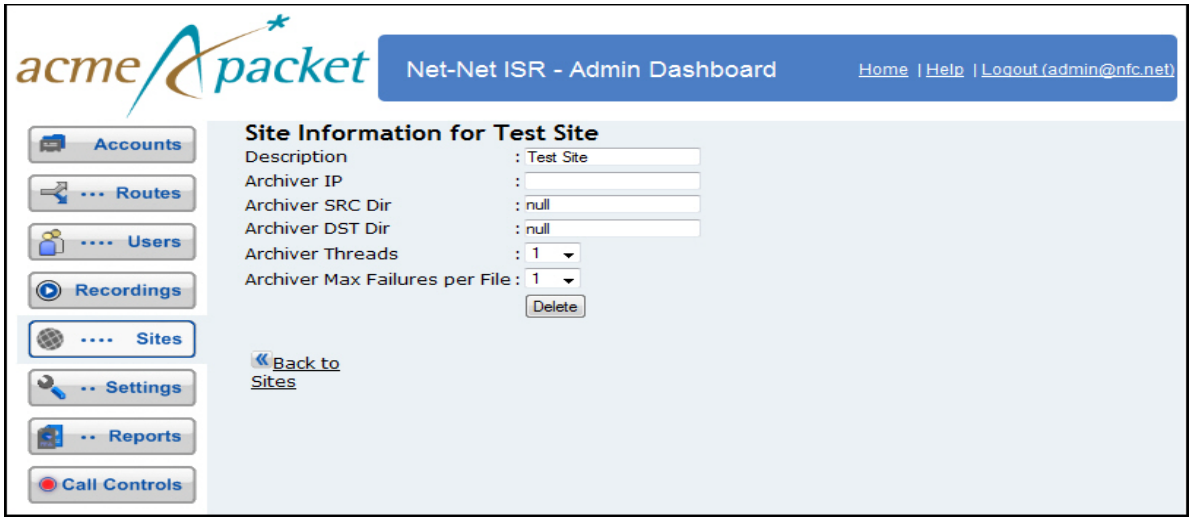
   The following page displays.



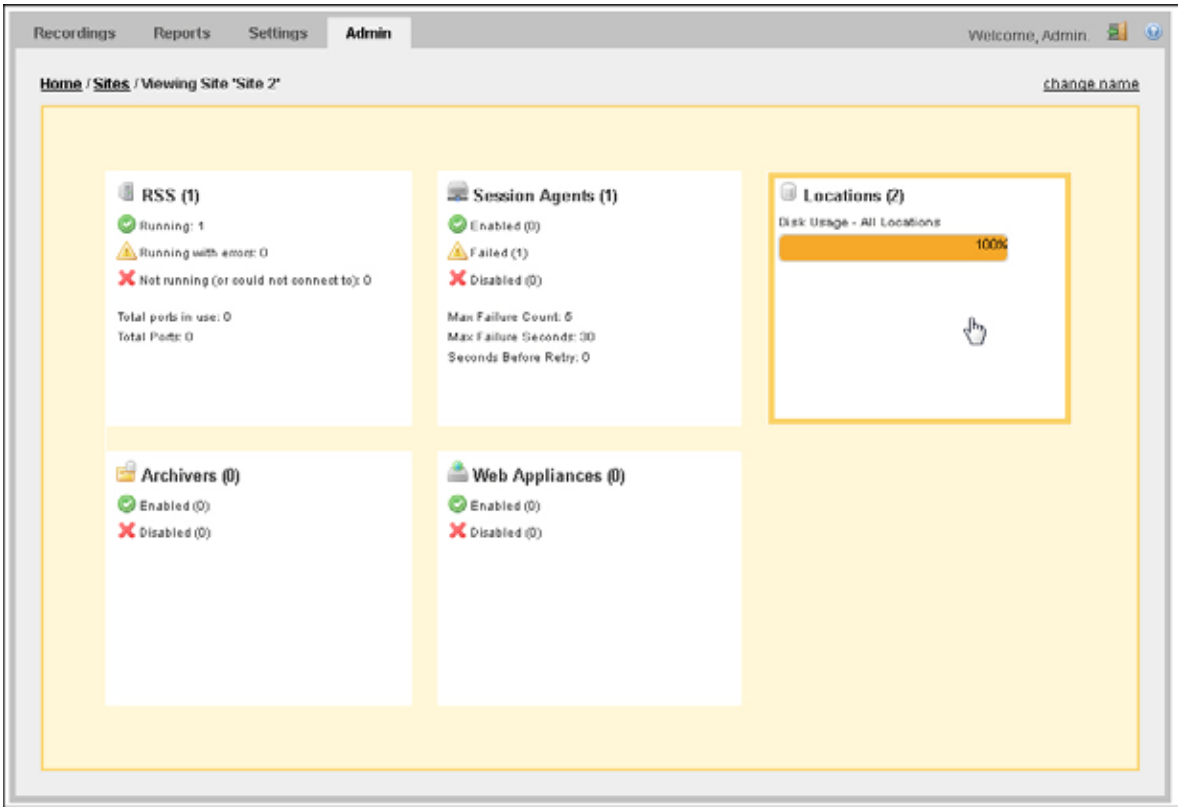
4. From the Main Menu, click **Admin**. The following page displays.



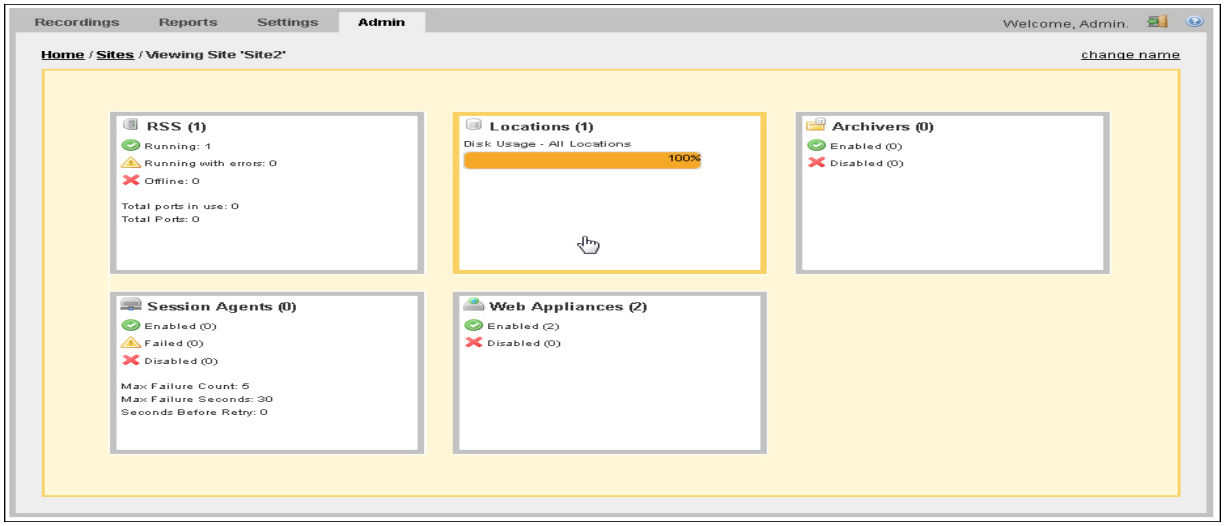
5. Click **Manage Sites**. The following page displays.



6. Click the  associated with a site that you want to edit. The following pages displays.



7. Click on the "**Locations**" tab. The following page displays.



8. Click the  to edit the configuration of that location. The following dialog box displays.

9. In the "*Recording Converter*" section, in the "**Converter IP Address**" field, specify the RMC IP address.
10. If the RMC is listening to XML-RPC requests on a port other than the default (Port 8890), specify the correct converter port number in the "**Converter Port**" field.
11. Click **Update** to update the location with the RMC information.

C Remote Archival Webservice WSDL

Remote Archival Webservice WSDL

The Remote Archival Webservice WSDL may also be found on a deployed Webservice host by pointing a browser to the following URL:

