Administrator Guide

AudioCodes One Voice for Microsoft® Skype for Business

SmartTAP

Call Recording Solution

Version 4.2

Table of Contents

List of Figures

List of Tables

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: August-27-2018

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our Web site at https://www.audiocodes.com/services-support/maintenance-and-support.

Email: support@audiocodes.com

North America: +1-732.652-1085, +1-800-735-4588

Israel: 1-800-30-50-70, +972-3-9764343

International Number: +800 444 22 444

APAC: +65-6493-6690

Note: Technical Support does not monitor Web or e-mail requests 24 hours a day. After normal business hours (as specified above), any communication through our support Web site or support e-mail are addressed the following business day.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Related Documentation

Document Name
SmartTAP Release Notes
SmartTAP Installation Guide

Document Revision Record

LTRT	Description
27160	Initial document release for Version 3.1.0.
27161	Initial document release for Version 3.2.0.
27162	Version 3.2. Recording Profiles. IM. Recording consent. User / Device Attributes. Media Folder. Recording purge date. Messages tab.
27163	Added Single Sign-On as an Appendix.
27164	Updated Figure 1-2.
27165	Managing Licenses, Defining Credentials, Alarm History, Configuring Alarm Notifications, Windows Event Log, SCOM Integration, Call tagging, Configuring HTTPS, Searching for Calls, Listening to / Emailing / Downloading a Call, Using the Evaluation feature, Searching for messages and Live Monitoring.
27166	Updated note under the Listening to / Emailing / Downloading a Call section.
27167	Video recordings; Peer to peer file transfer transactions recording; New fields, Media status and reason, added to call records; Recording Health Monitoring utility.
27168	There are no changes in this document.
27169	Skype for Business Desktop Sharing recording; updates to Managed Devices functionality; updates for LDAP mapping; Managing calls with Desktop sharing recording; Timeline view; new appendix Announcement Server (Skype for Business).Update for including the Subject Alternative Name in the generation of certificates.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site https://online.audiocodes.com/documentation-feedback.

1 About SmartTAP

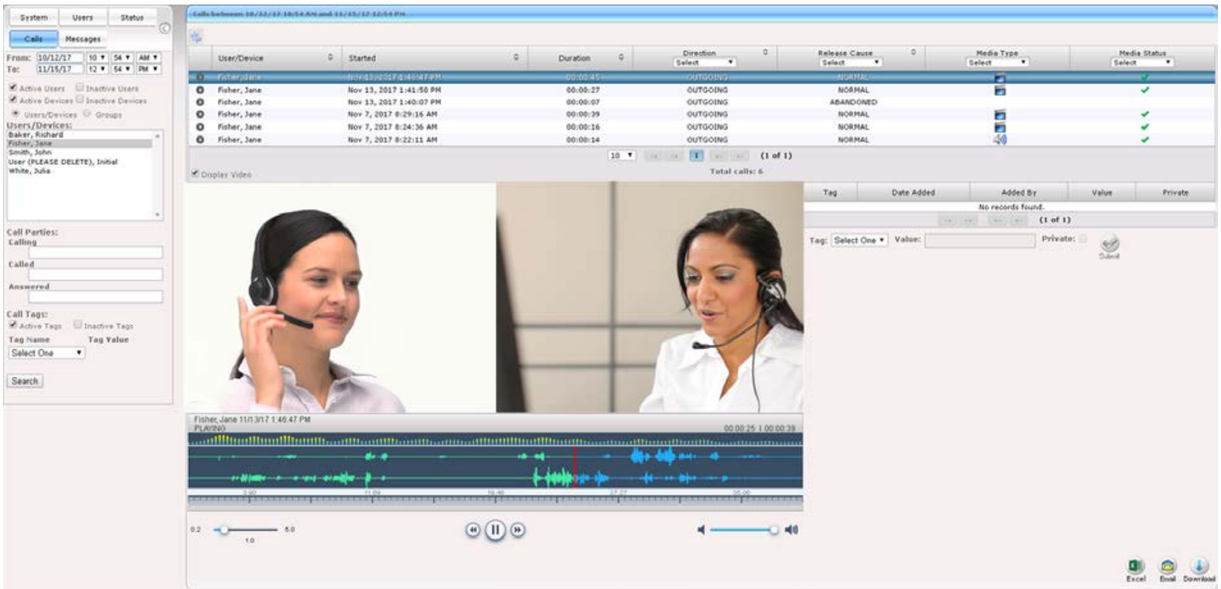
AudioCodes' SmartTAP for Microsoft Skype for Business is a certified and secure call recording solution that enables the recording of key business interactions within a Microsoft Skype for Business environment. SmartTAP is compatible with VoIP, TDM, and hybrid telephony environments.

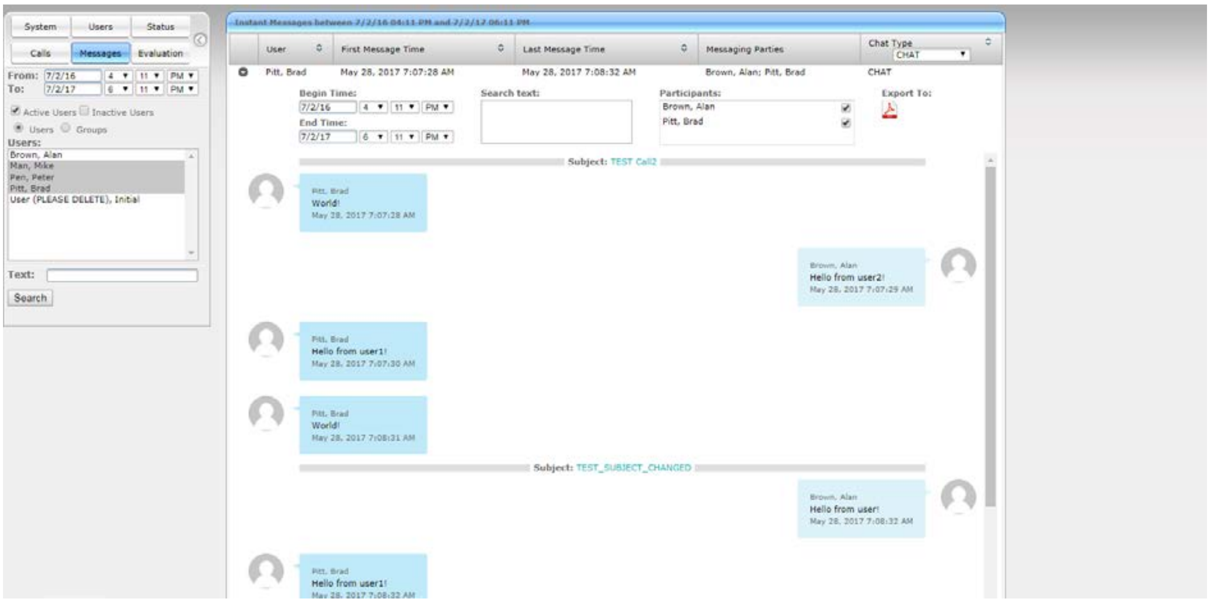
SmartTAP is an enterprise-wide compliance and liability recorder. Though most recorders in the market focus on Contact Center features, SmartTAP is deployed across the enterprise to capture calls, either on-demand or, in some cases, full time, when calls about compliance and liability occur more frequently.

With an integral Skype for Business recording toolbar, enterprise users can record with SmartTAP anywhere and anytime they are on Skype for Business calls.

SmartTAP can initially be deployed on a small scale and be scaled up to support many thousands of users using the product’s linear scalability feature.

SmartTAP includes audio video and instant messaging recording capabilities.





1.1 SmartTAP Benefits

SmartTAP benefits organizations and enterprises as follows:

- Recordings can be used for customer analytics to provide intelligence of customer dealings to serve at the basis for improving key performance indicators and thereby enhance customer satisfaction and loyalty.
- Minimizes exposure to disputes and mitigates the risk of reputation damage
- Improves internal policy compliance
- Complies with the increasing level of corporate and governmental regulation for customer dealings

1.2 Competitive Advantages

- **User Friendly**
  - Intuitive Web-based screens make training easy. No downtime for training.
  - All browser-based access with no additional client desktop software.
  - Supports any Wi-Fi tablet or smartphone.
- **Economic**
  - Large system features at a fraction of the cost.
  - Linear growth of SmartTAP concurrent conversations – no forklift upgrades.
  - Add one license at a time, or a hundred.
  - Lowest total cost of ownership.
  - Centralized architecture reduces hardware investments.
- **Scalable**
  - Start with as little as 8 concurrent recording channels and scale upwards.
  - 300 concurrent recording sessions per recording server.
  - Supports for single site, multi-site and cloud deployments.
  - Start with recording and then expand capabilities with easy-to-add modules.

1.3 Features Overview

The table below lists and describes AudioCodes' SmartTAP recording features.

Table 1-1: SmartTAP Features

Feature	Details
Status Page	▪ Displays the current user call status ▪ Live Call Monitoring ▪ Notes can be added to an active call ▪ Allows switching between Grid and List View ▪ Pause / Resume Recording ▪ Record or Save on Demand
Record or Save on Demand	▪ Record on Demand (ROD): Recording contains audio from the point network administrator decides to record the call. ▪ Save on Demand (SOD): Recording contains audio from the beginning of the call. ▪ Recording using ROD or SOD is manually selected from the GUI or Skype for Business client extension. ▪ Any target provisioned as ROD or SOD can manually control start/stop recording. ▪ Any user with appropriate security profile credentials can manually trigger a recording of another user's calls.
PCI Compliance	▪ Capability to pause / resume a recording during sensitive areas of a conversation with a customer, e.g., when taking Credit Card details. ▪ Manual process, executed from the Status page.
Recording Profiles	▪ Can be created and assigned to multiple parties to define the recording method. ▪ Full Time Recording – Automatic audio or video recording. ▪ Record on Demand – Audio recording is manually triggered from the Status page in the GUI or Skype for Business / Lync Conversation Window Extension (CWE) toolbar (see Figure 1-2). ▪ Save on Demand – Audio or Video recording is manually triggered from the Status page in the GUI or from the Skype for Business / Lync CWE toolbar (see ▪ Figure 1-1). ▪ PCI (Payment Card Industry) Pause / Resume Recording (Optional) – Audio recording is manually triggered from the Status page in the GUI or from the Skype for Business / Lync CWE toolbar. ▪ IM recording – automatic Instant Message recording.
Security Profiles	▪ Can be created and assigned to multiple parties to define security access in SmartTAP. ▪ All recordings can be performed using another user's ROD or SOD.
LDAP Integration	▪ Allows SmartTAP to use Active Directory users, groups, and security groups ▪ LDAP Filtering by user, group or security group.
Legal Hold	▪ The user's retention process does not purge their recordings when placed on legal hold.
Audit Trail	▪ Search audit trail based on date range, user, set of users. ▪ Filtering of search results directly in the results screen, sorting ascending/descending by clicking column header, shortcuts to the beginning/end page within the results screen.

Feature	Details
	▪ Export of Audit Trail results and call Meta Data to Excel file.
Flexible and Powerful Call and Instant Message Search Capabilities	▪ Search criteria based on date range, time of day range, user, set of users, group, set of groups, etc. ▪ Easily filter search results, sorting ascending/descending by clicking column header, shortcuts to the beginning/end page within the results screen. ▪ Use of a * symbol 'wild card' to apply a filter. ▪ Columns can be added to / removed from the results screen. ▪ Search for calls based on Calling (Caller ID), Called or Answering Party ▪ Search for calls based on assigned Call Tag, including Notes. ▪ Search for Instant Messages based on included strings. ▪ Easily export Call Meta Data from search results to Excel file. ▪ Easily export an Instant Message conversation to a PDF file.
Playback (Call Listen/Download/Email)	▪ Fast-forward / Rewind or select playback position controls. ▪ Volume control.
Call and Instant Message Retention	▪ N number of retention periods can be added and applied to specific user(s). ▪ Recordings are automatically deleted based on retention period. ▪ Option to retain recordings based on evaluation status.
Automatic Email Notifications	▪ Automatic email notifications when Alarms are triggered or thresholds are exceeded (Recording licenses or Storage capacity).
Encryption of Stored Recordings	▪ Option to encrypt stored audio recordings.
Recordings Storage in Local Drive, NAS or SAN	▪ Recordings stored in local hard disk or in NAS/SAN through Windows share (SMB).
Compression of Stored Recordings	▪ Audio recordings stored as G.711 (normal compression) or G.729a (high compression).
Agent Evaluation	▪ Evaluation forms can be created: agents evaluations, review evaluations, and reports can be generated.
Distributed Architecture	▪ One SmartTAP may be deployed across multiple physical locations. ▪ Recording on remote locations is not interrupted even if connection to main site is down.
Multiple Call Protocols and Physical Interfaces Share the Same UI	▪ One SmartTAP server is capable of recording diverse call signaling and voice protocols. ▪ SmartTAP records PSTN, Lync, Analog, and VoIP simultaneously and transparently to end users.
Skype for Business / Lync Client Toolbar	▪ Auto extended Lync CWE for convenient access to features like ROD / SOD, PCI and Call Tagging
Call Tagging	▪ User definable tags i.e., Customer Name, Account Number, Malicious Call, etc. ▪ Default Notes tag available by default. ▪ Tags are easily added live from the Status page or from Lync CWE, or post call, from the Calls tab.
Single Sign-On	▪ A user gains access into the SmartTAP GUI or Lync client toolbar after validation of their SmartTAP security profile and authentication of their credentials against Active Directory.

Feature	Details
SIPRec	▪ Session Initiation Protocol (SIP) establishes an active recording session and reporting of metadata to the SRS (SmartTAP) of the active communication session traversing the SRC (AudioCodes SBC or Gateway). ▪ https://datatracker.ietf.org/doc/draft-ietf-siprec-protocol/
REST API	▪ Allows third-party applications integrated with SmartTAP to add users, retrieve metadata, download recorders, target users, etc. Refer to separate documentation for more details. ▪ Initiate ROD or SOD from a third-party application using the API. ▪ Support for Server Sent Events (SSE). Third-party applications can receive call state events for targeted users / endpoints using SSE. Use events to determine when to ROD or SOD, Live Monitor, etc.
Call Recording Announcement Server	▪ Custom prompt to be played to external call participants so that their calls may be recorded in Lync / Skype for Business environments. Example: 'Your call may be recorded…' ▪ Custom IVR menu to request recording consent from external call participants and trigger recording when consent is given. ▪ Advantages: ✓ Plays announcement to inbound PSTN call participants ✓ Deploys on Physical or Virtual Servers ✓ Supports N+1 Resiliency
SmartTAP Media Proxy (Skype for Business / Lync)	▪ The software Proxy Service is an RTP Proxy for recorded user / device calls. ▪ A recorded call's media is redirected through the proxy, allowing SmartTAP to capture a copy of the SRTP conversation. ▪ Advantages: ✓ Proxy Server resides in the LAN ✓ Inter and intra region calls stay on the private network ✓ Allows easily recording internal, PSTN and conference calls ✓ Deployable in remote locations to reduce network bandwidth

Feature	Details
User / Device Attributes	A SmartTAP user or device attribute has three purposes: ▪ Additional information can be added to the user account within SmartTAP, i.e., Ext, Tel URI, Address, etc., for informational purposes only. ▪ Designates to SmartTAP what to use to trigger recording, i.e., adds a SIP_URI attribute and provides a value assigned to the user. If the user makes a SIP call, SmartTAP triggers a recording based on the SIP_URI. ▪ Enhances integration by mapping SmartTAP attributes to Active Directory attributes, in order to auto-populate user / device information within SmartTAP.
Automatic Instant Message Recording	• Recording of instant messages for person-to-person chat between two users or group chat between two or more users.
Video Recording	• Recording Profile: Full Time Recording and Save on Demand Video • Playback video from the Calls List and Evaluation menu • Download audio and video call types (together). • Video recording is only supported for Lync 2013 and higher clients
Desktop Recording	• Skype for Business desktop sharing over VBSS (Video Based Screen Sharing) recording is supported
Timeline View	• View call results data for a specific user/device over a time line. Each call type is represented on the timeline by a unique icon.
Automatic Registration of Managed Devices	Managed device other than of type 'Host' register automatically with the application server by sending periodic heartbeats. Devices also update their connection status information whenever the connection state changes information. •

Figure 1-1: Save on Demand (SOD) in SmartTAP Client (Skype for Business)

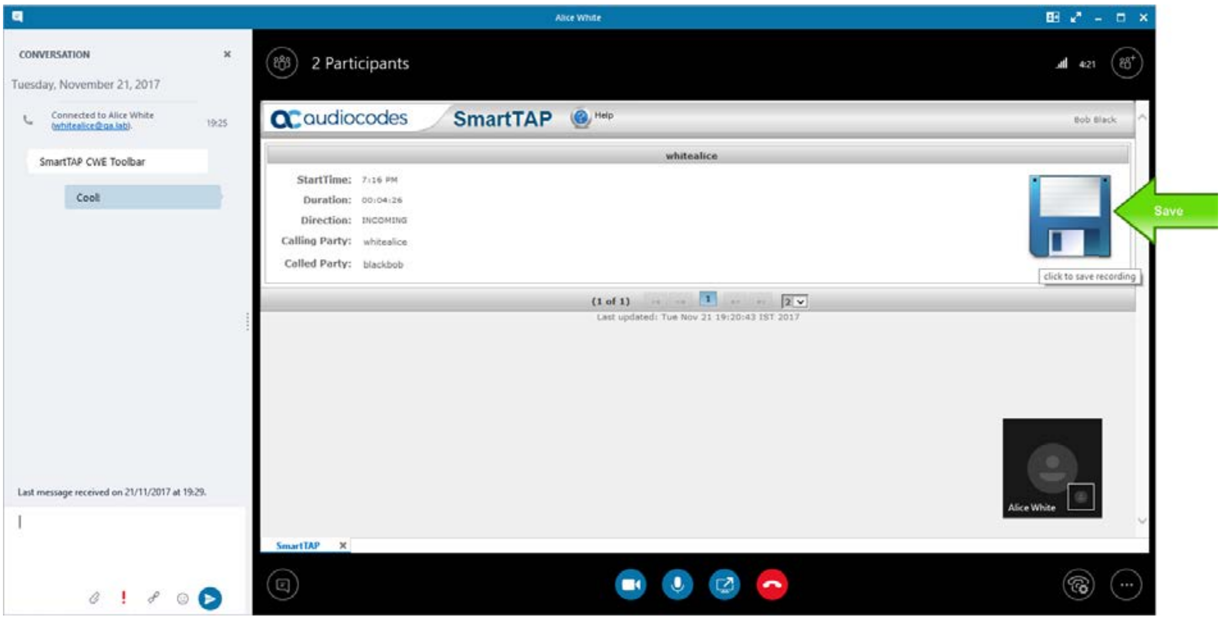
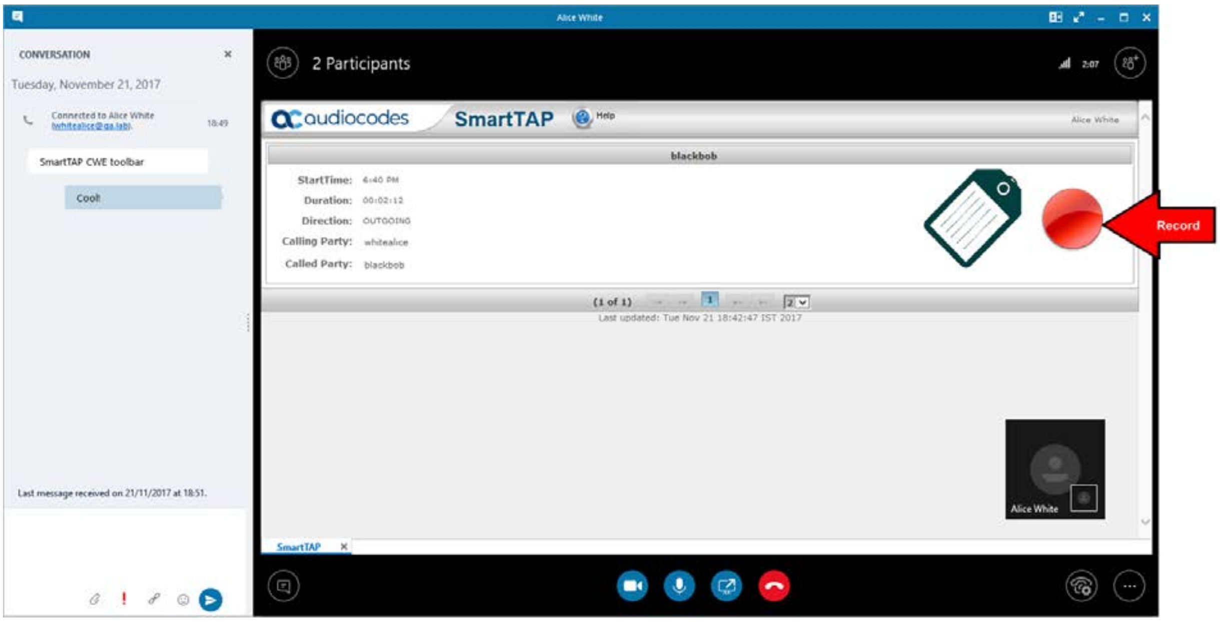