http://<RA WS host IP>:8080/RemoteArchiver/services/RemoteArchiverWS?wsdl

Note: The Remote Archival Webservice WSDL file is password protected. Remote Archival users must provide valid usernames and passwords when accessing this file.

```
<?xml version="1.0" encoding="UTF-8"?>
<definitions


targetNamespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
     xmlns="http://schemas.xmlsoap.org/wsdl/"
     xmlns:tns1="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
     xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
     xmlns:impl="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
     xmlns:apachesoap="http://xml.apache.org/xml-soap"
     xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
     xmlns:xsd="http://www.w3.org/2001/XMLSchema"
     xmlns:xs="http://www.w3.org/2001/XMLSchema"
     xmlns:wsdlsoap="http://schemas.xmlsoap.org/wsdl/soap/"
     xmlns:intf="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
     xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
    >
    <types>
        <schema
targetNamespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
xmlns=
"http://www.w3.org/2001/XMLSchema"

xmlns:ns0="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
xmlns:ns1=
     "http://www.acmepacket.com/NNISR/RemoteArchiverWS"

xmlns:ns2="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
xmlns:ns3=
             "http://www.acmepacket.com/NNISR/RemoteArchiverWS"

xmlns:ns4="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
xmlns:ns5=
             "http://www.acmepacket.com/NNISR/RemoteArchiverWS"

xmlns:ns6="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
xmlns:ns7=
     "http://www.acmepacket.com/NNISR/RemoteArchiverWS"

xmlns:ns8="http://www.acmepacket.com/NNISR/RemoteArchiverWS"
xmlns:ns9=
             "http://www.acmepacket.com/NNISR/RemoteArchiverWS">
```

```
            <import
namespace="http://schemas.xmlsoap.org/soap/encoding/"/>
            <complexType name="account">
                <xs:sequence>
                    <xs:element name="action" type="xs:int"/>
                    <xs:element name="accountId" type="xs:int"/>
                    <xs:element name="accountName" type="xs:string"/>
                    <xs:element name="accountDescription"
type="xs:string"/>
                    <xs:element name="accountMisc" type="xs:string"/>
                   <xs:element name="percentToRecord" type="xs:int"/>
                  <xs:element name="recordingEnabled" type="xs:int"/>
                   <xs:element name="callMetaDataSrc" type="xs:int"/>
                <xs:element name="announceEnabled" type="xs:boolean"/>
                    <xs:element name="defaultAnnounceAudioFile"
nillable="true" type="xs:string"/>
                    <xs:element name="defaultAnnounceAudioText"
nillable="true" type="xs:string"/>
                    <xs:element name="defaultOptOutVxmlFile"
nillable="true" type="xs:string"/>
                  <xs:element name="optOutEnabled" type="xs:boolean"/>
                    <xs:element name="recorderState" type="xs:int"/>
                    <xs:element name="defaultRecordingType"
type="xs:int"/>
                    <xs:element name="customDataLabelsSource"
type="xs:int"/>
                    <xs:element name="agentIdEditableFlag"
type="xs:boolean"/>
                    <xs:element name="ratingEditableFlag"
type="xs:boolean"/>
                    <xs:element name="completedEditableFlag"
type="xs:boolean"/>
                    <xs:element name="notesEditableFlag"
type="xs:boolean"/>
                   <xs:element name="customData1Name" nillable="true"
type="xs:string"/>
                    <xs:element name="customData1FriendlyName"
type="xs:string"/>
                    <xs:element name="customData1EditableFlag"
type="xs:boolean"/>
                  <xs:element name="customData2Name" nillable="true"
type="xs:string"/>
                    <xs:element name="customData2FriendlyName"
type="xs:string"/>
                    <xs:element name="customData2EditableFlag"
type="xs:boolean"/>
                  <xs:element name="customData3Name" nillable="true"
type="xs:string"/>
                    <xs:element name="customData3FriendlyName"
type="xs:string"/>
                    <xs:element name="customData3EditableFlag"
type="xs:boolean"/>
                 <xs:element name="customData4Name" nillable="true"
type="xs:string"/>
                    <xs:element name="customData4FriendlyName"
type="xs:string"/>
                    <xs:element name="customData4EditableFlag"
type="xs:boolean"/>
                    <xs:element name="application" nillable="true"
type="xs:string"/>
                    <xs:element name="playBeepBeforeRecord"
type="xs:boolean"/>
```

```
                <xs:element name="terminateOnDtmf" type="xs:boolean"/>
                    <xs:element name="terminateOnEos" type="xs:int"/>
                    <xs:element name="recurringBeepEnabled"
type="xs:boolean"/>
                    <xs:element name="recurringBeepInterval"
type="xs:int"/>
                 <xs:element name="recurringBeepFile" nillable="true"
type="xs:string"/>
                  <xs:element name="recordSaveDtmf" type="xs:string"/>
                    <xs:element name="maximumNumberOfPorts"
type="xs:int"/>
                 <xs:element name="numberOfBurstPorts" type="xs:int"/>
                    <xs:element name="acctPortLimit" type="xs:int"/>
                    <xs:element name="showApplianceTabInRouteView"
type="xs:boolean"/>
                   <xs:element name="storeDtmfSetting" type="xs:int"/>
                </xs:sequence>
            </complexType>
            <complexType name="route">
                <xs:sequence>
                    <xs:element name="action" type="xs:int"/>
                    <xs:element name="routeId" type="xs:int"/>
                    <xs:element minOccurs="0" name="routeType"
type="xs:int"/>
                    <xs:element minOccurs="0" name="routePattern"
type="xs:string"/>
                    <xs:element minOccurs="0" name="label"
type="xs:string"/>
                    <xs:element minOccurs="0" name="accountId"
type="xs:int"/>
                    <xs:element minOccurs="0" name="percentToRecord"
type="xs:int"/>
                   <xs:element minOccurs="0" name="recordingEnabled"
type="xs:int"/>
                 <xs:element minOccurs="0" name="defaultRecordingType"
type="xs:int"/>
                  <xs:element minOccurs="0" name="virtualRoutePattern"
type="xs:string"/>
                    <xs:element minOccurs="0" name="announceAudioFile"
nillable="true" type=
                     "xs:string"/>
                   <xs:element minOccurs="0" name="announceAudioText"
nillable="true" type=
    "xs:string"/>
                    <xs:element minOccurs="0" name="optOutVxmlFile"
nillable="true" type=
    "xs:string"/>
                    <xs:element minOccurs="0" name="optOutEnabled"
type="xs:boolean"/>
                    <xs:element minOccurs="0" name="announceEnabled"
type="xs:boolean"/>
                    <xs:element minOccurs="0" name="customData1Name"
nillable="true" type=
                     "xs:string"/>
                    <xs:element minOccurs="0"
name="customData1FriendlyName" type="xs:string"/>
                    <xs:element minOccurs="0"
name="customData1EditableFlag" type="xs:boolean"/>
                    <xs:element minOccurs="0" name="customData2Name"
nillable="true" type=
    "xs:string"/>
```

```
                    <xs:element minOccurs="0"
name="customData2FriendlyName" type="xs:string"/>
                    <xs:element minOccurs="0"
name="customData2EditableFlag" type="xs:boolean"/>
                    <xs:element minOccurs="0" name="customData3Name"
nillable="true" type=
                    "xs:string"/>
                    <xs:element minOccurs="0"
name="customData3FriendlyName" type="xs:string"/>
                    <xs:element minOccurs="0"
name="customData3EditableFlag" type="xs:boolean"/>
                    <xs:element minOccurs="0" name="customData4Name"
nillable="true" type=
                    "xs:string"/>
                    <xs:element minOccurs="0"
name="customData4FriendlyName" type="xs:string"/>
                    <xs:element minOccurs="0"
name="customData4EditableFlag" type="xs:boolean"/>
                    <xs:element minOccurs="0" name="application"
nillable="true" type="xs:string"/>
                  <xs:element minOccurs="0" name="playBeepBeforeRecord"
type="xs:boolean"/>
                    <xs:element minOccurs="0" name="terminateOnDtmf"
type="xs:boolean"/>
                    <xs:element minOccurs="0" name="terminateOnEos"
type="xs:int"/>
                    <xs:element minOccurs="0" name="priority"
type="xs:float"/>
                  <xs:element minOccurs="0" name="maximumNumberOfPorts"
type="xs:int"/>
                    <xs:element minOccurs="0" name="minimumStorageDays"
type="xs:int"/>
                    <xs:element minOccurs="0" name="numberOfBurstPorts"
type="xs:int"/>
                    <xs:element minOccurs="0" name="storageGracePeriod"
type="xs:int"/>
                  <xs:element minOccurs="0" name="recurringBeepEnabled"
type="xs:boolean"/>
                 <xs:element minOccurs="0" name="recurringBeepInterval"
type="xs:int"/>
                    <xs:element minOccurs="0" name="recurringBeepFile"
nillable="true" type=
                    "xs:string"/>
                    <xs:element minOccurs="0" name="recordSaveDtmf"
type="xs:string"/>
                    <xs:element minOccurs="0" name="callMetaDataSrc"
type="xs:int"/>
                  <xs:element minOccurs="0" name="agentIdEditableFlag"
type="xs:boolean"/>
                    <xs:element minOccurs="0" name="ratingEditableFlag"
type="xs:boolean"/>
                 <xs:element minOccurs="0" name="completedEditableFlag"
type="xs:boolean"/>
                    <xs:element minOccurs="0" name="notesEditableFlag"
type="xs:boolean"/>
                    <xs:element name="storeDtmfSetting" type="xs:int"/>
                  </xs:sequence>
              </complexType>
              <complexType name="memberRoute">
                  <xs:sequence>
                      <xs:element name="action" type="xs:int"/>
                   <xs:element name="routeGroupMemberId" type="xs:int"/>
```

```
                    <xs:element minOccurs="0" name="routeGroupMasterId"
type="xs:int"/>
                        <xs:element minOccurs="0" name="routePattern"
type="xs:string"/>
                     <xs:element minOccurs="0" name="virtualRoutePattern"
type="xs:string"/>
                    </xs:sequence>
                </complexType>
                <complexType name="metadataType">
                    <xs:sequence>
                        <xs:element name="action" type="xs:int"/>
                        <xs:element name="metadataTypeId" type="xs:int"/>
                        <xs:element minOccurs="0" name="name"
type="xs:string"/>
                        <xs:element minOccurs="0"
name="sessionCorrelationNumber" nillable="true" type=
    "xs:int"/>
                        <xs:element minOccurs="0" name="nodeType"
nillable="true" type="xs:string"/>
                        <xs:element minOccurs="0" name="srcTypeId"
type="xs:int"/>
                        <xs:element minOccurs="0" name="searchable"
nillable="true" type="xs:boolean"/>
                        <xs:element minOccurs="0" name="isDisplayed"
nillable="true" type="xs:boolean"/>
                    </xs:sequence>
                </complexType>
                <complexType name="getNewAdministrativeDataReqObject">
                    <xs:sequence>
                        <xs:element minOccurs="0" name="lastRunTime"
nillable="true" type="xs:dateTime"/>
                    </xs:sequence>
                </complexType>
                <complexType name="getNewAdministrativeDataRespObject">
                    <xs:sequence>
                        <xs:element name="returnCode" type="xs:int"/>
                        <xs:element name="returnString" nillable="true"
type="xs:string"/>
                        <xs:element minOccurs="0" name="currentRunTime"
type="xs:dateTime"/>
                        <xs:element maxOccurs="unbounded" minOccurs="0"
name="accounts" type=
                        "tns1:account"/>
                        <xs:element maxOccurs="unbounded" minOccurs="0"
name="routes" type="tns1:route"/>
                        <xs:element maxOccurs="unbounded" minOccurs="0"
name="memberRoutes" type=
    "tns1:memberRoute"/>
                        <xs:element maxOccurs="unbounded" minOccurs="0"
name="metadataTypes" type=
                        "tns1:metadataType"/>
                    </xs:sequence>
                </complexType>
                <complexType name="sessionStats">
                    <xs:sequence>
                        <xs:element name="routeId" type="xs:int"/>
                       <xs:element name="sessionDate" type="xs:dateTime"/>
                        <xs:element name="totalNumberOfSessions"
type="xs:int"/>
```

```
                    <xs:element name="peakNumberOfSessions"
type="xs:int"/>
                    <xs:element name="numberOfSessionsRejected"
type="xs:int"/>
                    <xs:element name="numberOfBurstSessions"
type="xs:int"/>
                 <xs:element name="recordingLengthMs" type="xs:long"/>
                    <xs:element name="numberOfSessionsRecorded"
type="xs:int"/>
                    <xs:element name="systemCapacityReached"
type="xs:int"/>
                    <xs:element name="routeCapacityReached"
type="xs:int"/>
                    <xs:element name="accountCapacityReached"
type="xs:int"/>
                </xs:sequence>
            </complexType>
            <complexType name="getSessionStatsReqObject">
                <xs:sequence>
                    <xs:element name="date" nillable="true"
type="xs:dateTime"/>
                </xs:sequence>
            </complexType>
            <complexType name="getSessionStatsRespObject">
                <xs:sequence>
                    <xs:element name="returnCode" type="xs:int"/>
                    <xs:element name="returnString" nillable="true"
type="xs:string"/>
                    <xs:element maxOccurs="unbounded" minOccurs="0"
name="sessionStatsArray"
                    nillable="true"
                         type="tns1:sessionStats"/>
                </xs:sequence>
            </complexType>
            <complexType name="reqObject">
                <xs:sequence>
                    <xs:element name="recordingId" type="xs:long"/>
                    <xs:element name="fileName" nillable="true"
type="xs:string"/>
                </xs:sequence>
            </complexType>
            <complexType name="respObject">
                <xs:sequence>
               <xs:element minOccurs="0" name="cdrId" type="xs:long"/>
                    <xs:element name="recordingId" type="xs:long"/>
                    <xs:element name="fileName" type="xs:string"/>
                    <xs:element minOccurs="0" name="fileStatus"
type="xs:int"/>
                 <xs:element minOccurs="0" name="ani" nillable="true"
type="xs:string"/>
                 <xs:element minOccurs="0" name="dnis" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="accountId"
type="xs:int"/>
                    <xs:element minOccurs="0" name="duration"
type="xs:long"/>
                    <xs:element minOccurs="0" name="timestamp"
type="xs:dateTime"/>
                    <xs:element minOccurs="0" name="directory"
nillable="true" type="xs:string"/>
```

```
                <xs:element minOccurs="0" name="vmgId" type="xs:int"/>
                    <xs:element minOccurs="0" name="custom1"
nillable="true" type="xs:string"/>
                    <xs:element minOccurs="0" name="custom2"
nillable="true" type="xs:string"/>
                    <xs:element minOccurs="0" name="custom3"
nillable="true" type="xs:string"/>
                    <xs:element minOccurs="0" name="custom4"
nillable="true" type="xs:string"/>
                    <xs:element minOccurs="0" name="archived"
type="xs:int"/>
                    <xs:element minOccurs="0" name="routeId"
type="xs:long"/>
                    <xs:element minOccurs="0" name="archivalRemarks"
nillable="true" type=
    "xs:string"/>
                  <xs:element minOccurs="0" name="archivalFailCount"
type="xs:int"/>
                    <xs:element minOccurs="0" name="agentId"
nillable="true" type="xs:string"/>
                    <xs:element minOccurs="0" name="agentTerminal"
nillable="true" type="xs:string"/>
                    <xs:element minOccurs="0" name="archiverMode"
type="xs:string"/>
                    <xs:element minOccurs="0" name="sensitive"
type="xs:int"/>
                    <xs:element minOccurs="0" name="lastPauseTime"
nillable="true" type=
                    "xs:dateTime"/>
                    <xs:element minOccurs="0" name="pauseLength"
type="xs:int"/>
                    <xs:element minOccurs="0" name="deleteFlag"
type="xs:boolean"/>
                   <xs:element minOccurs="0" name="previousFileName"
nillable="true" type=
                    "xs:string"/>
                    <xs:element minOccurs="0" name="archiverAction"
type="xs:int"/>
                   <xs:element minOccurs="0" name="conversionStatus"
type="xs:int"/>
                    <xs:element minOccurs="0" name="isrUcid"
nillable="true" type="xs:string"/>
                    <xs:element minOccurs="0" name="ingressCallId"
nillable="true" type="xs:string"/>
                    <xs:element minOccurs="0" name="egressCallId"
nillable="true" type="xs:string"/>
                    <xs:element maxOccurs="unbounded" minOccurs="0"
name="siprecDataSets" type=
                    "tns1:siprecData"/>
                    <xs:element maxOccurs="unbounded" minOccurs="0"
name="dtmfEntries" type=
                    "tns1:dtmfEntry"/>
                    <xs:element name="returnCode" type="xs:int"/>
                    <xs:element name="returnString" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="downloadable"
type="xs:boolean"/>
                    <xs:element minOccurs="0" name="fileNotFound"
type="xs:boolean"/>
                    <xs:element minOccurs="0" name="splitFile"
type="xs:boolean"/>
                <xs:element maxOccurs="2" minOccurs="0" name="return"
nillable="true" type=
```

```
                        "xs:base64Binary"/>
                    </xs:sequence>
                </complexType>
                <complexType name="metadataCorrelationSet">
                    <xs:sequence>
                        <xs:element name="mcsId" type="xs:long"/>
                       <xs:element name="metadataTypeId1" type="xs:int"/>
                      <xs:element name="metadataValue1" type="xs:string"/>
                        <xs:element name="metadataTypeId2" type="xs:int"/>
                      <xs:element name="metadataValue2" type="xs:string"/>
                    </xs:sequence>
                </complexType>
                <complexType name="extensionData">
                    <xs:sequence>
                       <xs:element name="extensionDataId" type="xs:long"/>
                        <xs:element name="nodeId" type="xs:long"/>
                        <xs:element name="metadataTypeId" type="xs:int"/>
                    <xs:element minOccurs="0" name="value" nillable="true"
type="xs:string"/>
                        <xs:element minOccurs="0" name="indexedValue"
nillable="true" type="xs:string"/>
                     <xs:element minOccurs="0" name="mcs" nillable="true"
type=
                        "impl:metadataCorrelationSet"/>
                    </xs:sequence>
                </complexType>
                <complexType name="siprecParticipant">
                    <xs:sequence>
                       <xs:element name="participantId" type="xsd:long"/>
                    <xs:element name="siprecParticipantId" nillable="true"
type="xsd:string"/>
                        <xs:element name="participantAor" nillable="true"
type="xsd:string"/>
                      <xs:element name="participantName" nillable="true"
type="xsd:string"/>
                     <xs:element name="participantStart" nillable="true"
type="xsd:dateTime"/>
                        <xs:element name="participantEnd" nillable="true"
type="xsd:dateTime"/>
                        <xs:element maxOccurs="unbounded" minOccurs="0"
name="participantExtensionData"
                             type="impl:extensionData"/>
                    </xs:sequence>
                </complexType>
                <complexType name="siprecSession">
                    <xs:sequence>
                        <xs:element name="sessionId" type="xsd:long"/>
                     <xs:element name="siprecSessionId" nillable="true"
type="xsd:string"/>
                        <xs:element name="sessionStart" nillable="true"
type="xsd:dateTime"/>
                        <xs:element name="sessionEnd" nillable="true"
type="xsd:dateTime"/>
                        <xs:element maxOccurs="unbounded" minOccurs="0"
name="sessionExtensionData"
                        type="impl:extensionData"/>
                    </xs:sequence>
                </complexType>
```

```
            <complexType name="siprecStream">
                <xs:sequence>
                    <xs:element name="streamId" type="xsd:long"/>
                   <xs:element name="siprecStreamId" nillable="true"
type="xsd:string"/>
                    <xs:element name="streamLabel" nillable="true"
type="xsd:string"/>
                    <xs:element name="streamMode" nillable="true"
type="xsd:string"/>
                    <xs:element name="participantId" nillable="true"
type="xsd:long"/>
                    <xs:element name="streamStart" nillable="true"
type="xsd:dateTime"/>
                    <xs:element name="streamEnd" nillable="true"
type="xsd:dateTime"/>
                    <xs:element maxOccurs="unbounded" minOccurs="0"
name="streamExtensionData" type="impl:extensionData"/>
                </xs:sequence>
            </complexType>
            <complexType name="siprecData">
                <xs:sequence>
                    <xs:element maxOccurs="unbounded" minOccurs="0"
name="siprecParticipants"
                    nillable="true"
                         type="impl:siprecParticipant"/>
                    <xs:element name="siprecSession" nillable="true"
type="impl:siprecSession"/>
                    <xs:element maxOccurs="unbounded" minOccurs="0"
name="siprecStreams" nillable=
                    "true"
                         type="impl:siprecStream"/>
                </xs:sequence>
            </complexType>
            <complexType name="dtmfEntry">
                <xs:sequence>
                    <xs:element minOccurs="0" name="msOffset"
type="xs:long"/>
                    <xs:element minOccurs="0" name="originSource"
type="xs:int"/>
                    <xs:element minOccurs="0" name="dtmfDigit"
type="xs:int"/>
                </xs:sequence>
            </complexType>
            <complexType name="reqObject_Array">
                <xs:sequence>
                    <xs:element maxOccurs="unbounded" minOccurs="0"
name="gfRequest" nillable=
                    "true" type="tns1:reqObject"/>
                </xs:sequence>
            </complexType>
            <complexType name="respObject_Array">
                <xs:sequence>
                    <xs:element maxOccurs="unbounded" minOccurs="0"
name="gfResponse" nillable="true" type="tns1:respObject"/>
                </xs:sequence>
            </complexType>
            <complexType name="getListReqObj">
                <xs:sequence/>
            </complexType>
```

```
            <complexType name="recordItem">
                <xs:sequence>
                    <xs:element name="cdrId" type="xs:long"/>
                    <xs:element name="recordingId" type="xs:long"/>
                    <xs:element name="fileName" nillable="true"
type="xs:string"/>
                </xs:sequence>
            </complexType>
            <complexType name="recordItem_array">
                <xs:sequence>
                    <xs:element maxOccurs="unbounded" minOccurs="0"
name="recordItemArray"
                     nillable="true"
                         type="tns1:recordItem"/>
                </xs:sequence>
            </complexType>
            <complexType name="getListRespObj">
                <xs:sequence>
                    <xs:element name="recordingList" nillable="true"
type="tns1:recordItem_array"/>
                    <xs:element name="returnCode" type="xs:int"/>
                    <xs:element name="returnString" nillable="true"
type="xs:string"/>
                </xs:sequence>
            </complexType>
            <complexType name="statusUpdateReqObj">
                <xs:sequence>
                    <xs:element name="cdrId" type="xs:long"/>
                    <xs:element name="recordingId" type="xs:long"/>
                    <xs:element name="status" type="xs:int"/>
                    <xs:element name="reason" nillable="true"
type="xs:string"/>
                </xs:sequence>
            </complexType>
            <complexType name="statusUpdateRespObj">
                <xs:sequence>
                    <xs:element name="returnCode" type="xs:int"/>
                    <xs:element name="returnString" nillable="true"
type="xs:string"/>
                </xs:sequence>
            </complexType>
            <xsd:element name="getSessionStats">
                <xsd:complexType>
                    <xsd:sequence>
                    <xsd:element form="unqualified" name="parameters"
type=
                        "ns0:getSessionStatsReqObject"/>
                    </xsd:sequence>
                </xsd:complexType>
            </xsd:element>
            <xsd:element name="getList">
                <xsd:complexType>
                    <xsd:sequence>
                    <xsd:element form="unqualified" name="parameters"
type="ns1:getListReqObj"/>
                    </xsd:sequence>
                </xsd:complexType>
```

```
            </xsd:element>
            <xsd:element name="statusUpdate">
                <xsd:complexType>
                    <xsd:sequence>
                    <xsd:element form="unqualified" name="parameters"
type=
                        "ns2:statusUpdateReqObj"/>
                    </xsd:sequence>
                </xsd:complexType>
            </xsd:element>
            <xsd:element name="getNewAdministrativeData">
                <xsd:complexType>
                    <xsd:sequence>
                    <xsd:element form="unqualified" name="parameters"
type=
                        "ns3:getNewAdministrativeDataReqObject"/>
                    </xsd:sequence>
                </xsd:complexType>
            </xsd:element>
            <xsd:element name="getFile">
                <xsd:complexType>
                    <xsd:sequence>
                    <xsd:element form="unqualified" name="parameters"
type="ns4:reqObject_Array"/>
                    </xsd:sequence>
                </xsd:complexType>
            </xsd:element>
            <xsd:element name="getSessionStatsResponse">
                <xsd:complexType>
                    <xsd:sequence>
                    <xsd:element form="unqualified" name="parameters"
type=
                        "ns5:getSessionStatsRespObject"/>
                    </xsd:sequence>
                </xsd:complexType>
            </xsd:element>
            <xsd:element name="getListResponse">
                <xsd:complexType>
                    <xsd:sequence>
                    <xsd:element form="unqualified" name="parameters"
type="ns6:getListRespObj"/>
                    </xsd:sequence>
                </xsd:complexType>
            </xsd:element>
            <xsd:element name="statusUpdateResponse">
                <xsd:complexType>
                    <xsd:sequence>
                    <xsd:element form="unqualified" name="parameters"
type=
                        "ns7:statusUpdateRespObj"/>
                    </xsd:sequence>
                </xsd:complexType>
            </xsd:element>
            <xsd:element name="getNewAdministrativeDataResponse">
                <xsd:complexType>
                    <xsd:sequence>
```

```
                    <xsd:element form="unqualified" name="parameters"
type="ns8:getNewAdministrativeDataRespObject"/>
                    </xsd:sequence>
                </xsd:complexType>
            </xsd:element>
            <xsd:element name="getFileResponse">
                <xsd:complexType>
                    <xsd:sequence>
                    <xsd:element form="unqualified" name="parameters"
type=
                        "ns9:respObject_Array"/>
                    </xsd:sequence>
                </xsd:complexType>
            </xsd:element>
        </schema>
    </types>
    <message name="getNewAdministrativeDataRequest">
        <part name="parameters"
type="tns1:getNewAdministrativeDataReqObject"/>
    </message>
    <message name="getNewAdministrativeDataResponse">
        <part name="parameters"
type="tns1:getNewAdministrativeDataRespObject"/>
    </message>
    <message name="getSessionStatsRequest">
       <part name="parameters" type="tns1:getSessionStatsReqObject"/>
    </message>
    <message name="getSessionStatsResponse">
      <part name="parameters" type="tns1:getSessionStatsRespObject"/>
    </message>
    <message name="getFileRequest">
        <part name="parameters" type="tns1:reqObject_Array"/>
    </message>
    <message name="getFileResponse">
        <part name="parameters" type="tns1:respObject_Array"/>
    </message>
    <message name="getListRequest">
        <part name="parameters" type="tns1:getListReqObj"/>
    </message>
    <message name="getListResponse">
        <part name="parameters" type="tns1:getListRespObj"/>
    </message>
    <message name="statusUpdateRequest">
        <part name="parameters" type="tns1:statusUpdateReqObj"/>
    </message>
    <message name="statusUpdateResponse">
        <part name="parameters" type="tns1:statusUpdateRespObj"/>
    </message>
    <portType name="RemoteArchiverWSPortType">
        <operation name="getNewAdministrativeData">
            <input name="getNewAdministrativeDataRequest"
message="tns1:getNewAdministrativeDataRequest"/>
            <output name="getNewAdministrativeDataResponse"
message="tns1:getNewAdministrativeDataResponse"/>
        </operation>
        <operation name="getSessionStats">
```

```
            <input name="getSessionStatsRequest"
message="tns1:getSessionStatsRequest"/>
            <output name="getSessionStatsResponse"
message="tns1:getSessionStatsResponse"/>
        </operation>
        <operation name="getFile">
          <input name="getFileRequest" message="tns1:getFileRequest"/>
            <output name="getFileResponse"
message="tns1:getFileResponse"/>
        </operation>
        <operation name="getList">
          <input name="getListRequest" message="tns1:getListRequest"/>
            <output name="getListResponse"
message="tns1:getListResponse"/>
        </operation>
        <operation name="statusUpdate">
            <input name="statusUpdateRequest"
message="tns1:statusUpdateRequest"/>
            <output name="statusUpdateResponse"
message="tns1:statusUpdateResponse"/>
        </operation>
    </portType>
    <binding name="RemoteArchiverWSSoapBinding"
type="tns1:RemoteArchiverWSPortType">
        <wsdlsoap:binding style="rpc"
transport="http://schemas.xmlsoap.org/soap/http"/>
        <operation name="getNewAdministrativeData">
            <wsdlsoap:operation soapAction=""/>
            <input name="getNewAdministrativeDataRequest">
                <wsdlsoap:body use="literal"
namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"

encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
            </input>
            <output name="getNewAdministrativeDataResponse">
                <wsdlsoap:body use="literal"
namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"

encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
            </output>
        </operation>
        <operation name="getSessionStats">
            <wsdlsoap:operation soapAction=""/>
            <input name="getSessionStatsRequest">
                <wsdlsoap:body use="literal"
namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"

encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
            </input>
            <output name="getSessionStatsResponse">
                <wsdlsoap:body use="literal"
namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"

encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
            </output>
        </operation>
        <operation name="getFile">
            <wsdlsoap:operation soapAction=""/>
            <input name="getFileRequest">
```

```
                <wsdlsoap:body use="literal"
namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"

encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
            </input>
            <output name="getFileResponse">
                <wsdlsoap:body use="literal"
namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"

encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
            </output>
        </operation>
        <operation name="getList">
            <wsdlsoap:operation soapAction=""/>
            <input name="getListRequest">
                <wsdlsoap:body use="literal"
namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"

encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
            </input>
            <output name="getListResponse">
                <wsdlsoap:body use="literal"
namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"

encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
            </output>
        </operation>
        <operation name="statusUpdate">
            <wsdlsoap:operation soapAction=""/>
            <input name="statusUpdateRequest">
                <wsdlsoap:body use="literal"
namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"

encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
            </input>
            <output name="statusUpdateResponse">
                <wsdlsoap:body use="literal"
namespace="http://www.acmepacket.com/NNISR/RemoteArchiverWS"

encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
            </output>
        </operation>
    </binding>
    <service name="RemoteArchiverWS">
        <port name="RemoteArchiverWSService"
binding="tns1:RemoteArchiverWSSoapBinding">
            <wsdlsoap:address
location="http://169.254.1.30:8080/RemoteArchiver/services/RemoteArch
iverWS/"/>
        </port>
    </service>
</definitions>
```