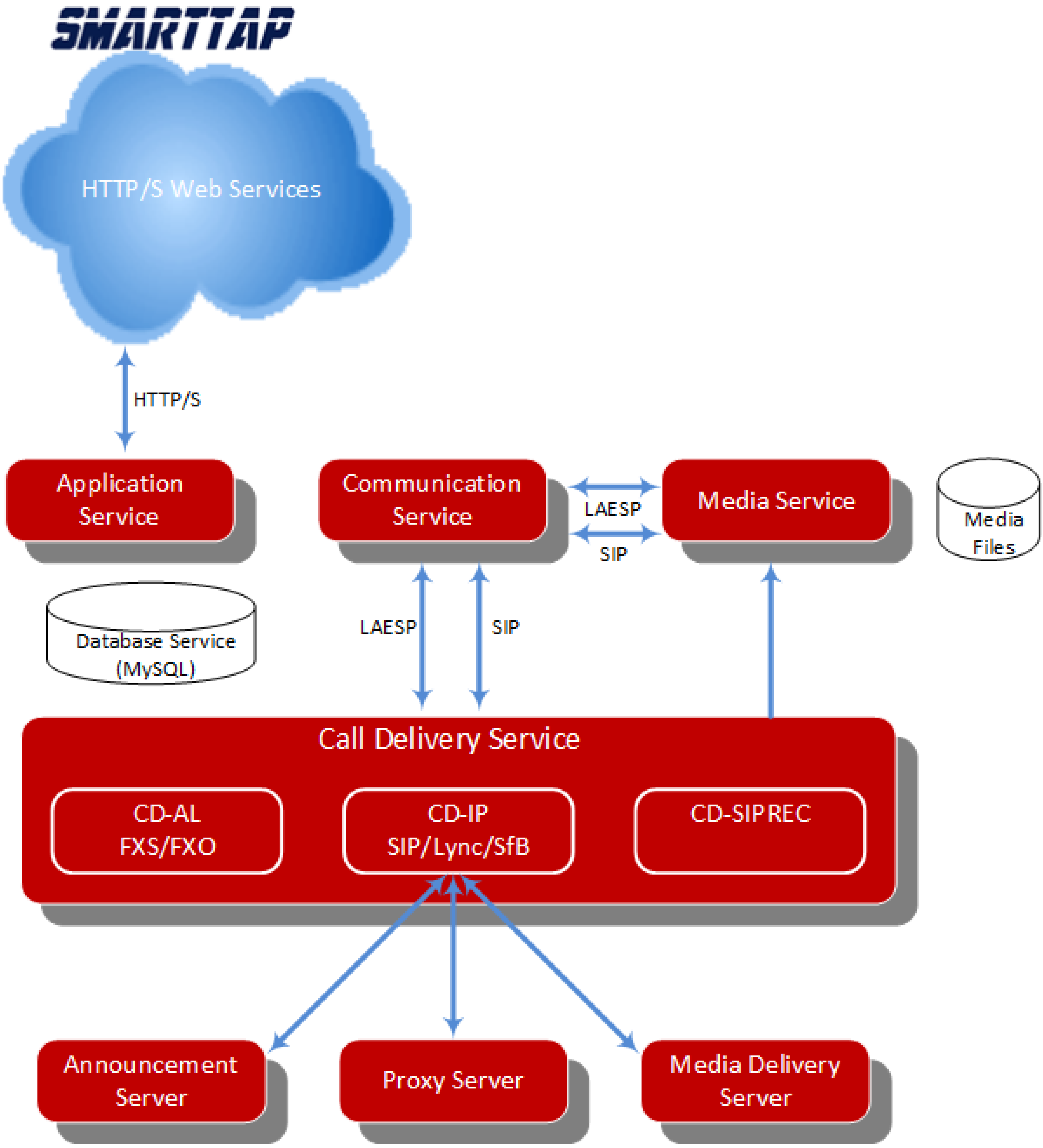
Figure 1-2: Record on Demand (ROD) in SmartTAP Client (Skype for Business)



1.4 Architecture

The figure below illustrates SmartTAP architecture.

Figure 1-3: SmartTAP Architecture



1.5 About this Guide

This guide helps enterprise network administrators obtain full benefit from the SmartTAP Call Recording System. The guide comprises the following sections:

Table 1-2: About this Document

Section	Title	Description
2	Logging in	Shows how to log in to the SmartTAP management GUI.
3	Getting Acquainted with the GUI	Gets the network administrator acquainted with the SmartTAP management GUI.
4	Performing Initial Configuration	Describes the steps to take to perform initial SmartTAP configuration in order to record a call.
5	Testing the Initial Configuration	Shows how to record a call to test the initial configuration.
6	Configuring Advanced Features	Details the user interface, features and procedures.
Appendix	**Title**	**Description**
A	Single Sign-On for SmartTAP	Shows how to simplify the login process for domain users with Single Sign-On (SSO).
B	SmartTAP Lync Toolbar	Shows how to use the SmartTAP Lync toolbar.
C	Media Exporter	Describes the Bulk Media Exporter tool to download Meta Data and Call Records.
0D	API Integration	Describes the API Reference.
E	Recording Health Monitor	Describes the Recording Health Monitor utility

2 Logging in

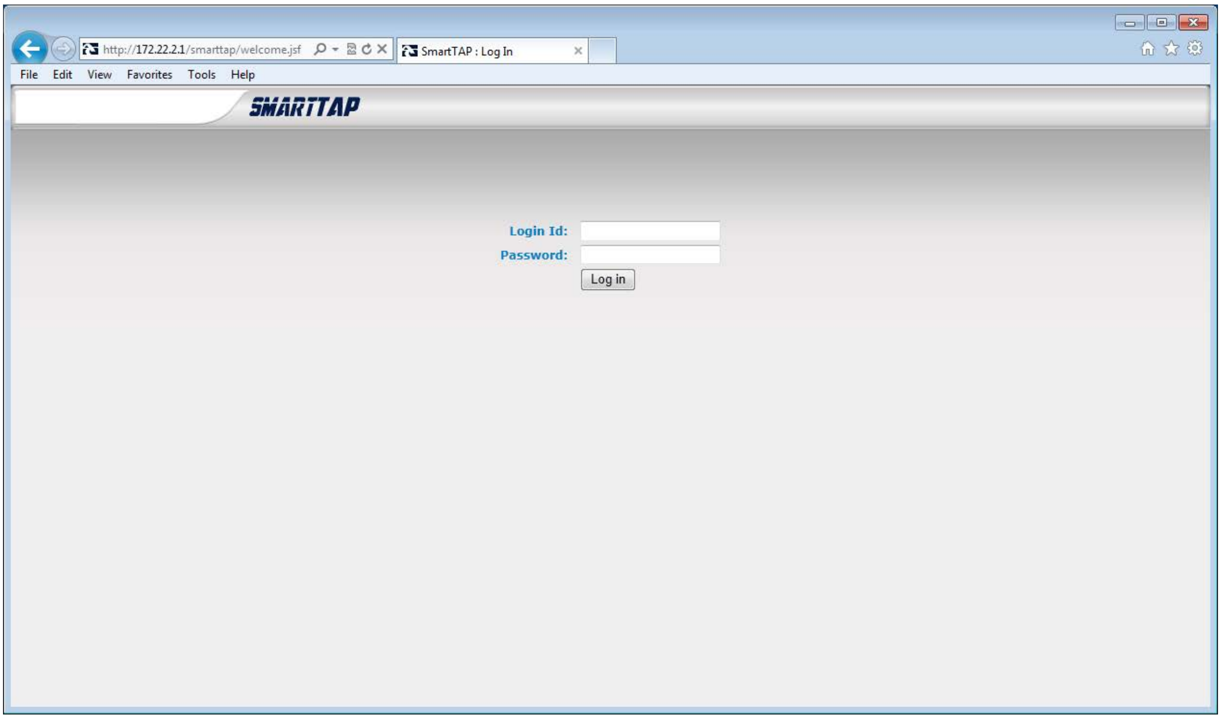
After the SmartTAP software is installed, an Admin user account is created by default. This user account allows the administrator to access the SmartTAP's Web-based management tool for the first time and start initial configuration and administration (see Chapter 4).

This section shows network administrators how to log in for the first time.

➢ **To log in for the first time:**

1. Access the SmartTAP user interface from a browser.
2. Enter the SmartTAP server IP address or hostname; the Login page opens.

Figure 2-1: Login Page



3. Use the table below as a reference.

Table 2-1: Default Admin Credentials

Field	Value
Login ID	admin
Password	admin

4. Click the **Log in** button.

This page is intentionally left blank.

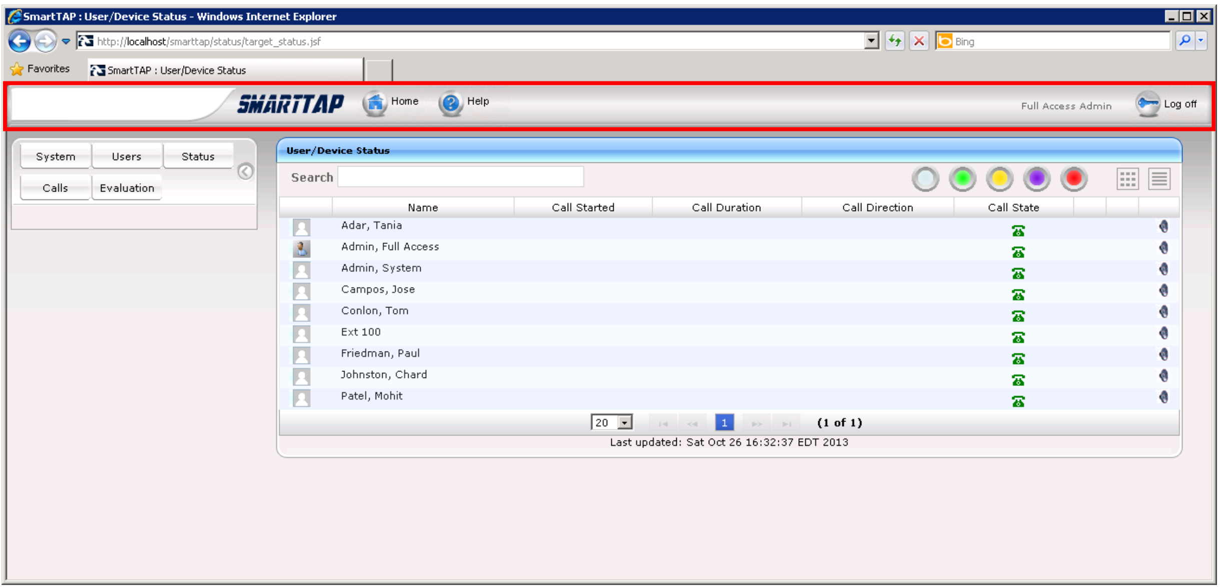
3 Getting Acquainted with the GUI

This section introduces the SmartTAP management GUI.