D ISR Database Schema Definitions and Descriptions

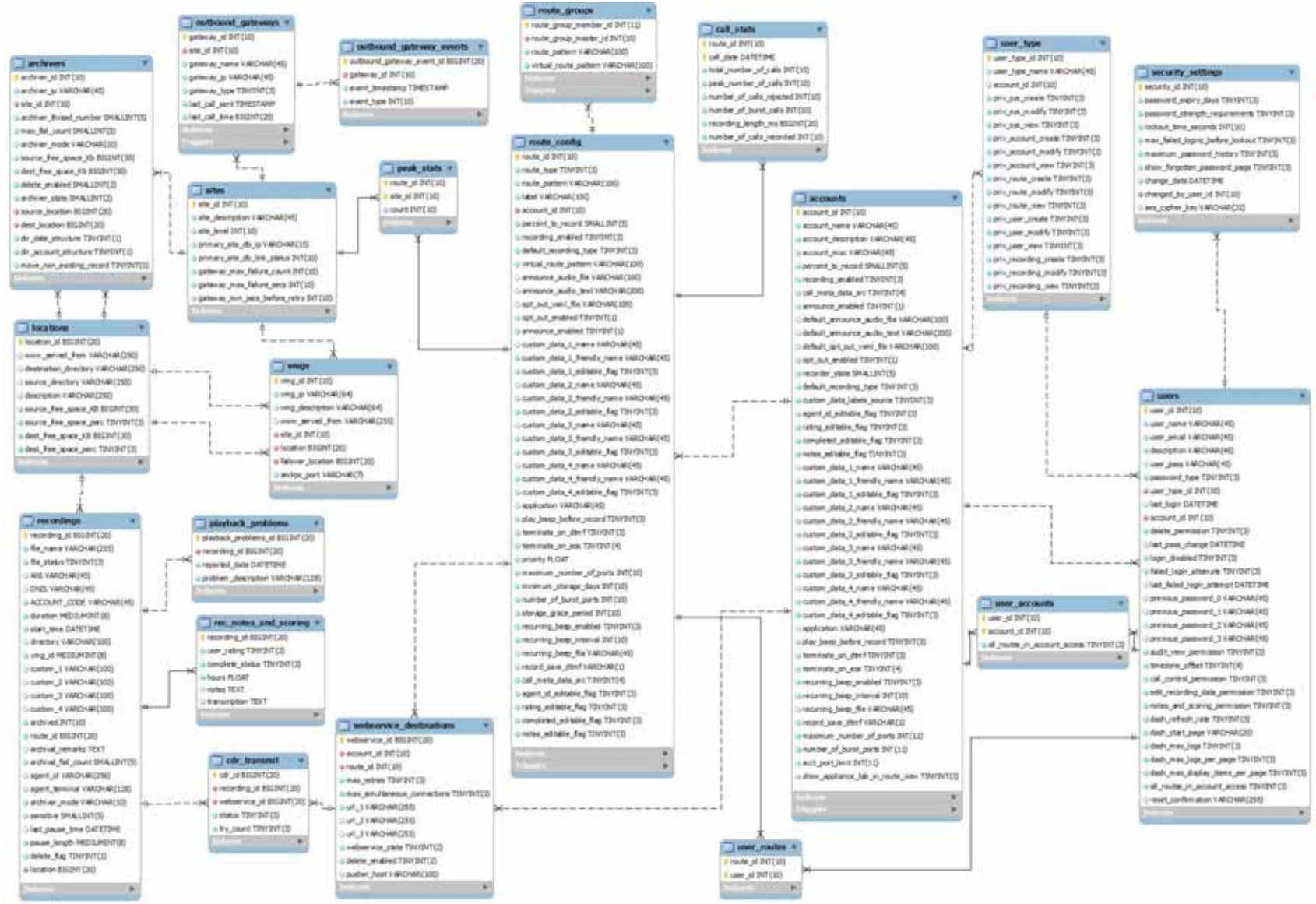
Introduction

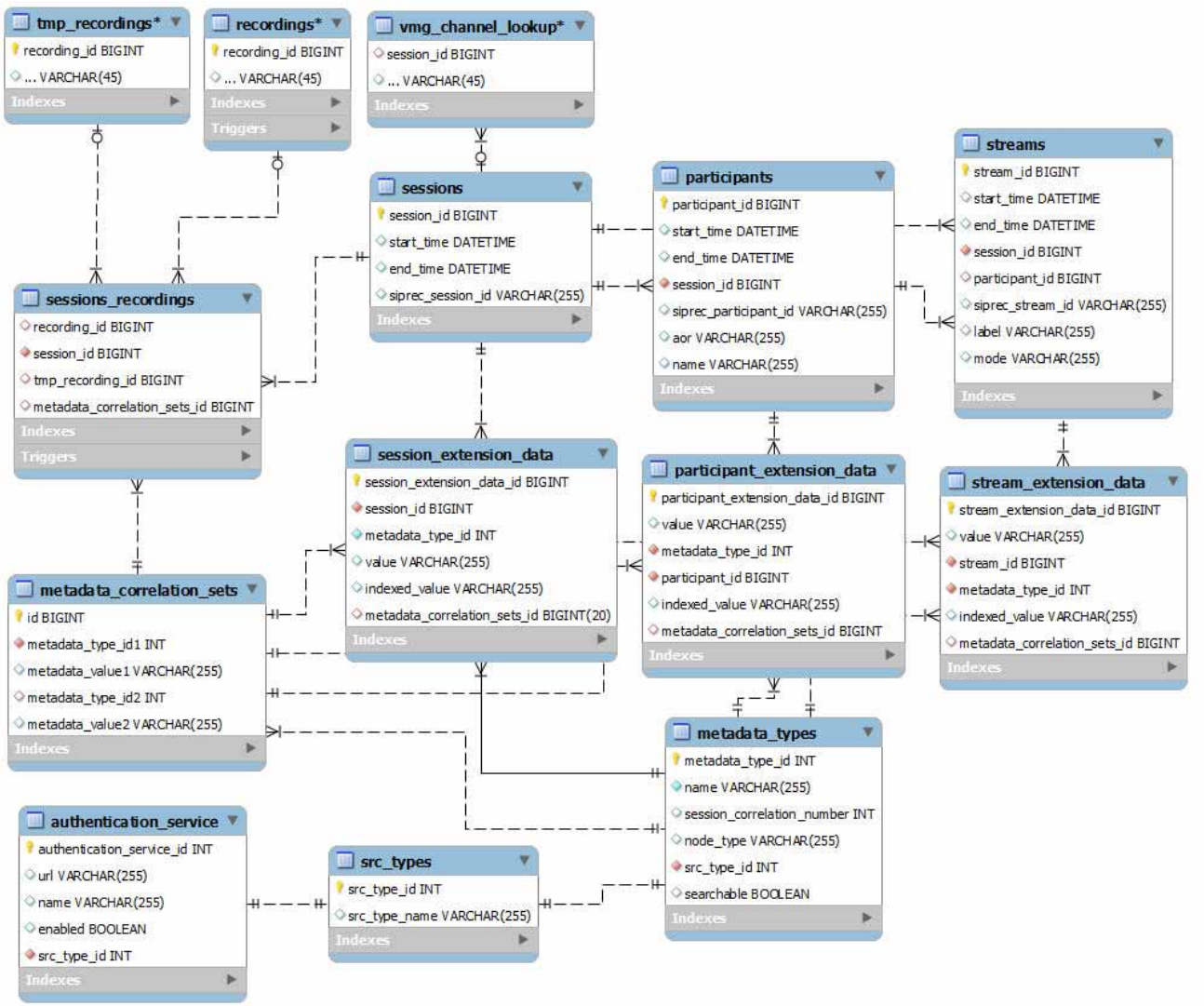
This appendix provides the Database Schema Definitions and Descriptions for the ISR Administrator Dashboard. It lists, in table format, the parameters contained in the Administrator Dashboard and provides the schema and descriptions of each parameter.

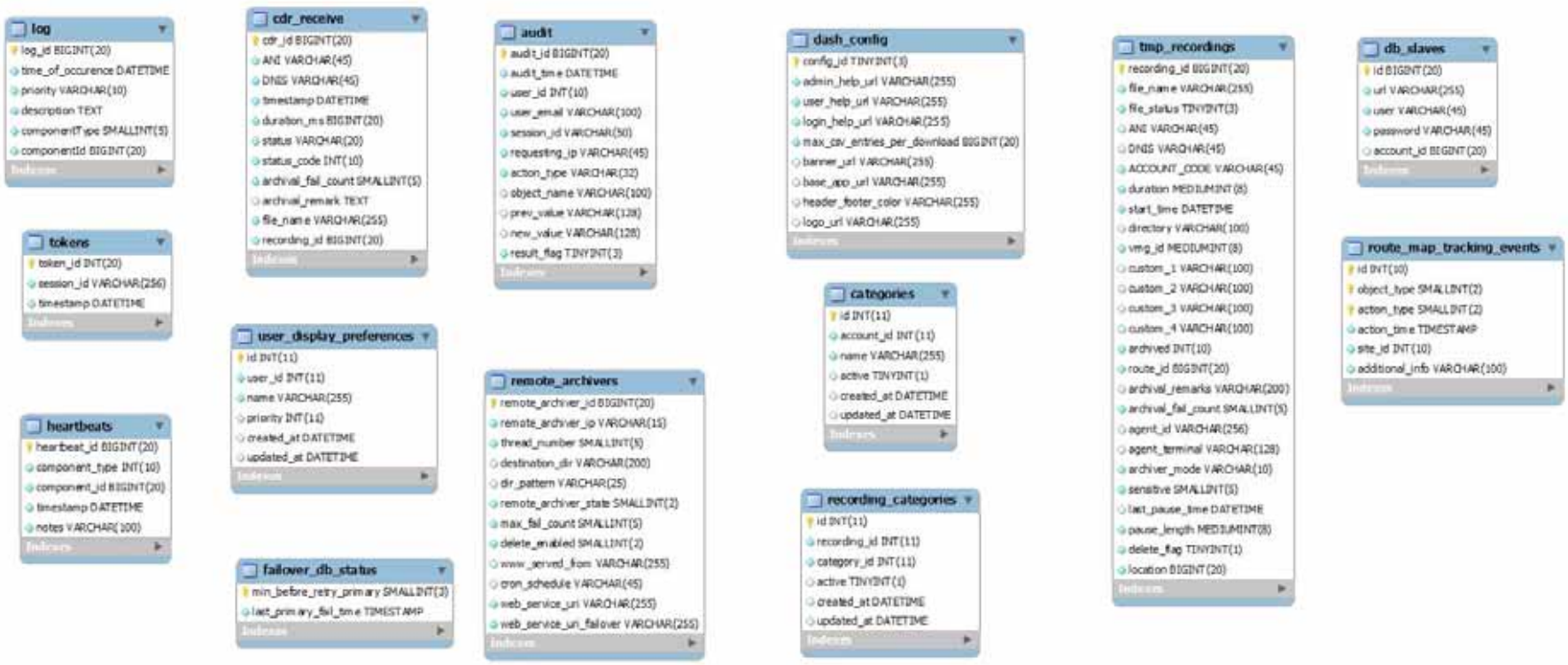
The following tables are included in the ISR Administrator Database Schema Descriptions:

- accounts
- archivers
- audit
- call_stats
- categories
- cdr_receive
- cdr_transmit
- dash_config
- db_slaves
- failover_db_status
- heartbeats
- locations
- log
- outbound_gateway_events
- outbound_gateways
- peak_stats
- playback_problems
- rec_notes_and_scoring
- recording_categories
- recordings
- remote_archivers
- route_groups
- route_map_tracking_events
- saved_searches
- security_settings
- sites
- tokens
- user_accounts
- user_display_preferences
- user_routes
- user_type
- users
- vmg_channel_lookup
- vmgs

ISR Administrator Database Schema Parameters




tmp_recordings*
recording_id BIGINT
... VARCHAR(45)
Indexes
recordings*
recording_id BIGINT
... VARCHAR(45)
Indexes
Triggers
vmg_channel_lookup*
session_id BIGINT
... VARCHAR(45)
Indexes
sessions
session_id BIGINT
start_time DATETIME
end_time DATETIME
siprec_session_id VARCHAR(255)
Indexes
participants
participant_id BIGINT
start_time DATETIME
end_time DATETIME
session_id BIGINT
siprec_participant_id VARCHAR(255)
aor VARCHAR(255)
name VARCHAR(255)
Indexes
streams
stream_id BIGINT
start_time DATETIME
end_time DATETIME
session_id BIGINT
participant_id BIGINT
siprec_stream_id VARCHAR(255)
label VARCHAR(255)
mode VARCHAR(255)
Indexes
sessions_recordings
recording_id BIGINT
session_id BIGINT
tmp_recording_id BIGINT
metadata_correlation_sets_id BIGINT
Indexes
Triggers
session_extension_data
session_extension_data_id BIGINT
session_id BIGINT
metadata_type_id INT
value VARCHAR(255)
indexed_value VARCHAR(255)
metadata_correlation_sets_id BIGINT(20)
Indexes
participant_extension_data
participant_extension_data_id BIGINT
value VARCHAR(255)
metadata_type_id INT
participant_id BIGINT
indexed_value VARCHAR(255)
metadata_correlation_sets_id BIGINT
Indexes
stream_extension_data
stream_extension_data_id BIGINT
value VARCHAR(255)
stream_id BIGINT
metadata_type_id INT
indexed_value VARCHAR(255)
metadata_correlation_sets_id BIGINT
Indexes
metadata_correlation_sets
id BIGINT
metadata_type_id1 INT
metadata_value1 VARCHAR(255)
metadata_type_id2 INT
metadata_value2 VARCHAR(255)
Indexes
metadata_types
metadata_type_id INT
name VARCHAR(255)
session_correlation_number INT
node_type VARCHAR(255)
src_type_id INT
searchable BOOLEAN
Indexes
authentication_service
authentication_service_id INT
url VARCHAR(255)
name VARCHAR(255)
enabled BOOLEAN
src_type_id INT
Indexes
src_types
src_type_id INT
src_type_name VARCHAR(255)
Indexes


log
log_id BIGINT(20)
time_of_occurence DATETIME
priority VARCHAR(10)
description TEXT
componentType SMALLINT(5)
componentId BIGINT(20)
cdr_receive
cdr_id BIGINT(20)
ANI VARCHAR(45)
DNIS VARCHAR(45)
timestamp DATETIME
duration_ms BIGINT(20)
status VARCHAR(20)
status_code INT(10)
archival_fail_count SMALLINT(5)
archival_remark TEXT
file_name VARCHAR(255)
recording_id BIGINT(20)
audit
audit_id BIGINT(20)
audit_time DATETIME
user_id INT(10)
user_email VARCHAR(100)
session_id VARCHAR(50)
requesting_ip VARCHAR(45)
action_type VARCHAR(32)
object_name VARCHAR(100)
prev_value VARCHAR(128)
new_value VARCHAR(128)
result_flag TINYINT(3)
dash_config
config_id TINYINT(3)
admin_help_url VARCHAR(255)
user_help_url VARCHAR(255)
login_help_url VARCHAR(255)
max_csv_entries_per_download BIGINT(20)
banner_url VARCHAR(255)
base_app_url VARCHAR(255)
header_footer_color VARCHAR(255)
logo_url VARCHAR(255)
tmp_recordings
recording_id BIGINT(20)
file_name VARCHAR(255)
file_status TINYINT(3)
ANI VARCHAR(45)
DNIS VARCHAR(45)
ACCOUNT_CODE VARCHAR(45)
duration MEDIUMINT(8)
start_time DATETIME
directory VARCHAR(100)
vmg_id MEDIUMINT(8)
custom_1 VARCHAR(100)
custom_2 VARCHAR(100)
custom_3 VARCHAR(100)
custom_4 VARCHAR(100)
archived INT(10)
route_id BIGINT(20)
archival_remarks VARCHAR(200)
archival_fail_count SMALLINT(5)
agent_id VARCHAR(256)
agent_terminal VARCHAR(128)
archiver_mode VARCHAR(10)
sensitive SMALLINT(5)
last_pause_time DATETIME
pause_length MEDIUMINT(8)
delete_flag TINYINT(1)
location BIGINT(20)
db_slaves
id BIGINT(20)
url VARCHAR(255)
user VARCHAR(45)
password VARCHAR(45)
account_id BIGINT(20)
tokens
token_id INT(20)
session_id VARCHAR(256)
timestamp DATETIME
categories
id INT(11)
account_id INT(11)
name VARCHAR(255)
active TINYINT(1)
created_at DATETIME
updated_at DATETIME
route_map_tracking_events
id INT(10)
object_type SMALLINT(2)
action_type SMALLINT(2)
action_time TIMESTAMP
site_id INT(10)
additional_info VARCHAR(100)
user_display_preferences
id INT(11)
user_id INT(11)
name VARCHAR(255)
priority INT(11)
created_at DATETIME
updated_at DATETIME
remote_archivers
remote_archiver_id BIGINT(20)
remote_archiver_ip VARCHAR(15)
thread_number SMALLINT(5)
destination_dir VARCHAR(200)
dir_pattern VARCHAR(25)
remote_archiver_state SMALLINT(2)
max_fail_count SMALLINT(5)
delete_enabled SMALLINT(2)
www_served_from VARCHAR(255)
cron_schedule VARCHAR(45)
web_service_uri VARCHAR(255)
web_service_uri_failover VARCHAR(255)
heartbeats
heartbeat_id BIGINT(20)
component_type INT(10)
component_id BIGINT(20)
timestamp DATETIME
notes VARCHAR(100)
recording_categories
id INT(11)
recording_id INT(11)
category_id INT(11)
active TINYINT(1)
created_at DATETIME
updated_at DATETIME
failover_db_status
min_before_retry_primary SMALLINT(3)
last_primary_fail_time TIMESTAMP

ISR Administrator Database Schema Descriptions

Table Name: Accounts — Purpose: Configuration and setup of accounts (tenants)

Field Name	Field Type	Nullable	Supported Values	Default	Description
account_id	int(10) unsigned	NOT NULL		auto increment	Primary key
account_name	varchar(45)	NOT NULL	Text		Name of the account
account_description	varchar(45)	NOT NULL	Text		Description of the account
account_misc	varchar(45)	NOT NULL	Text		Miscellaneous field for account identification
percent_to_record	smallint(5)	NOT NULL	1-100	25	Default recording percentage for routes created under this account
recording_enabled	tinyint(3)	NOT NULL	0=recording disabled 1=recording enabled	1	Whether recording is enabled by default for routes created under this account
call_meta_data_src	tinyint(1)	NOT NULL	0 = none 1 = TSPAI	0	For future use
announce_enabled	tinyint(1)	NOT NULL	0= announcement disabled 1=announcement enabled	0	Whether announcements are enabled by default for routes created under this account
default_announce_audio_file	varchar(100)		Text		Default announcement audio file for routes created under this account
default_announce_audio_text	varchar(200)		Text		Default announcement text for routes created under this account*
default_opt_out_vxml_file	varchar(100)		Text		Default VXML file for implementing opt-out on routes created under this account*
opt_out_enabled	tinyint(1)	NOT NULL	0 = disabled 1 = enabled	0	Whether opt out is enabled by default for routes created under this account*
recorder_state	smallint(5) unsigned	NOT NULL	0 = disabled 1 = enabled	0	Whether calls can currently be recorded for calls on routes under this account
default_recording_type	tinyint(3) unsigned	NOT NULL	See the admin guide for the supported recording formats.	0	The default recording format used for all routes under this account
custom_data_labels_source	tinyint(3) unsigned	NOT NULL	0=Route 1=Account	0	If 0, custom field labels defined at route will be shown. If 1, labels defined at account will be.
agent_id_editable_flag	tinyint(3) unsigned	NOT NULL	0 = not editable 1 = editable	0	Can users edit the data in the recordings.agent_id field
rating_editable_flag	tinyint(3) unsigned	NOT NULL	0 = not editable 1 = editable	0	Can users edit the data in the scoring rating? (rec_notes_and_scoring.user_rating)
completed_editable_flag	tinyint(3) unsigned	NOT NULL	0 = not editable 1 = editable	0	Can users edit the data in the complete transaction flag? (rec_notes_and_scoring.complete_status)
notes_editable_flag	tinyint(3) unsigned	NOT NULL	0 = not editable 1 = editable	0	Can users edit the scoring notes (rec_notes_and_scoring.notes)
custom_data_1_name	varchar(45)		Text	*NULL*	Name of Custom Data 1 Field (must match API calls)
custom_data_1_friendly_name	varchar(45)		Text	*Custom Data Field 1*	Displayed name of Custom Data 1 Field
custom_data_1_editable_flag	tinyint(3) unsigned	NOT NULL	0 = not editable 1 = editable	*0*	Can users edit Custom Data 1 Field?
custom_data_2_name	varchar(45)		Text	*NULL*	Name of Custom Data 2 Field (must match API calls)
custom_data_2_friendly_name	varchar(45)		Text	*Custom Data Field 2*	Displayed name of Custom Data 2 Field
custom_data_2_editable_flag	tinyint(3) unsigned	NOT NULL	0 = not editable 1 = editable	*0*	Can users edit Custom Data 2 Field?
custom_data_3_name	varchar(45)		Text	*NULL*	Name of Custom Data 3 Field (must match API calls)
custom_data_3_friendly_name	varchar(45)		Text	*Custom Data Field 3*	Displayed name of Custom Data 3 Field
custom_data_3_editable_flag	tinyint(3) unsigned	NOT NULL	0 = not editable 1 = editable	*0*	Can users edit Custom Data 3 Field?
custom_data_4_name	varchar(45)		Text	*NULL*	Name of Custom Data 4 Field (must match API calls)
custom_data_4_friendly_name	varchar(45)		Text	*Custom Data Field 4*	Displayed name of Custom Data 4 Field
custom_data_4_editable_flag	tinyint(3) unsigned	NOT NULL	0 = not editable 1 = editable	*0*	Can users edit Custom Data 4 Field?

application	varchar(45)		passthru, conference, callparking, recordandsave, VAMTest	NULL	Default route type used for routes under this account.
play_beep_before_record	tinyint(3) unsigned	NOT NULL	*0 = do not play* *1 = play*	0	Should the beep tone be played by default on a conference route under this account?
terminate_on_dtmf	tinyint(3) unsigned	NOT NULL	*0 = do not terminate on dtmf press* *1 = terminate on dtmf press*	0	Should a conference mode recording terminate on DTMF entry
terminate_on_eos	tinyint(4)	NOT NULL	*0 = do not terminate on eos* *1 = terminate on eos*	-1	Should a conference mode recording terminate on End of Speech *
recurring_beep_enabled	tinyint(3) unsigned	NOT NULL	*0=disabled* *1=enabled*	0	Enable/Disable recurring beep played during recording
recurring_beep_interval	int(10) unsigned	NOT NULL		30	If enabled, how often should the beep be played
recurring_beep_file	varchar(45)		*File Name*	*beep.wav*	Name of file, stored in RSS Cache, that should be played
record_save_dtmf	varchar(1)	NOT NULL	*0-9, #, * *	*#*	single dtmf digit that will save a recording made on a Record & Save route
maximum_number_of_ports	int(10) unsigned	NOT NULL		*24*	Default maximum number of simultaneous sessions a route created on this account will be able to support.
number_of_burst_ports	int(10) unsigned	NOT NULL		*6*	Default number of ports over maximum that the route will be able to use. These ports are reported separately.
acct_port_limit	int(11)	NOT NULL		*-1*	-1 for unlimited, The maximum number of sessions ALL routes on this account will be able to use.
show_appliance_tab_in_route_view	tinyint(3) unsigned	NOT NULL		*0*	Whether account's routes should be allowed to see and use the Appliance Tab