Figure 3-1 shows the main screen. The following areas are identical across all GUI screens:

- Upper banner (see the figure below)
- Navigation (see the next page)
- Results display & data entry area (see the next page)
- Execution results area (in the case of some commands) (see the next page)

Figure 3-1: SmartTAP Main Screen – Upper Banner

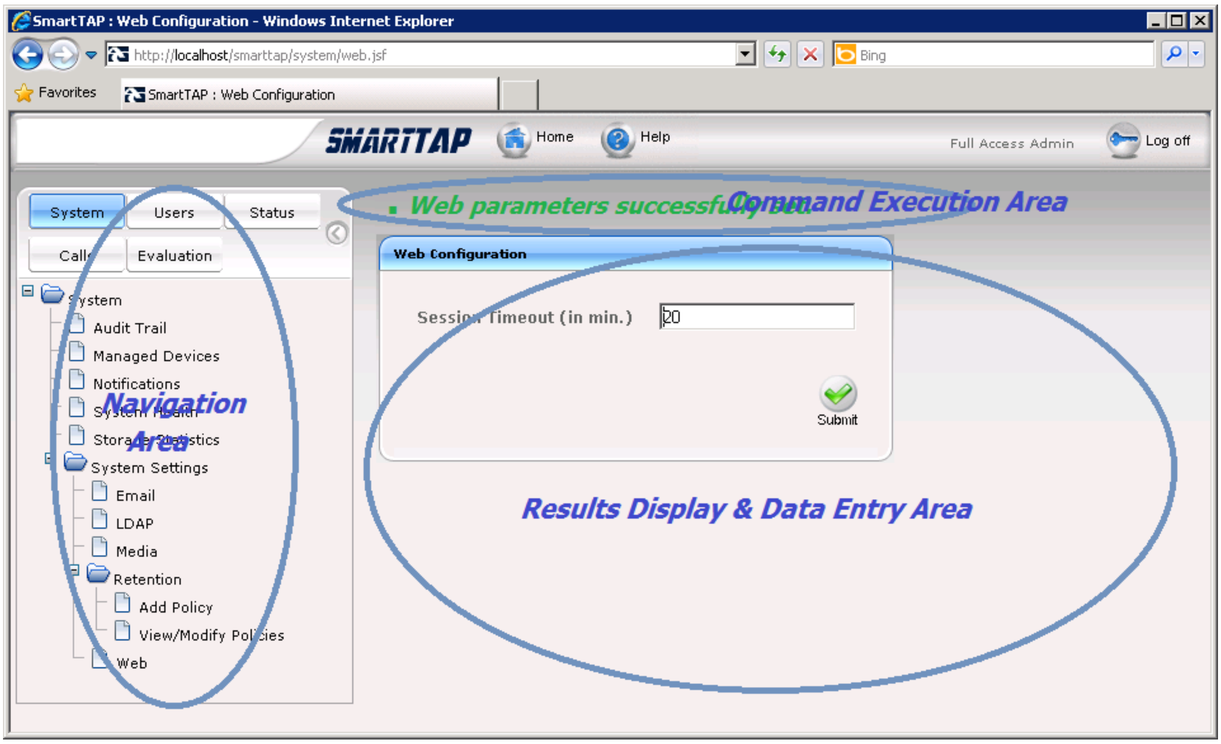


The table below describes the active buttons on the upper banner.

Table 3-1: SmartTAP Main Screen – Active Buttons on the Upper Banner

Button	Icon	Description
Home		Go to the Home Page (default start page)
Help		Displays help for the currently displayed content
Log off		Log off user (identified to the left of this button)

Figure 3-2: SmartTAP Main Screen



The figure above shows the following three areas below the upper banner:

- Navigation area, allowing users to perform queries, configuration, and all the other features available on the platform.
- Results display and data entry area, showing displays associated with the items selected in the Navigation area.
- Command execution results and data entry display area, displayed when an executed command results in fail/success:
  - **Green** font = successful execution
  - **Red** font = failed execution, with the reason for the failure

3.1 Determining User/Device Status

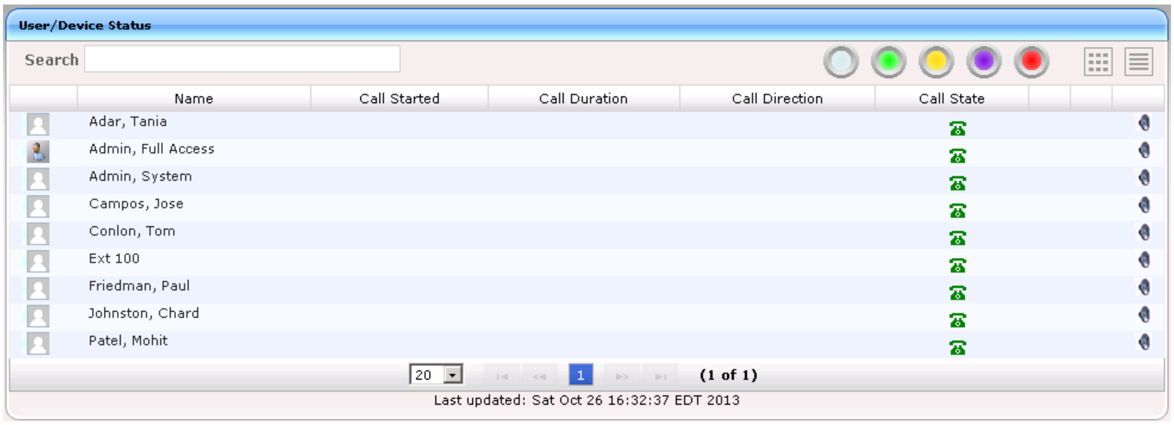
The User/Device Status screen is accessible by clicking the **Home** button on the upper banner, or by selecting **Status** tab > **User Call Status**. The screen features two views:

- Grid
- List

Both of the above options offer the same functionality, therefore either can be used..

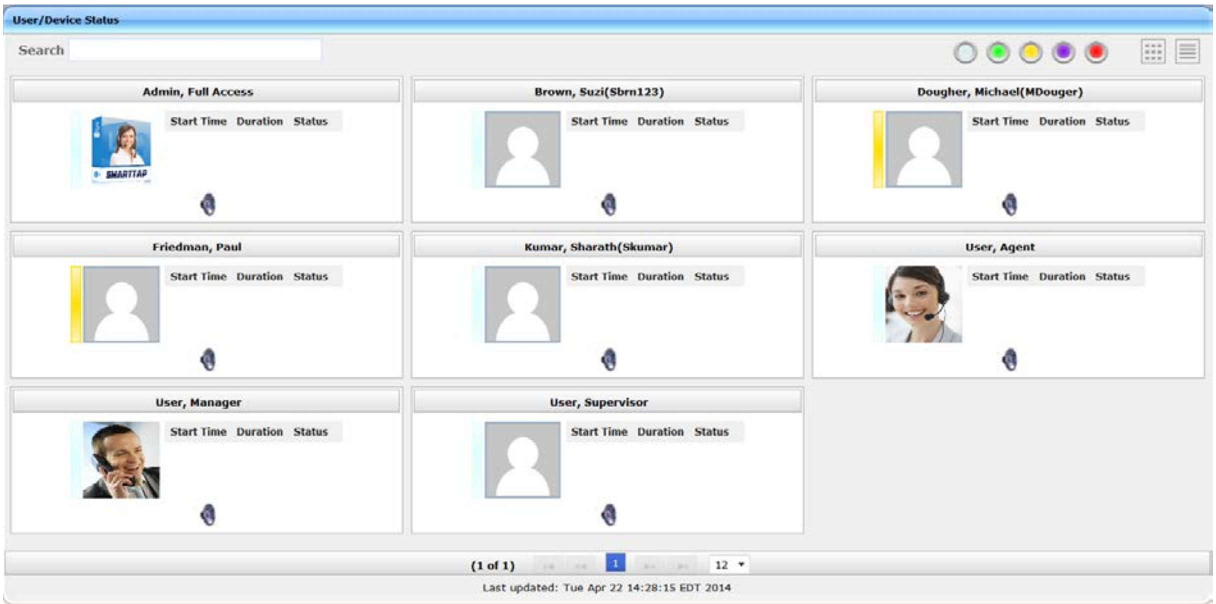
The figure below shows the List View

Figure 3-3: List View



The figure below shows the Grid View

Figure 3-4: Grid View

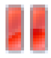
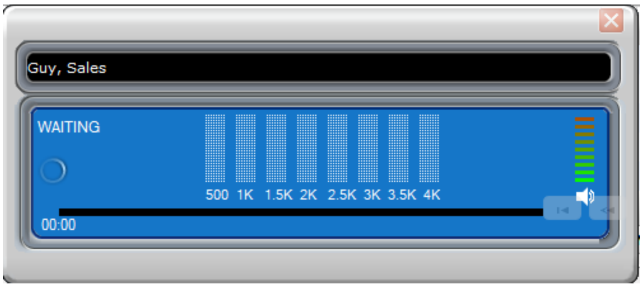


The screen provides near real-time information on the targeted users and their recording status.

The table below describes the Status screen features.

Table 3-2: Status Features

Field	Description		
Name	Sorted ascending/descending by clicking header up/down arrows. Name field entry displays only entries with matching pattern.		
Call Started	The time the call started. Sortable by clicking the up/down arrows.		
Call Duration	The duration of the call. Sortable by clicking the up/down arrows.		
Call Direction	INBOUND or OUTBOUND. Sortable by clicking the up/down arrows. Call Direction dropdown displays only matching entries.		
User / Device Status	Not Filtered	Filtered	Status Filters 'Not Filtered' includes all users/devices in the displayed results. 'Filtered' hides all users/devices from the displayed results.
			Status Unknown: the targeted user has not made a call since the Application Server was started up.
			Status Inactive: the targeted user has not made a call for more than five minutes.
			Status Idle: the targeted user has made a call within the last five minutes.
			Status Active: the targeted user is on a call but recording has not been initiated.
			Status Record: the targeted user is on a call and recording has been initiated.
Call Status		INACTIVE (user is not on a call)	
		RINGING	
		ACTIVE (the call is being recorded)	
		ACTIVE (the call is not being recorded)	
Call Info		Click the icon to launch the Call Detail screen in order to view additional call data.  	
Call Notes		Add a tag - live call or post call. Tags are defined by the system administrator and can be applied during a call or post call.	

<table>
<tr><th>Field</th><th colspan="3">Description</th></tr>
<tr><td rowspan="2">Pause / Resume Recording</td><td></td><td colspan="2">Select to pause the recording (for PCI compliance).</td></tr>
<tr><td></td><td colspan="2">Select to Resume the recording (for PCI compliance).</td></tr>
<tr><td rowspan="2">ROD / SOD</td><td></td><td>ROD (Record on Demand)</td><td>Click to start recording from the current point in the call. The audio file will contain audio from the trigger point on.</td></tr>
<tr><td></td><td>SOD (Save on Demand)</td><td>Click to save the recording of the complete call.</td></tr>
<tr><td>Live Monitor</td><td></td><td colspan="2">Users with 'Live Monitoring' privilege can listen to active calls by clicking the Live Monitor microphone button. The following popup player launches:

</td></tr>
<tr><td>Page Navigation buttons</td><td colspan="3">These are shortcuts to the beginning/end, previous page/next page of the displayed entries. The dropdown allows changing the number of entries per page.</td></tr>
</table>

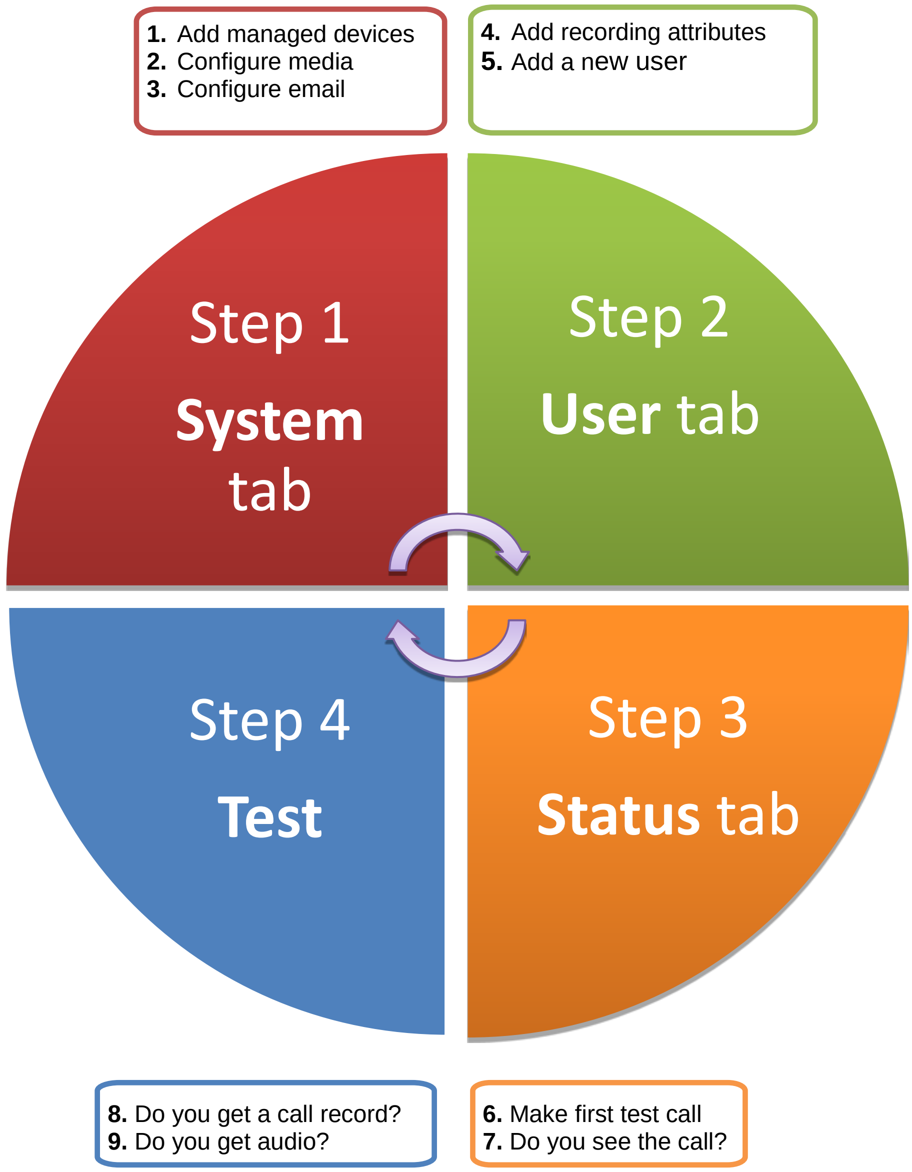
This page is intentionally left blank.

4 Performing Initial Configuration

The figure below shows the steps to take to perform initial SmartTAP configuration (Step 1-Step 2) in order to record a call. Detailed instructions follow below it.

It's assumed SmartTAP software components were installed on the servers necessary for your environment, and were configured based on the *SmartTAP Installation Guide*.

Figure 4-1: Performing Initial Setup



➢ **To perform initial setup:**

1. Log in for the first time (see Chapter 2 for more information)
2. Configure media (see Section 6.10.3 for more information).
3. Configure email (see Section 6.10.2 for more information).
4. Add a user attribute for recording purposes (see page 110 for details).
   a. Add a user (see under Section 6.11.7 for more information).
   b. Make sure the new user is assigned a recording profile (see under Section 6.11.4 for more information).
   c. Make sure the user's recording attribute field is populated (see under Section 6.11.4 for more information).

5 Testing the Initial Configuration

Testing the initial configuration and then troubleshooting it if necessary can be performed (step 3 and step 4 respectively, as shown in Figure 4-1). The objective is to validate the configuration and the recording functionality.

After making sure recording is functioning correctly, continue to Section 6 to set up advanced features like LDAP, Single Sign-On, etc.

➢ **To test the initial configuration:**

1. In the SmartTAP GUI, navigate to the Status page.
2. Make your first test call.
   a. Do you see the call trigger recording?
   b. Do you get a call record?
   c. Does the record contain audio?

5.1 Making Sure a Recording is in Progress

This section shows how to make sure that a recording is in progress.

➢ **To make sure that a recording is in progress:**

1. Open the User/Device Status screen:
   - Click the **Home** button on the upper banner -or-
   - Click the **Status** tab > **User Call Status**

■ The icon indicates that a recording is in progress.

5.1.1 Listening to a Recording and View a Video

This section shows how to listen to a recording and to view call video.

➢ **To listen to a recording:**

1. Click the **Calls** tab; the Search Calls screen opens.
2. In the Search Navigation screen (left side), enter the date range and select the type of Users and Devices.
   - Select either the **Users/Devices** or the **Groups** button. Selecting the **Users/Devices** option changes the display below to show a list of Users/Devices.
   - Selecting the **Groups** option changes the display below to show a list of Groups and Sub Groups (if the 'Search Sub Groups' option is selected).
3. Select one of more User/Devices or Groups by highlighting them in the list (see the notes on the Search Calls Navigation screen's field descriptions for how to select more than one User/Device or Group).
4. Click Search to start the search for calls matching the search criteria; the results are displayed in the Search Calls Results screen to the right.
5. Select the recording you wish to playback c.
6. If the call is a video call type, select the 'Display Video' check box to display the call video as well.
7. Click the button to start listening to the call or to watch the video.

This page is intentionally left blank.

6 Configuring Advanced Features

After performing initial setup and then testing it, n configure the advanced SmartTAP features described in this section.

6.1 Viewing/Searching an Audit Trail

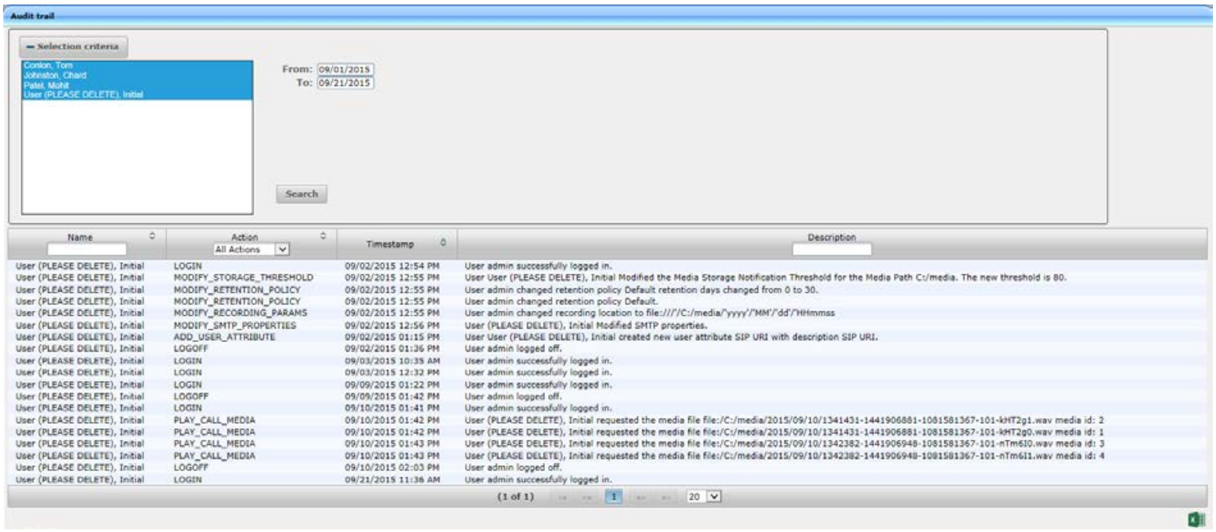
The Audit Trail feature allows the administrator to search the history of all user activity on SmartTAP. The Audit Trail is searchable but cannot be edited or deleted. You can view / search the user changes made to the SmartTAP database.

➢ **To view / search user activities:**

1. Open the Audit Trail screen (**System** tab > **System** folder > **Audit Trail**).

> **Note:** The **System** tab is only accessible to administrators assigned the **Configure System** option in their security profile.

Figure 6-1: Audit Trail



2. Use the table below as reference.

Table 6-1: Audit Trail

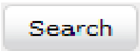
Field	Description
− Selection criteria	Click to hide the Search area
+ Selection criteria	Click to show the Search area
<list of users>	Select the user to view by clicking the user name; hold <ctrl> to select multiple users; hold <shift> and click the top user and the bottom user to select all users within a range.
From:	Select the date *from which* to search.
To:	Select the date *to which* to search.
Search	Click to perform the search and display the results.

Field	Description
Name	Sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.
Action	Sorted ascending/descending by clicking header up/down arrows. Default is 'All Actions'. Field entry displays only entries with matching drop down menu.
Timestamp	Time of day when entry was created
Description	If defined, the field entry displays only matching entries.
	Click **Excel** icon to export Audit Trail.
Navigation buttons under the search display:  Buttons are shortcuts to the beginning/end, previous/next page of the displayed entries. The dropdown allows changing the number of entries per page.	

6.1.1 Exporting an Audit Trail

You can export the audit trail to an Excel file for accountability purposes.

➢ **To export the audit trail:**

1. Open the Audit Trail screen (**System** tab > **System Folder** > **Audit Trail**).
2. Select the User or Users to view and date range.
3. Click  to see the results.
4. Click the Excel  icon.

5. Click Open / Save to manage the Excel file.
6. Once opened, the following tabs can be seen:
   - Tab #1 **Search Criteria Details**
   - Tab #2 **Audit Trail Data**

6.2 Managing Licenses

This section describes how to manage the SmartTAP licenses. This interface displays data on the purchased and loaded license items:

- Targeted user licenses
- Concurrent recording licenses

6.2.1 Targeted User Licenses

The targeted user licenses enable SmartTAP users to be assigned to recording profiles for different types of communication recordings in an enterprise. The following Targeted recording licenses can be configured:

- **Audio & IM Targets:** this license sets the number of users that can be assigned to a Recording Profile for recording Audio and Instant Messages. Audio Concurrent licenses (described below) are required to record these users calls.
- **IM Targets:** this license sets the number of users that can be assigned to a Recording Profile for recording Instant Messages only. Other types of user communications i.e. audio or video recordings are not available under this license.
- **Video & Audio & IM Targets**: this license sets the number of users that can be assigned to a Recording Profile for recording Audio and Video and Instant Messages. Video & Audio Concurrent Recording licenses (described below) are required to record these users calls.