* deprecated

Table Name: archivers — Purpose: Definition and configuration of archivers

Field Name	Field Type	Nullable	Supported Values	Default	Description
archiver_id	int(10)	NOT NULL		auto increment	Primary key
archiver_ip	varchar(45)	NOT NULL	ip addresses	''	Archiver's IP Address
site_id	int(10)	NOT NULL		0	sites.site_id this archiver is associated with
source_directory	varchar(200)	NOT NULL			Directory where archiver should move files from – replaced with locations table; left for backwards compatibility
destination_directory	varchar(200)	NOT NULL			Directory where archiver should move files to – replaced with locations table; left for backwards compatibility
archiver_tread_number	smallint(5) unsigned	NOT NULL		1	Number of files to be moved simultaneously
max_fail_count	smallint(5) unsigned	NOT NULL		0	Number of times the archiver should attempt to move a file before permanently marking it failed
source_free_space_Kb	bigint(30) unsigned	NOT NULL		0	Amount of free space remaining on the source_directory
dest_free_space_Kb	bigint(30) unsigned	NOT NULL		0	Amount of free space remaining on the destination_directory
delete_enabled	smallint(2) unsigned	NOT NULL	0 = disabled 1 = enabled	0	Should the archiver delete files from the destination_directory after route_config.minimum_storage_days
archiver_state	smallint(2) unsigned	NOT NULL	0 = paused 1 = active	1	Is the archiver active?
archiver_mode	varchar(10)		Primary Failover	NULL	
source_location	bigint(20)	NOT NULL		-1	locations.location_id of the source location for this archiver
dest_location	bigint(20)	NOT NULL		-1	locations.location_id of the destination location for this archiver
dir_date_structure	tinyint(1)	NOT NULL	0 = do not archive with date structure 1 = archive with date structure	1	Should recordings be archived by date
move_non_existing_record	tintyint(1)	NOT NULL	0 = do not move non-existing files 1 = move non-existing files	0	if recording is not found, should record be removed from recordings db and added to recordings_missing table for tracking.

Table Name: audit — Purpose: Log user activity within the Admin Dashboard

Field Name	Field Type	Nullable	Supported Values	Default	Description
audit_id	bigint(20) unsigned	NOT NULL		auto increment	Primary key
audit_time	datetime	NOT NULL			Date entry added to table
user_id	int(10) unsigned	NOT NULL			users.user_id performing the action
user_email	varchar(100)	NOT NULL			users.email performing the action
session_id	varchar(50)	NOT NULL			User's session ID
requesting_ip	varchar(16)	NOT NULL			IP address the request originated from
action_type	varchar(16)	NOT NULL			Action the user performed
object_name	varchar(100)		VIEW_XXX Modify_XXX Create_XXX Delete_XXX where XXX=Account, Route, Site, User, Recording	NULL	Object the action was performed on
prev_value	varchar(128)			NULL	Value of the field before the edit
new_value	varchar(128)			NULL	Value of the field after the edit
result_flag	tinyint(3) unsigned	NOT NULL	0 = failed 1 = success	0	Was the action successful

Table Name: call_stats — Purpose: Track various system statistics to be used for reports

Field Name	Field Type	Nullable	Supported Values	Default	Description
route_id	int(10)	NOT NULL		0	route_config.route_id that is being tracked
call_date	datetime	NOT NULL		0000-00-00 00:00:00	date of statistical information
total_number_of_calls	int(10) unsigned	NOT NULL		0	Total number of INVITEs received by the RSS
peak_number_of_calls	int(10) unsigned	NOT NULL		0	Maximum number of simultaneous sessions for the call_date
number_of_calls_rejected	int(10) unsigned	NOT NULL		0	Total number of sessions RSS did not accept because session exceeds accounts.acct_port_limit or route_config.maximum_number_of_ports + route_config.number_of_burst_ports or RSS total licensed session capacity
number_of_burst_calls	int(10) unsigned	NOT NULL		0	Number of sessions handled on a burst port, if configured
recording_length_ms	bigint(20) unsigned	NOT NULL		0	Total length of all recordings on route_id for call_date
number_of_calls_recorded	int(10) unsigned	NOT NULL		0	Total number of RECORD START commands received by RSS

Table Name: categories — Purpose: Track various system statistics to be used for reports

Field Name	Field Type	Nullable	Supported Values	Default	Description
id	int(11)	NOT NULL		auto increment	Primary key
account_id	int(11)	NOT NULL			accounts.account_id category pertains to
name	varchar(255)	NOT NULL			name of category
active	tinyint(1)		0 = inactive 1 = active	0	Is category still used?
created_at	datetime			NULL	Date category was created
updated_at	datetime			NULL	Date category last updated

Table Name: cdr_receive — Purpose: Log of CDR records received on Remote Archiver Appliance

Field Name	Field Type	Nullable	Supported Values	Default	Description
cdr_id	bigint(20) unsigned	NOT NULL		auto increment	Primary key
ANI	varchar(45)	NOT NULL			ANI
DNIS	varchar(45)	NOT NULL			DNIS
timestamp	datetime	NOT NULL		0000-00-00 00:00:00	Time of call
duration_ms	bigint(20) unsigned	NOT NULL		0	Duration of Call
status	varchar(20)	NOT NULL		Complete	Status of receipt
status_code	integer unsigned	NOT NULL	0 = pending 1 = success 2 = fail 3 = maxfail 4 = processing	0	Status code for remote archiving
archival_fail_count	smallint(5) unsigned	NOT NULL		0	Number of failed attempts to archive
archival_remark	text			NULL	Comments about archival
file_name	varchar(255)	NOT NULL			Recording file name
recording_id	bigint(20) unsigned	NOT NULL			recordings.recording_id of the recording file

Table Name: cdr_transmit — Purpose: Log of CDR records sent to Remote Archiver Appliance

Field Name	Field Type	Nullable	Supported Values	Default	Description
crd_id	bigint(20) unsigned	NOT NULL		auto_increment	Primary key
recording_id	bigint(20) unsigned	NOT NULL			recordings.recording_id value transmitted
webservice_id	bigint(20) unsigned	NOT NULL			webservice_destinations.webservice_id used
status	tinyint(3) unsigned	NOT NULL	0 = pending 2 = attempted 3 = sent 4 = aborted	0	status of CDR transmission
try_count	tinyint(3)	NOT NULLL		0	number of transmission attempts currently made

Table Name: dash_config — Purpose: Global dashboard settings

Field Name	Field Type	Nullable	Supported Values	Default	Description
config_id	tinyint(3) unsigned	NOT NULL		auto_increment	Primary key
admin_help_url	varchar(255)	NOT NULL		adminHelp.jsp	Page to display when an Admin selects Help link
user_help_url	varchar(255)	NOT NULL		userHelp.jsp	Page to display when a user selects Help link
login_help_url	varchar(255)	NOT NULL		loginHelp.jsp	Page to display when a user selects Login help
max_csv_entries_per_download	bigint(20) unsigned	NOT NULL		10000	Maximum number of records to allow for a CSV download
banner_url	varchar(255)			logo2.gif	URL of banner to be displayed in User Dashboard
base_app_url	varchar(255)			http://localhost:9000/ipcr_dash	URL of base user dashboard application
header_footer_color	varchar(255)			#008DA8	Color to be used for header/footer show on user dashboard
logo_url	varchar(255)			acmepacket_logo.png	URL of logo for User dashboard branding

Table Name: db_slaves

Purpose: Configure database slaves to be used for read only access for certain accounts

Field Name	Field Type	Nullable	Supported Values	Default	Description
id	bigint(20) unsigned	NOT NULL		auto_increment	Primary Key
url	varchar(255)	NOT NULL			URL of database slave to be used
user	varchar(45)	NOT NULL			Database User
password	varchar(45)	NOT NULL			Database password
account_id	bigint(20) unsigned			NULL	accounts.account_id for which this db will be used

Table Name: failover_db_status

Purpose: Track the status of failover databases

Field Name	Field Type	Nullable	Supported Values	Default	Description
min_before_retry_primary	smallint(3) unsigned	NOT NULL		0	Minutes before db connection will be reattempted
last_primary_fail_time	timestamp	NOT NULL		0000-00-00 00:00:00	Timestamp of last failure to connect to primary db

Table Name: heartbeats

Purpose: Used by VAM SIP Test Route Type to track health of components

Field Name	Field Type	Nullable	Supported Values	Default	Description
heartbeat_id	bigint(20) unsigned	NOT NULL		auto_increment	Primary key
component_type	int(20) unsigned	NOT NULL	0 = unspecified 1 = archiver 2 = VxmlApi 3 = Dashboard		
component_id	bigint(20) unsigned	NOT NULL			The relevant foreign key
timestamp	datetime	NOT NULL		0000-00-00 00:00:00	Timestamp of last heartbeat
notes	varchar(100)	NOT NULL			

Table Name: locations — Purpose: Locations for recording storage and archival

Field Name	Field Type	Nullable	Supported Values	Default	Description
location_id	bigint(20)	NOT NULL		auto_increment	Primary key
www_served_from	varchar(250)			NULL	URL where files stored in this location will be served from
destination_directory	varchar(250)			NULL	Directory files will be moved to
source_directory	varchar(250)			NULL	Directory files will be moved from
description	varchar(250)			NULL	Descriptive text about this location
source_free_space_KB	bigint(30) unsigned	NOT NULL		0	Source directory free space
source_free_space_perc	tinyint(3) unsigned	NOT NULL		0	Source directory percentage of free space
dest_free_space_KB	bigint(30) unsigned	NOT NULL		0	Destination directory free space
dest_free_space_perc	tinyint(3) unsigned	NOT NULL		0	Destination directory percentage of free space

Table Name: log — Purpose: Log entries for RSS / displayed in Dashboard -> Sites

Field Name	Field Type	Nullable	Supported Values	Default	Description
log_id	bigint(20) unsigned	NOT NULL		auto increment	Primary key
time_of_occurrence	datetime	NOT NULL		0000-00-00 00:00:00	Date of log entry
priority	varchar(10)	NOT NULL		INFO	Log entry priority
description	text	NOT NULL			
componentType	smallint(5) unsigned	NOT NULL	0 = unspecified 1 = archiver 2 = VxmlApi 3 = Dashboard	0	
componentId	bigint(20) unsigned	NOT NULL		0	The relevant foreign key

Table Name: outbound_gateway_events Purpose: Track events on the outbound session agents

Field Name	Field Type	Nullable	Supported Values	Default	Description
outbound_gateway_event_id	bigint(20) unsigned	NOT NULL		auto_increment	Primary key
gateway_id	int(10) unsigned	NOT NULL			outbound_gateway.gateway_id the event occurred on
event_timestamt	timestamp	NOT NULL		CURRENT_TIMESTAMP	time of event
event_type	int(10) unsigned	NOT NULL	0 = unavailable 1 = tmp_disabled 2 = disabled 3 = back_in_service 4 = enabled	0	Status of outbound gateway

Table Name: outbound_gateways Purpose: Configure gateways RSS will connect calls to after applying recording logic

Field Name	Field Type	Nullable	Supported Values	Default	Description
gateway_id	int(10) unsigned	NOT NULL		auto_increment	Primary key
site_id	int(10) unsigned	NOT NULL			sites.site_id gateway is affiliated with
gateway_name	varchar(45)	NOT NULL			Gateway name
gateway_ip	varchar(45)	NOT NULL			IP Address of gateway. Can also include port.
gateway_type	tinyint(3) unsigned	NOT NULL	0 = in service 1 = temporarily disabled 2 = disabled 3 = failover 4 = temporarily disabled failover 5 = disabled failover	0	Status of gateway
last_call_sent	timestamp	NOT NULL		CURRENT_TIMESTAMP	Date/Time last call was delivered to this gateway
last_call_time	bigint(20) unsigned	NOT NULL		0	