> **Note:**
>
> - Desktop Sharing recording does not require a target user license. Only the concurrent recording license can be enabled for users with Audio& IM targets or Video & Audio & IM targets.
> - Check with your AudioCodes representative for which types of content can be recorded.

6.2.2 Concurrent Recording Licenses

Concurrent recording licenses determine the maximum number of calls that can be simultaneously recorded. Ideally the concurrent calls license should be equal the maximum number of simultaneous calls that can be made by the targeted users.

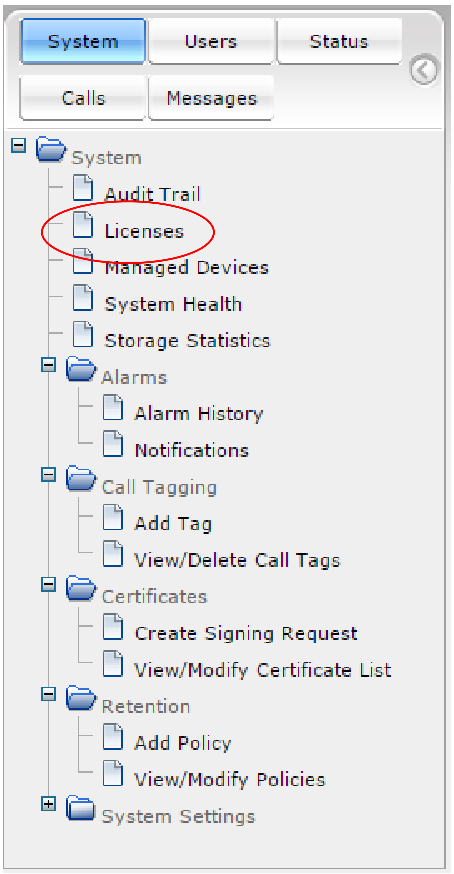
The following Concurrent recording licenses can be configured:

- **Audio Concurrent Recordings:** this license determines the maximum number of concurrent Audio recordings of users that are assigned to Audio (Video disabled) enabled recording profile.
- **Video & Audio Concurrent Recordings:** this license determine the maximum number of concurrent Video and Audio recordings of the users that are assigned to Audio and Video enabled recording profile.
- **Desktop Sharing Concurrent Recordings:** this license determines the maximum number of concurrent Desktop Sharing recordings of users that are assigned to an audio orvideo, recording profile...

➢ **To view Managed Licenses:**

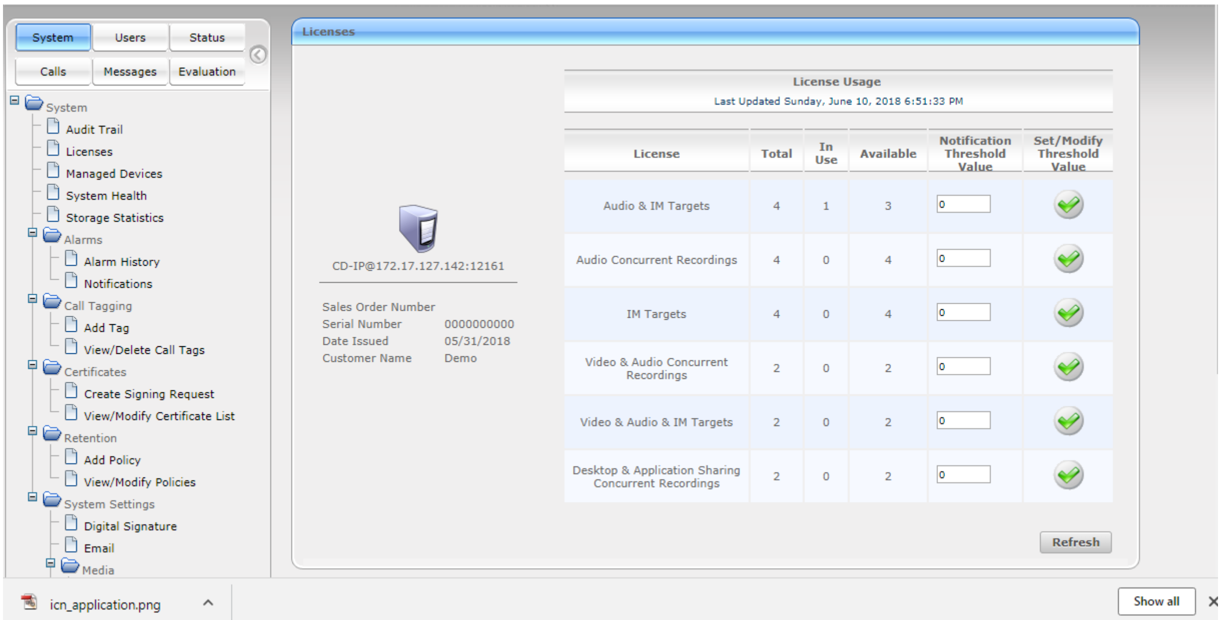
1. Open the Licenses screen (**System** tab > **System Folder** > **Licenses**).

Figure 6-2: License Menu



A table of available licenses is displayed.

Figure 6-3: License Usage



6.2.3 License Configuration Parameters

- **Total:** The total number of purchased licenses
- **In Use:** The number of licenses that are currently utilized reflects the number of recording enabled users or the number of user calls recorded at the time of the page refresh.
- **Available:** the number of licenses available to enable users for recording or to record concurrently.
- **The Notification Threshold Value:** this value is measured in terms of the number of licenses; zero implies that no notifications are sent. For example, in the figure above, the Notification Threshold Value **3** is configured for the “Audio & IM Targets” item, therefore when 3 or more licenses are used for this item, the alarm "Resource Threshold Exceeded" is generated. When the license usage falls below the threshold, the alarm "Resource Threshold Cleared" is raised. See also Section 6.5.
- **Set/Modify Threshold Value:** Set or modify the Threshold value by selecting the adjacent button for each license item.

  In addition, general license information is displayed on the left-hand side of the screen including the Sales Order Number, Serial Number, Date Issued and Customer Name.

6.3 Viewing Managed Devices

SmartTAP architecture comprises several services which together perform all tasks and provide all functionalities for the recorder.

Since any of the services required for an installation may not be in a single server, the initial administrator (admin) must configure the services for SmartTAP to record calls.

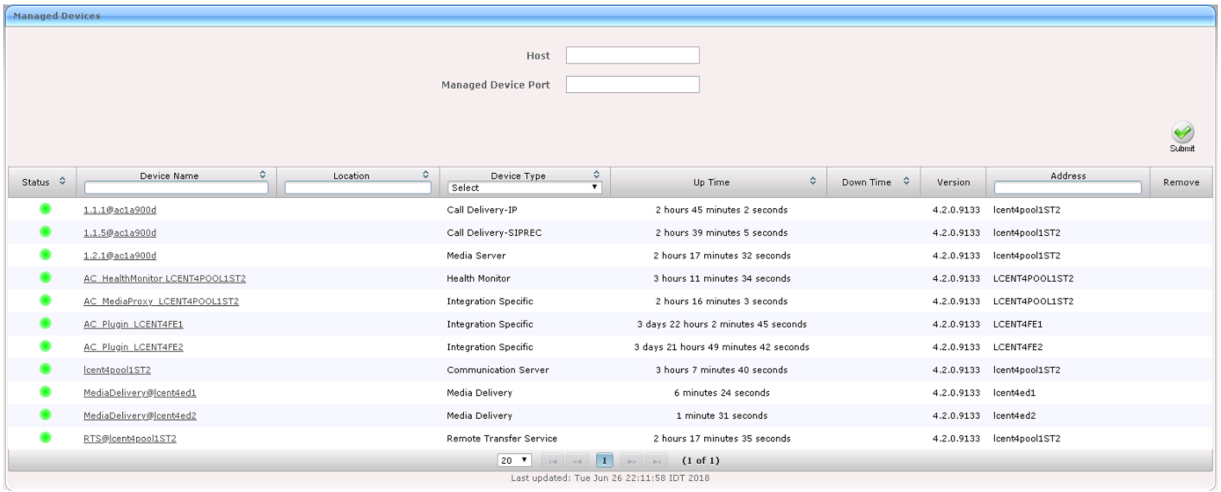
A managed device other than of type 'Host' will register automatically with the application server. Such devices update their status by sending periodic heartbeats to the application server. Devices also update their connection status information whenever the connection state changes. A device of type 'Host' needs to be manually added to the application server in the Managed Devices screen. The Application server will periodically poll 'Host' type device to retrieve the device status information.

> **Note:**. In a correctly setup deployment, all device types are added automatically, except for devices of type “Host”. See Section 6.4 for the procedure to add Host devices.

➢ **To view managed devices:**

- Open the Managed Devices screen (**System** tab > **System Folder** > **Managed Devices**):

Figure 6-4: Managed Devices



- Use the table below as reference.

Table 6-2: Managed Devices Field Descriptions

Field	Description	
Host	Host Name or IP Address of the managed device to add. By default, the type of this device is set as 'Host'.	
Port	SNMP UDP Listening Port of the managed device to add.	
Status	Indicates the status of the managed device.	
		Device status is UP: the device has registered and is sending heartbeats periodically at regular 30 second intervals.

Field	Description	
		Device status is UNKNOWN: the device has registered but has not yet send any heartbeat message.
		Device Status is SETTLING: the device is in DOWN state and has started sending heartbeats again. If the device continues to send heartbeats without any timeout or failure for the settling period (two minutes by default), the status will change to green.
Device Name	Display Name of the Device. Sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries. **Note**: Clicking the **Device Name** link opens the control panel page for this device.	
Device Location	Devices location information. Sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.	
Device Type	Type of the device provided during registration. A manually added device has type 'Host'. In SmartTAP, valid device types are as follows: Unknown; Host; Call Delivery-IP; Call Delivery-SIPREC; Media Server; Communication Server; Integration Specific; Health Monitor; Remote Transfer Service and Media Delivery Sorted ascending/descending by clicking header up/down arrows. The dropdown only displays matching entries. 'Unknown' devices are devices unreachable by the Application Server's Web service.	
Up Time	Time elapsed since the device status became UP.	
Down Time	Time elapsed since the device status became DOWN.	
Version	Version of the registered device.	
Address	IP address or Host name of the registered device.	
Remove ( )	Delete button to remove managed device information from the system. An auto-registered device can only be deleted if its state is either 'DOWN' or 'UNKNOWN'	
Submit	Submit button to add a managed device of type 'Host' to the system.	
Filtering	Typing in a column input field or selecting a value from a drop down in column headings will filter the table entries by the value typed or the option selected.	

6.4 Adding a Device Manually to the Application Server

The Application Server's Web service manages all devices (software elements). It must be configured with those software elements performing specialized tasks within the SmartTAP environment. There should be at least one:

- Call Delivery Server (required to record)
- Communication Server (required to record)
- Media Server (required to record)
- Host (required to monitor system health)

When the administrator adds a new software element on the local or remote physical/virtual server, the Application Server attempts to establish a connection with the new element. If successful, the Device Type in the main screen changes from 'Unknown' to the device type just added. Click the device name to navigate to the Control Panel for that device.