Table Name: peak_stats — Purpose: Track peak number of calls per route/site

Field Name	Field Type	Nullable	Supported Values	Default	Description
route_id	int(10) unsigned	NOT NULL		0	route_config.route_id being tracked
site_id	int(10) unsigned	NOT NULL		0	sites.site_id
count	int(10) unsigned	NOT NULL		0	number of sessions

Table Name: playback_problems — Purpose: Track recordings with playback issues

Field Name	Field Type	Nullable	Supported Values	Default	Description
playback_problems	bigint unsigned	NOT NULL		auto increment	Primary key
recording_id	bigint unsigned	NOT NULL			recordings.recording_id with playback issue
reported_date	datetime	NOT NULL			Date problem reported
problem_description	varchar(128)	NOT NULL			Description of issue encountered

Table Name: rec_notes_and_scoring — Purpose: Notes and transcription data for recordings

Field Name	Field Type	Nullable	Supported Values	Default	Description
recording_id	bigint(20) unsigned	NOT NULL			recordings.recording_id
user_rating	tinyint(3) unsigned	NOT NULL		0	Rating the user assigns to this recording
complete_status	tinyint(3) unsigned	NOT NULL		0	Does the recording show a complete transaction
hours	float	NOT NULL		0	Hours spent on analysis
notes	text				Users notes on the recording
transcription	text				Transcription of the session recording

Table Name: recording_categories Purpose: Link recordings to categories

Field Name	Field Type	Nullable	Supported Values	Default	Description
id	int(11)	NOT NULL		auto increment	Primary key
recording_id	int(11)	NOT NULL			recordings.recording_id category assigned to
category_id	int(11)	NOT NULL			categories.category_id assigned
active	tinyint(1)		0 = inactive 1 = active	0	Is category still used
created_at	datetime			NULL	Date category was affiliated to recording
updated_at	datetime			NULL	Date affiliation last updated

Table Name: recordings Purpose: Recording details and meta data

Field Name	Field Type	Nullable	Supported Values	Default	Description
recording_id	bigint(20) unsigned	NOT NULL		auto_increment	Primary key
file_name	varchar(255)	NOT NULL			Recording file name
file_status	tinyint(3) unsigned	NOT NULL	0 = normal 1 = 404 File Not Found 2 = Playback problem reported	0	Recent file status
ANI	varchar(45)			NULL	ANI
DNIS	varchar(45)			NULL	DNIS
ACCOUNT_CODE	varchar(45)	NOT NULL			accounts.account_id
duration	mediumint(8)unsigned	NOT NULL		0	duration of recording
start_time	datetime	NOT NULL		0000-00-00 00:00:00	Session start time
directory	varchar(100)			NULL	recording location
vmg_id	mediumint(8) unsigned	NOT NULL		0	vmgs.vmg_id of the RSS the session was recorded on
custom_1	varchar(100)			NULL	Account/Route specific session information
custom_2	varchar(100)			NULL	Account/Route specific session information
custom_3	varchar(100)			NULL	Account/Route specific session information
custom_4	varchar(100)			NULL	Account/Route specific session information
archived	int(10) unsigned	NOT NULL		0	Archived state
route_id	bigint(20) unsigned	NOT NULL		0	route_config.route_id this session was recorded against
archival_remarks	text				Comments about archived state
archival_fail_count	smallint(5)unsigned	NOT NULL		0	Number of failed attempts to archive this recording
agent_id	varchar(256)			NULL	Agent ID
agent_terminal	varchar(128)			NULL	Agent Extension
archiver_mode	varchar(10)	NOT NULL	Primary Failover	Primary	Whether file archival by primary or failover archiver

sensitive	smallint(5) unsigned	NOT NULL		0	
last_pause_time	datetime			NULL	Last record pause timestamp for this recording. If null, was not paused.
pause_length	mediumint(8) unsigned	NOT NULL		0	Duration of last pause
delete_flag	tinyint(1)	NOT NULL	0 = do not delete 1 = delete	0	Mark the recording to be deleted after the session ends
location	bigint(20)	NOT NULL		-1	locations.location_id of the current location of this recording file

Table Name: remote_archivers Purpose: Configure archival to remote locations

Field Name	Field Type	Nullable	Supported Values	Default	Description
remote_archiver_id	bigint(20) unsigned	NOT NULL		auto_increment	Primary key
remote_archiver_ip	varchar(15)	NOT NULL			Remote IP address
thread_number	smallint(5) unsigned	NOT NULL		1	Number of simultaneous threads
destination_dir	varchar(200)			NULL	local directory where the remote archiver archives to
dir_pattern	varchar(25)			NULL	Storage pattern: %DATE% %HOUR% %MINUTE% supported
remote_archiver_state	smallint(2) unsigned	NOT NULL	0 = paused 1 = active	0	Status of remote archiver
max_fail_count	smallint(5) unsigned	NOT NULL		0	Number of times the archiver should attempt to move a file before permanently marking it failed
delete_enabled	smallint(2) unsigned	NOT NULL	0 = disabled 1 = enabled	0	Should the archiver delete files from the destination_directory after route_config.minimum_storage_days
www_served_from	varchar(255)			NULL	URL where recordings will be served from, location storage on remote archiver
cron_schedule	varchar(45)			NULL	cron schedule of the remote archival job
web_service_uri	varchar(255)	NOT NULL			remote archival web service URI
web_service_uri_failover	varchar(255)	NOT NULL			remote archival web service failover URI

Table Name: route_config

Purpose: Configure recording rules base on DNIS and/or ANI

Field Name	Field Type	Nullable	Supported Values	Default	Description
route_id	int(10) unsigned	NOT NULL	*Auto increment*		Primary key
route_type	tinyint(3) unsigned	NOT NULL	0 = DNIS 1 = ANI 2 = ANI/DNIS	0	Type of route
route_pattern	varchar(100)	NOT NULL			Value to be evaluated
label	varchar(100)	NOT NULL			Value to be shown as DNIS in recordings list
account_id	int(10) unsigned	NOT NULL		0	accounts.account_id route belongs to
percent_to_record	smallint(5)	NOT NULL	1-100	-1	Percentage of sessions to record
recording_enabled	tinyint(3)	NOT NULL	0=recording disabled 1=recording enabled	-1	Is recording enabled for this route
call_meta_data_src	tinyint(4)	NOT NULL	0 = none 1 = TSAPU	0	FUTURE USE
default_recording_type	tinyint(3) unsigned	NOT NULL	See the admin guide for the supported recording formats.	0	The default recording format used for this route
agent_id_editable_flag	tinyint(3) unsigned	NOT NULL	0 = not editable 1 = editable	0	Can users edit the data in the agent_id field
rating_editable_flag	tinyint(3) unsigned	NOT NULL	0 = not editable 1 = editable	0	Can users edit the data in the scoring rate information
completed_editable_flag	tinyint(3) unsigned	NOT NULL	0 = not editable 1 = editable	0	Can users edit the data in the complete transaction flag?
notes_editable_flag	tinyint(3) unsigned	NOT NULL	0 = not editable 1 = editable	0	Can users edit the scoring notes
virtual_route_pattern	varchar(100)			NULL	User value that will be set in the SIP URI on call leg from RSS
announce_audio_file	varchar(100)		Text	NULL	Announcement to be played on this route
announce_audio_text	varchar(200)		Text		TTS fallback in the event the announcement file is not available
opt_out_vxml_file	varchar(100)		Text		VXML file for implementing opt-out on this route*
opt_out_enabled	tinyint(1)	NOT NULL	0 = disabled 1 = enabled	0	Whether opt out is enabled
announce_enabled	tinyint(1)	NOT NULL	0= announcement disabled 1=announcement enabled	0	Whether announcements are enabled for this route
custom_data_1_name	varchar(45)		Text	*NULL*	Name of Custom Data 1 Field (must match API calls)
custom_data_1_friendly_name	varchar(45)		Text	*Custom Data Field 1*	Displayed name of Custom Data 1 Field
custom_data_1_editable_flag	tinyint(3) unsigned	NOT NULL	0 = not editable 1 = editable	*0*	Can users edit Custom Data 1 Field
custom_data_2_name	varchar(45)		Text	*NULL*	Name of Custom Data 2 Field (must match API calls)
custom_data_2_friendly_name	varchar(45)		Text	*Custom Data Field 2*	Displayed name of Custom Data 2 Field
custom_data_2_editable_flag	tinyint(3) unsigned	NOT NULL	0 = not editable 1 = editable	*0*	Can users edit Custom Data 2 Field
custom_data_3_name	varchar(45)		Text	*NULL*	Name of Custom Data 3 Field (must match API calls)
custom_data_3_friendly_name	varchar(45)		Text	*Custom Data Field 3*	Displayed name of Custom Data 3 Field
custom_data_3_editable_flag	tinyint(3) unsigned	NOT NULL	0 = not editable 1 = editable	*0*	Can users edit Custom Data 3 Field

custom_data_4_name	varchar(45)		Text	*NULL*	Name of Custom Data 4 Field (must match API calls)
custom_data_4_friendly_name	varchar(45)		Text	*Custom Data Field 4*	Displayed name of Custom Data 4 Field
custom_data_4_editable_flag	tinyint(3) unsigned	NOT NULL	0 = not editable 1 = editable	*0*	Can users edit Custom Data 4 Field
application	varchar(45)		passthru, conference, callparking, recordandsave, VAMTest	NULL	route type used for this route
play_beep_before_record	tinyint(3) unsigned	NOT NULL	*0*	0	Should the beep tone be played on route
terminate_on_dtmf	tinyint(3) unsigned	NOT NULL	*0*	0	Should a conference mode recording terminate on DTMF entry
terminate_on_eos	tinyint(4)	NOT NULL		-1	Should a conference mode recording terminate on End of Speech
priority	float	NOT NULL		0.5	order in which routes will be evaluated
maximum_number_of_ports	int(11) unsigned	NOT NULL		*24*	Maximum number of simultaneous sessions this route will be able to support.
number_of_burst_ports	int(10) unsigned	NOT NULL		*6*	Default number of ports over maximum that the route will be able to use. These ports are reported separately.
storage_grace_period	int(10) unsigned	NOT NULL		0	Number of days over minimum_storage_days that archiver should keep the recording before deleting
recurring_beep_enabled	tinyint(3) unsigned	NOT NULL	*0=disabled* *1=enabled*	0	Enable/Disable recurring beep played during recording
recurring_beep_interval	int(10) unsigned	NOT NULL		30	If enabled, how often should the beep be played
recurring_beep_file	varchar(45)		*File Name*	*beep.wav*	Name of file, stored in RSS Cache, that should be played
record_save_dtmf	varchar(1)	NOT NULL		*#*	single-digit dtmf that will save a recording made on a Record & Save route

Table Name: route_groups

Purpose: Create and define a group of routes that should all have the same master requirements

Field Name	Field Type	Nullable	Supported Values	Default	Description
route_group_member_id	int(11)	NOT NULL		auto_increment	Primary key
route_group_master_id	int(10) unsigned	NOT NULL			route_config.route_id of the master ID
route_pattern	varchar(100)	NOT NULL			route pattern to be evaluated
virtual_route_pattern	varchar(100)	NOT NULL			user value of end destination

Table Name: route_map_tracking_events

Purpose: Track events related to the route map caching

Field Name	Field Type	Nullable	Supported Values	Default	Description
id	int(10) unsigned	NOT NULL		auto_increment	Primary key
object_type	smallint(2) unsigned	NOT NULL	0 = account 1 = route 2 = obgateway		Object event pertains to
action_type	smallint(2) unsigned	NOT NULL	0 = add 1 = changed 2 = delete		Type of action
action_time	timestamp	NOT NULL		CURRENT_TIMESTAMP	Time of event
site_id	int(10)	NOT NULL		-1	sites.site_id event pertains to
additional_info	varchar(100)	NOT NULL			Additional information