Note: As mentioned in Section 6.3, in a correctly setup deployment only the Host server needs to be added manually to the Application Server.

➢ To add a device manually:

1. Open the 'Managed Devices' screen.
2. Enter the Host IP address of the new device.
3. Enter the published Managed Device Port of the new device (see the table below).
4. Click **Submit**.

Note: In a standalone SmartTAP recorder, all managed devices reside in the same server and are associated with the local host or IP address.

Table 6-3: Managed Devices

Hostname of Device	UDP Port	Description
Host	161	Server Platform Host MIB

➢ To make sure the device was added to the server:

1. After adding a device, the new device is displayed in the list of devices.
2. Once the new device is discovered, 'Device Type' changes from 'Unknown' to the correct device type added.

6.5 Alarms

This section describes the Alarms History and Alarm Notification screens.

6.5.1 Alarm History

1. Open the Alarm History screen (**System** tab > **Alarms** Folder > **Alarm History**).

Figure 6-5: Alarm History

Communication Up	Communication between processes has been restored.	lcent4fe1.lcent4.local	19 May 2017 12:37:55	Connection to server: 'CallDelivery', Address 172.26.144.23, established successfully.
Communication Up	Communication between processes has been restored.	lcent4fe2.lcent4.local	19 May 2017 12:37:55	Connection to server: 'CallDelivery', Address 172.26.144.23, established successfully.
Communication Down	Communication between processes has been lost.	lcent4fe1.lcent4.local	19 May 2017 12:37:04	Lost connection to server: 'CallDelivery', Address 172.26.144.23
Communication Down	Communication between processes has been lost.	lcent4fe2.lcent4.local	19 May 2017 12:37:03	Lost connection to server: 'CallDelivery', Address 172.26.144.23

Filtering of the the display can be done according to date range and sort records according to name, description, source, summary and details.

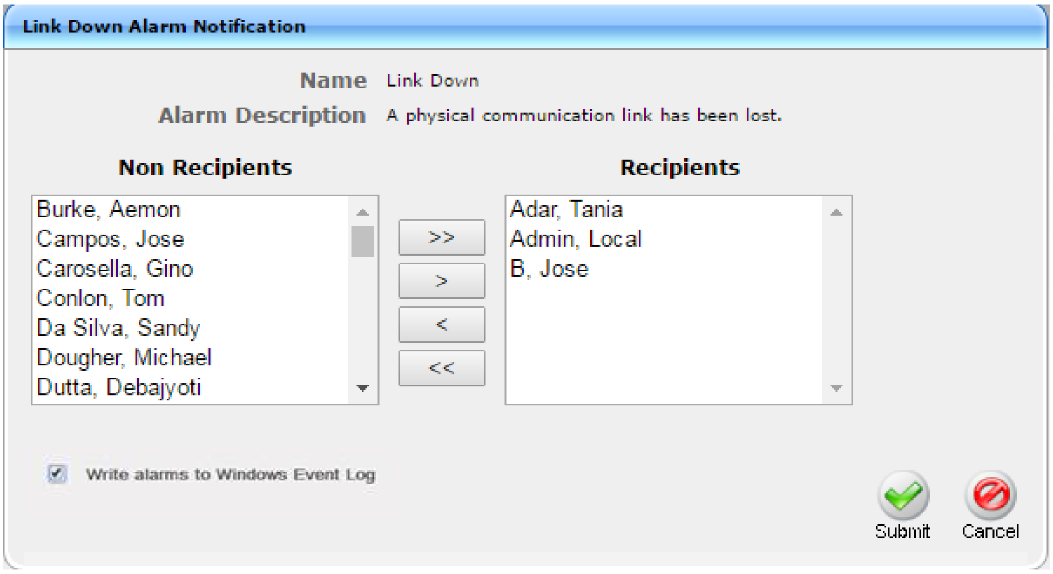
6.5.2 Alarm Notifications

SmartTAP features the ability to automatically send email alarm notifications to selected network administrators. The notification sent is based on the type of alarm generated by the system.

➢ **To configure alarm notifications:**

1. Open the View/Modify Alarm Notifications screen (**System** tab > **System Folder** > **Notifications**).
2. Click **Modify** ( ) on the Alarm that you wish to modify.
3. Move the users to receive Email Notifications from the 'Non Recipients' side to the 'Recipients'.
4. Clear the ‘Write alarms to Windows Event Log’ option if you do not wish to write alarm notifications to the Windows Event Log. This option enables you to write SmartTAP alarms to the Windows Event Log. By default, this feature is enabled for all alarms/notifications. (For more information, see Section 6.5.46.5.4).
5. Use the assignment keys to assign recipients of the alarm notifications:
   - Click the >> or << keys to move all users between the Non-Recipients and the Recipients list.
   - Select users and then use the < or > keys to move users between the Non Recipients and Recipients lists (use the CTRL key to select multiple users.
6. Click Submit to submit changes.

Figure 6-6: Alarm Notification



7. Use the table below as reference to the Viewing/Modifying Alarm Notifications screen.

Table 6-4: Viewing/Modifying the Alarm Notifications Screen

Field	Description
Alarm	Alarm name. Sorted ascending/descending by clicking header up/down arrows. If defined, field entry displays only matching entries.
Description	Alarm description. Sorted ascending/descending by clicking header up/down arrows. If defined, field entry displays only matching entries.
Modify ( )	Click to modify the list of users receiving this alarm notification.

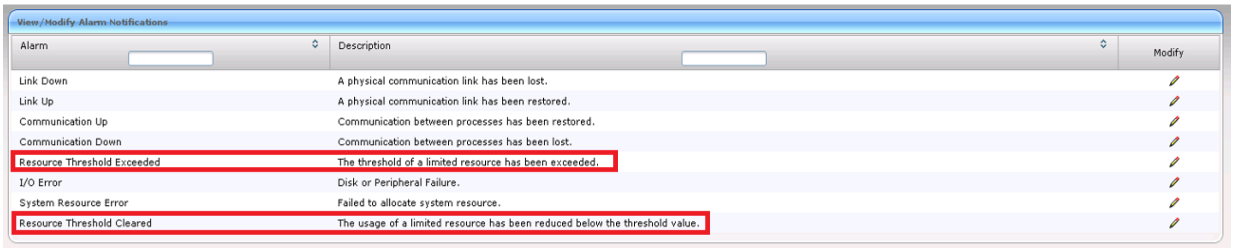
Table 6-5: List of Alarms and Possible Causes with Recommended Remedial Action

Alarm	Explanation	Remedial Action
Link Up / Down	Caused by loss of signaling with network or passive tap connection	Check the host PC network connections. Analog or Digital Station Integration – Make sure the cable is properly connected to the device.
Communication UP / Down	Communication between SmartTAP software elements has been lost	▪ Run system_profile.exe (..\AUDIOCODES\Tools) ▪ Contact AudioCodes Support with the notification received. ✓ If the notification is a failure from the Application Server polling the managed devices, it will indicate the address and port of the managed device it was trying to communicate with. ✓ If it is from a trap from another device, the trap OID will indicate the specific failure between which devices.
Resource Threshold Exceeded	The peak number of concurrent calls has exceeded the number of available licenses.	SmartTAP has insufficient purchased recording licenses to record the peak number of concurrent calls. You can also activate a warning notification alarm when a configured threshold value for a specific license parameter is reached (see Section 6.2).

Alarm	Explanation	Remedial Action
	The media storage location threshold has been reached.	▪ Add additional storage capacity to the file server, for more media files (recordings). The file server is exterior to SmartTAP. ▪ Check the resource threshold setting. It's possible that sufficient storage still remains and that the threshold just needs to be adjusted.
I/O Error	Sent if the Media Server fails to write media to disk.	▪ Check the Media Server and Media Server Transfer services and logs. Media Server Transfer is the bulk transfer of recordings from a local (branch) location to a centralized location. ▪ Make sure the appropriate permissions were provided to SmartTAP. ▪ Check if the permissions changed. ▪ Check the Media storage drive for possible disk failures.
System Resource Error	Occurs when the Media Server fails to bind to a port.	▪ Run system_profile.exe (…\AUDIOCODES\Tools) and contact AudioCodes Support. ▪ Make sure UDP port range 40000-45000 is available.

The figure below shows alarm notifications for the 'Resource Threshold Exceeded' notification; sent when the system utilization has exceeded the maximum number of available licenses. The 'Resource Threshold Cleared' notification is sent when the system license utilization falls back within the threshold limit.

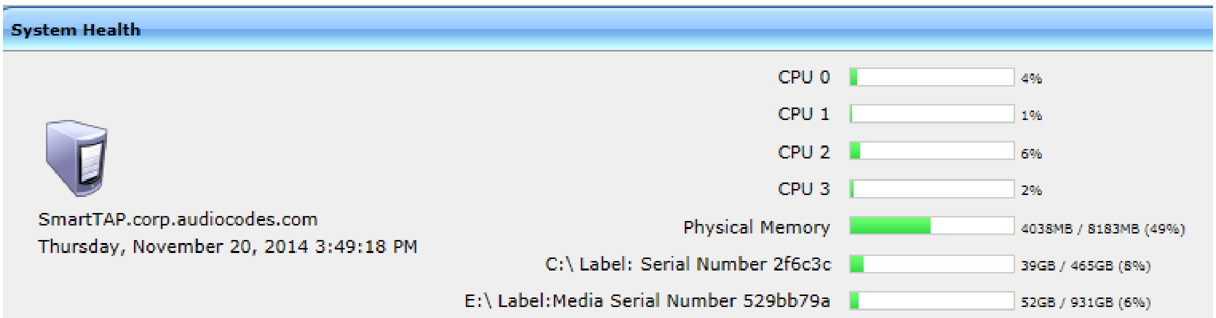
Figure 6-7: View/Modify Alarm Notifications



6.5.3 Determining System Health

The health of the SmartTAP server is based on the host platform MIB. The System Health screen shown in the figure below displays the current health statistics of the server.