Table Name: saved_searches Purpose: Define searches saved in User Dashboard

Field Name	Field Type	Nullable	Supported Values	Default	Description
id	int(11)	NOT NULL		auto increment	primary key
user_id	int(11)	NOT NULL			users.user_id which saved the search
name	varchar(255)	NOT NULL			name of saved search
mode	int(11)			1	Type of Saved search
category_id	int(11)			NULL	Search category ID
ANI	varchar(255)			NULL	ANI provided in search
DNIS	varchar(255)			NULL	DNIS provided in search
filename	varchar(255)			NULL	filename provided in search
agented	varchar(255)			NULL	agent id provided in search
duration	varchar(255)			NULL	duration of recordings provided in search
custom1	varchar(255)			NULL	value to search in custom data field 1
custom2	varchar(255)			NULL	value to search in custom data field 2
custom3	varchar(255)			NULL	value to search in custom data field 3
custom4	varchar(255)			NULL	value to search in custom data field 4
vmg	varchar(255)			NULL	value to search in vmg
duration_start	varchar(255)			NULL	search duration minimum duration
duration_stop	varchar(255)			NULL	search duration maximum duration
date_start	varchar(255)			NULL	search calls after this date
date_stop	varchar(255)			NULL	search calls before this date
allow_partial	tinyint(1)		0 = do not allow 1 = allow		search for partial match of values within specified fields
active	tinyint(1)		0 = inactive 1 = active		Search is currently active
date_relative	varchar(255)			NULL	search relative to which date
date_search_type	varchar(255)			range	what type of date search to perform
created_at	datetime			NULL	Date search initially saved
updated_at	datetime			NULL	Date of last update to search criteria

Table Name: security_settings Purpose: Configure dashboard security settings

Field Name	Field Type	Nullable	Supported Values	Default	Description
security_id	int(10) unsigned	NOT NULL		auto increment	Primary key
password_expiry_days	tiyint(3) unsigned	NOT NULL		90	Number of days before a user password expires
password_strength_requirements	tinyint(3) unsigned	NOT NULL	0 = 1 = 2 =	2	how strong does a user password need to be
lockout_time_seconds	int(10) unsigned	NOT NULL		3600	Length of time a user will be locked out after max_failed_logins_befpre_lockout
max_failed_logins_before_lockout	tinyint(3) unsigned	NOT NULL		5	Number of failed login attempts a user will be allowed before being locked out
maximum_password_history	tinyint(3) unsigned	NOT NULL		4	Number of password changes before a user can reuse a password
show_forgotten_password_page	tinyint(3) unsigned	NOT NULL	0 = do not show 1 = show	0	Should users see the link to be emailed a password
aes_cypher_key	varchar(32)			NULL	Cypher key used for encryption of data
change_date	datetime	NOT NULL			Date of last security change
changed_by_user_id	int(10) unsigned	NOT NULL			users.user_id who made last change

Table Name: sites — Purpose: Configuration of site information

Field Name	Field Type	Nullable	Supported Values	Default	Description
site_id	int(10) unsigned	NOT NULL		auto increment	Primary key
site_description	varchar(45)	NOT NULL			Site name
site_level	int(10) unsigned	NOT NULL	0 = Primary 1 = Secondary	0	Site type
primary_site_db_ip	varchar(15)	NOT NULL			database IP to be used with this site
primary_site_db_link_status	int(10) unsigned	NOT NULL	0 = Up 1 = Down 2 = Sync Needed 3 = Sync in Progress	0	DB status
gateway_max_failure_count	int(10) unsigned	NOT NULL		5	Sets the maximum number of outbound gateway failures allowed in max_fail_seconds before gateway is disabled.
gateway_max_failure_secs	int(10) unsigned	NOT NULL		30	Number of seconds that number of failures can occur before gateway is disabled
gateway_min_secs_before_retry	int(10) unsigned	NOT NULL		300	once temp disabled, how long before the gateway will be retried

Table Name: tokens — Purpose: Assign tokens to sessions

Field Name	Field Type	Nullable	Supported Values	Default	Description
token_id	int(20) unsigned	NOT NULL		auto increment	Primary key, zero fill
session_id	varchar(256)	NOT NULL			Session ID token assigned to
timestamp	datetime	NOT NULL		0000-00-00 00:00:00	Session time

Table Name: user_accounts — Purpose: Affiliate users with accounts

Field Name	Field Type	Nullable	Supported Values	Default	Description
user_id	int(10) unsigned	NOT NULL			users.user_id
account_id	int(10) unsigned	NOT NULL			accounts.account_id
alt_routes_in_account_access	tinyint(3) unsigned	NOT NULL	0 = disabled 1 = enabled	does user have access to all routes in account	

Table Name: user_display_preferences Purpose: configure user preferences in User Dashboard

Field Name	Field Type	Nullable	Supported Values	Default	Description
id	int(11)	NOT NULL		auto increment	Primary key
user_id	int(11)	NOT NULL			users.user_id preferences pertain to
name	varchar(255)	NOT NULL			
priority	int(11)			0	Priority
created_at	datetime			NULL	Date preferences created
updated_at	datetime			NULL	Date preferences last updated

Table Name: user_routes Purpose: Affiliate users with routes

Field Name	Field Type	Nullable	Supported Values	Default	Description
route_id	int(10) unsigned	NOT NULL			route_config.route_id
user_id	int(10) unsigned	NOT NULL			users.user_id

Table Name: user_type

Purpose: Define user types and the privileges available to each

Field Name	Field Type	Nullable	Supported Values	Default	Description
user_type_id	int(10) unsigned	NOT NULL		auto increment	Primary key
user_type_name	varchar(45)	NOT NULL			name of this user type
account_id	int(10) unsigned			NULL	account id this user is specifically tied to
priv_sys_create	tinyint(3) unsigned	NOT NULL	0 = disabled 1 = enabled	0	User can create system elements
priv_sys_modify	tinyint(3) unsigned	NOT NULL	0 = disabled 1 = enabled	0	User can modify system elements
priv_sys_view	tinyint(3) unsigned	NOT NULL	0 = disabled 1 = enabled	0	User can view system elements
priv_account_create	tinyint(3) unsigned	NOT NULL	0 = disabled 1 = enabled	0	User can create accounts
priv_account_modify	tinyint(3) unsigned	NOT NULL	0 = disabled 1 = enabled	0	User can modify accounts
priv_account_view	tinyint(3) unsigned	NOT NULL	0 = disabled 1 = enabled	0	User can view accounts
priv_route_create	tinyint(3) unsigned	NOT NULL	0 = disabled 1 = enabled	0	User can create routes
priv_route_modify	tinyint(3) unsigned	NOT NULL	0 = disabled 1 = enabled	0	User can modify routes
priv_route_view	tinyint(3) unsigned	NOT NULL	0 = disabled 1 = enabled	0	User can view routes
priv_user_create	tinyint(3) unsigned	NOT NULL	0 = disabled 1 = enabled	0	User can create users
priv_user_modify	tinyint(3) unsigned	NOT NULL	0 = disabled 1 = enabled	0	User can modify users
priv_user_view	tinyint(3) unsigned	NOT NULL	0 = disabled 1 = enabled	0	User can view users
priv_recording_create	tinyint(3) unsigned	NOT NULL	0 = disabled 1 = enabled	0	User can create recordings
priv_recording_modify	tinyint(3) unsigned	NOT NULL	0 = disabled 1 = enabled	0	User can modify recording / data
priv_recording_view	tinyint(3) unsigned	NOT NULL	0 = disabled 1 = enabled	0	User can view recordings / data

Table Name: users

Purpose: Define users, track login history and their dashboard preferences

Field Name	Field Type	Nullable	Supported Values	Default	Description
user_id	int(10) unsigned	NOT NULL		auto increment	primary key
user_name	varchar(45)	NOT NULL			User's name
user_email	varchar(45)	NOT NULL			user's login
description	varchar(45)	NOT NULL			User description
user_pass	varchar(45)			NULL	user's password
password_type	tinyint(3) unsigned	NOT NULL	0 = MD5 1 = AES	0	what type of encryption was used on password
user_type_id	int(10) unsigned	NOT NULL		0	user_types.user_type_id
last_login	datetime			NULL	date of last login
account_id	int(10) unsigned	NOT NULL		0	Primary account user is affiliated with
delete_permission	tinyint(3) unsigned	NOT NULL	0 = disabled (cannot delete) 1 = enabled (can delete)	1	Can user delete recordings
last_pass_change	datetime			NULL	Date of last password change
login_disabled	tinyint(3) unsigned	NOT NULL	0 = enabled 1 = disabled		Login active
failed_login_attempts	tinyint(3) unsigned	NOT NULL		0	Number of failed login attempts since last successful login
last_failed_login_attempt	datetime			NULL	Date and time of last failed login attempt
previous_password_0	varchar(45)			NULL	users prior password
previous_password_1	varchar(45)			NULL	users prior password
previous_password_2	varchar(45)			NULL	users prior password
previous_password_3	varchar(45)			NULL	users prior password`
audit_view_permission	tinyint(3) unsigned	NOT NULL	0 = cannot view audit logs 1 = can view audit logs	0	Can user view audit logs
timezone_offset	tinyint(4)	NOT NULL		0	Users timezone in relation to GMT
call_control_permission	tinyint(3) unsigned	NOT NULL	0 = cannot view 1 = can view	0	Can user see call controls option
edit_recording_data_permission	tinyint(3) unsigned	NOT NULL	0 = cannot edit 1 = can edit	0	can user edit recording metadata
notes_and_scoring_permission	tinyint(3) unsigned	NOT NULL	1 = cannot view 1 = can view	0	Can user view notes and scoring option
dash_refresh_rate	tinyint(3) unsigned	NOT NULL		10	Rate at which dashboard refreshes
dash_start_page	varchar(20)	NOT NULL		recordings	page displayed when user logs in
dash_max_logs	tinyint(3) unsigned	NOT NULL		40	Number of pages of logs to show
dash_max_logs_per_page	tinyint(3) unsigned	NOT NULL		10	Number of logs to show per page
dash_max_display_items_per_page	tinyint(3) unsigned	NOT NULL		15	Number of items (not logs) to show per page
all_routes_in_account_access	tinyint(3) unsigned	NOT NULL	0 = not by default 1 = by default	0	Does user have access to all routes under their assigned account (only implemented in User Dashboard)
reset_confirmation	varchar(255)				

Table Name: vmg_channel_lookup Purpose: Mapping of sessions to channels on the RSS

Field Name	Field Type	Nullable	Supported Values	Default	Description
vmg_id	int(10) unsigned	NOT NULL		0	vmgs.vmg_id; RSS handling session
channel_no	int(10) unsigned	NOT NULL		0	channel number handling session
ANI	varchar(45)	NOT NULL			ANI of active session
DNIS	varchar(45)	NOT NULL			DNIS of active session
start_of_call	datetime	NOT NULL		0000-00-00 00:00:00	session start time
recording_file_name	varchar(100)			NULL	name of file being recorded for this session
virtual_dnis	varchar(45)			NULL	virtual route pattern invoked on this session
route_id	bigint(20)unsigned	NOT NULL		0	route ID invoked on this session
account_id	int(10) unsigned	NOT NULL		1	account ID for this session
call_state	tinyint(3) unsigned	NOT NULL	0 = Unknown 1 = Observed	0	Current call state

Table Name: vmgs Purpose: RSS configuration

Field Name	Field Type	Nullable	Supported Values	Default	Description
vmg_id	int(10) unsigned	NOT NULL		auto increment	Primary key
vmg_ip	varchar(64)			NULL	RSS IP address – SIP signaling
vmg_description	varchar(64)			NULL	Description
www_served_from	varchar(255)			NULL	URL where recordings stored on this RSS will be served from
site_id	int(10) unsigned	NOT NULL		0	Site this RSS is affiliated with
location	bigint(20)	NOT NULL		-1	locations.location_id for primary recording storage
failover_location	bigint(20)	NOT NULL		-1	locaitons.location_id for failover recording storage
xmlrpc_port	varchar(7)	NOT NULL		8888	xmlrpc port this RSS is listening on

Table Name: webservice_destinations Purpose: Configure webservices (through appliances tab)

Field Name	Field Type	Nullable	Supported Values	Default	Description
webservice_id	bigint(20) unsigned	NOT NULL		auto increment	Primary key
account_id	int(10) unsigned	NOT NULL			accounts.account_id info that will be sent to this webservice
route_id	int(10) unsigned	NOT NULL			route_config.route_id info that will be sent to this webservice
max_retries	tinyint(3) unsigned	NOT NULL		5	Number of attempts to send a record to webserivce before marked as failure; 0 = unlimited attempts
max_simultaneous_connections	tinyint(3) unsigned	NOT NULL		24	maximum number of simultaneous connections; 0=unlimited
url_1	varchar(255)	NOT NULL			Primary web service URL
url_2	varchar(255)			NULL	Secondary web service URL
url_3	varchar(255)			NULL	Tertiary web service URL
webservice_state	tinyint(2) unsigned	NOT NULL	0 = paused 1 = unpaused	0	Webservice state
delete_enabled	tinyint(2) unsigned	NOT NULL	0 = disabled 1 = enabled	0	Can web service delete
pusher_host	varchar(100)			NULL	current pusher host name