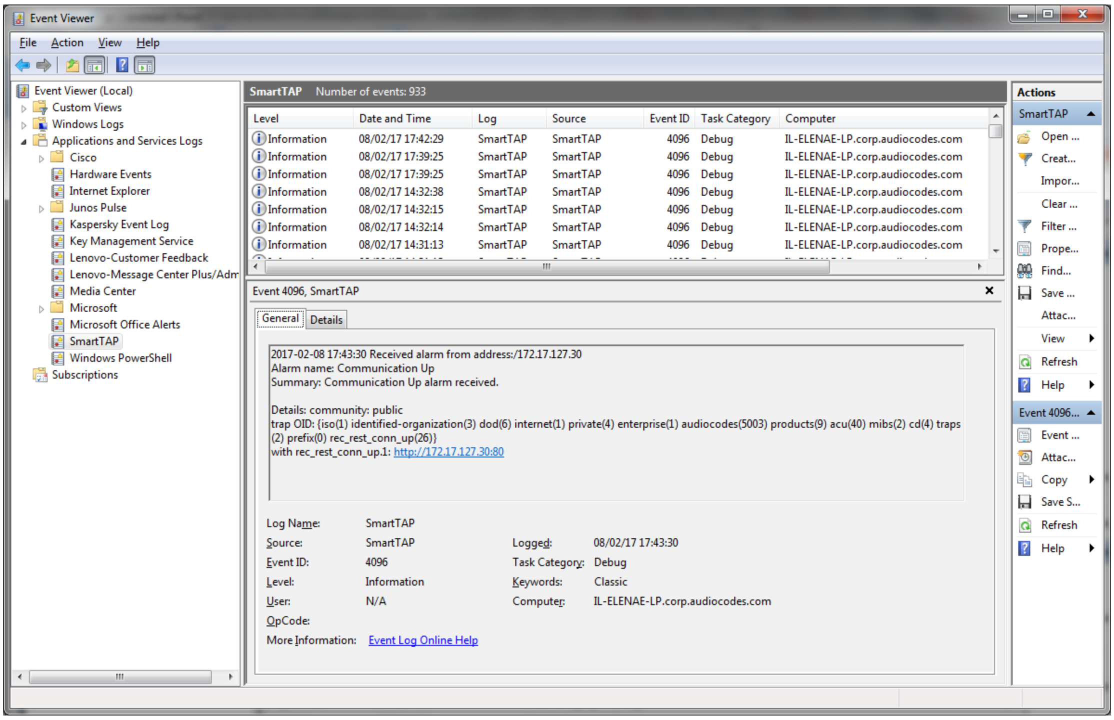
Figure 6-8: System Health



6.5.4 Windows Event Log

When the Alarm Notification is written to the Windows Event Log, the Application Server creates a log file “SmartTAP” under “Applications and Services Logs” category in the Windows Event Log. This log includes all alarms that were logged while running according to logging configuration. The source attribute of these alarms is “SmartTAP” and Event ID=4096.

Figure 6-9: Event Viewer



6.5.4.1 SCOM Integration

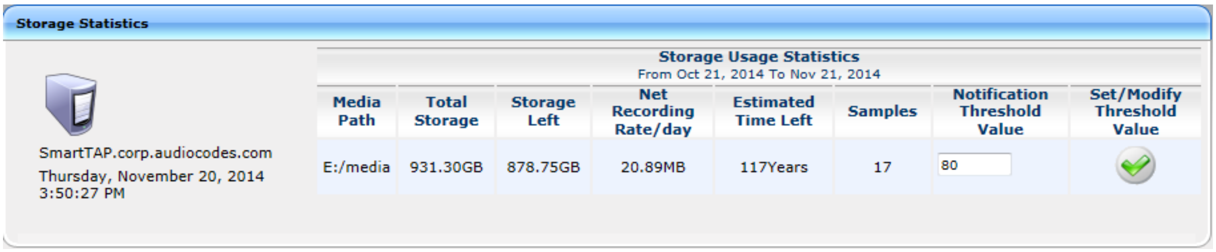
The SmartTAP platform can be configured to generate the event monitor or send an alert based on a Windows event to the Microsoft SCOM platform. In case of SmartTAP, the monitored events source should be configured to “SmartTAP” with Event ID 4096.

For more information, see the following link: [Monitor Event Log]

6.6 Determining Storage Statistics

The SmartTAP server estimates the number of days remaining until the recordings storage device reaches its maximum. The Storage Usage Statistics screen shows parameters used for this calculation. The calculation factors in not only size and rate of new recordings but also size and rate at which older recordings, which exceed the retention value, are deleted. The notification threshold allows the network administrator to set up an automated notification to trigger when the number of days of storage remaining falls below the Notification Threshold Value.

Figure 6-10: Storage Statistics Screen



Use the table below as reference.

Table 6-6: Storage Statistics Fields

Field	Description
Media Path	Location in which the recordings are stored.
Total Storage	The total storage available for the media. **Note**: the drive's total storage is assumed. The storage reflects all media types (audio and video).
Storage Left	The current value of the remaining storage left for media.
Net Recording Rate / day	The net average storage space consumed per day, calculating the net between the recording rate and the deletion (retention) rate.
Estimated Time Left	Estimated time remaining before the Media Path is full.
Samples	Number of days used to calculate the Net Recording Rate.
Notification Threshold Value	Specify the % of space consumed before an alarm is triggered. > % value consumed = send alarm. Default: **0** (never notify).
Submit	Apply changes

➢ **To receive the 'Resource Threshold Exceeded' alarm:**

1. Configure the Notification Threshold value:
   - Access the Storage Usage Statistics (**System** tab > **System Folder** > **Storage Statistics**).
   - In the Storage Statistics screen, change 'Notification Threshold Value' to the number of days, to send notification, before the disk is full.
   - Click Submit to submit changes.
2. Select the users who will receive the automated notification when the threshold is crossed:
   - Access the View/Modify Alarm Notifications (**System** tab > **System Folder** > **Notifications** menu).

- Click **Modify** (✎) on the 'I/O Error' Alarm.
- Move the users to receive Email Notifications for this alarm from the 'Non Recipients' side to the 'Recipients'.
- Click Submit to submit changes.

6.7 Using Call Tagging

Call Tagging can be implemented in two ways: The network administrator can define tags allowing users to enter data manually on their screen during the course of a call, or via a third-party application. Calls can be tagged with relevant information and subsequently used for quick and easy retrieval.

Benefits:

- Categorizes calls by type or outcome, making searches easy (i.e., Malicious, Account ID, etc.). By default, the Notes tag is already defined within the system.
- Saves money by dramatically reducing the time to find individual recorded calls.
- Improves internal processes by using the call tags as searchable data fields for other applications.

Table 6-7: Call Tagging Fields

Field	Description
Tag Name	User-defined meaningful name to be displayed to administrators when selecting a tag from the management interface.
Tag Description	Administrator-defined description of the purpose of the tag..
Input Type	Define the field type for the tag: ▪ **None** (Tag requires no administrator input) ▪ **Text** (the 'Notes' field supports a maximum of 256 characters) ▪ **Boolean** (Select/clear the checkbox: Yes / No or True / False) ▪ **Select_One** (Define a list of options for the administrator to choose from, i.e., Excellent, Very Good, Good, Poor)
Allow Private	Allows an administrator to add the tag as private. Once tagged as private, only the specific administrator account will be able to view the tag.
	Applies changes.
	Cancels changes.

6.7.1 Adding a Call Tag

This section describes how to add a new call tag.

➢ **To add a new Call Tag**

1. Open the Call Tagging screen (**System** tab > **System** folder > **Call Tagging** > **Add Tag**).

Figure 6-11: Add Call Tag Screen

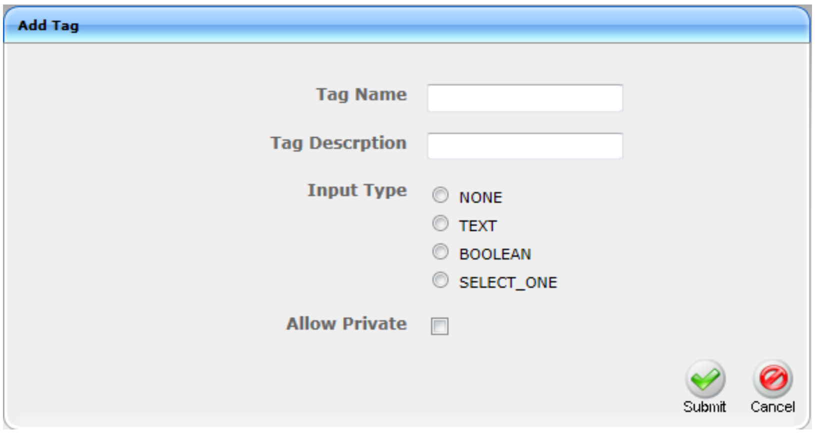


Table 6-8: Call Tagging Fields

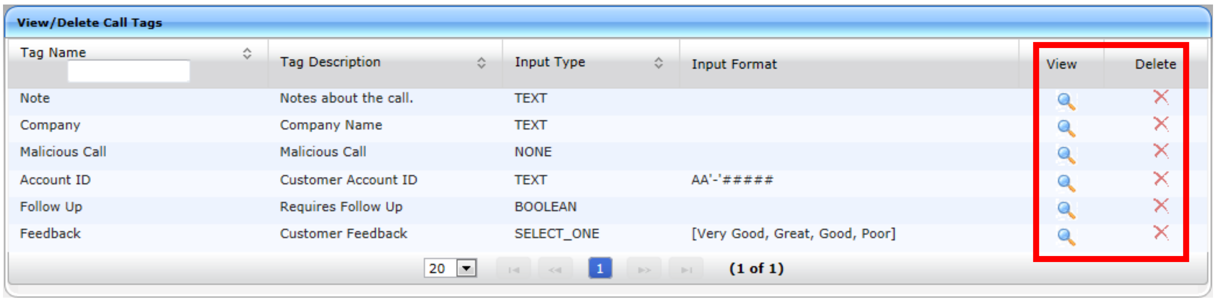
Field	Description
Tag Name	Administrator-defined Tag name. Enter the tag name to the filter list.
Tag Description	Administrator-defined description of the purpose of the tag, to expedite management efficiency. Easily sorts column A-Z or Z-A.
Input Type	Tag Type: ▪ **None** (Tag requires no user input) ▪ **Text** (the 'Notes' field supports a maximum of 256 characters) ▪ **Boolean** (Select/clear the checkbox: Yes / No or True / False) ▪ **Select_One** (Define a list of options for the user to choose from, i.e., Excellent, Very Good, Good, Poor) Mask (Use with Text Tag Types): May be defined for **Text** input type. If defined, the tag value must conform to the MASK. If undefined, the tag value can be any combination of printable characters: ***** (Any printable character) # (Must be a digit: 0-9) **A** (Must be a letter: A-Z, a-z) **$** (Must be alpha or numeric: A-Z, a-z, 0-9) **\\** (Following character is a fixed literal character) **' '** (All characters within single quotes are a fixed literal string) For example, the mask for a tag with the format **'Sales-'#######A$** will accept user inputs like **Sales-1234567QA** OR **Sales-9876543P2**, etc.
View ( )	Click to view tag details.
Delete ( )	Click to delete tag.
Submit	Apply changes.
Cancel	Cancel changes.

Previously added tags can be viewed and deleted from SmartTAP, but not modified.

6.7.2 Viewing / Deleting a Call Tag

The View / Delete Call Tags screen below indicates how to view and/or delete a call tag.

Figure 6-12: View/Delete Call Tags Screen



View/Delete Call Tags

Tag Name	Tag Description	Input Type	Input Format	View	Delete
Note	Notes about the call.	TEXT			
Company	Company Name	TEXT			
Malicious Call	Malicious Call	NONE			
Account ID	Customer Account ID	TEXT	AA'-'#####		
Follow Up	Requires Follow Up	BOOLEAN			
Feedback	Customer Feedback	SELECT_ONE	[Very Good, Great, Good, Poor]		

20 1 (1 of 1)

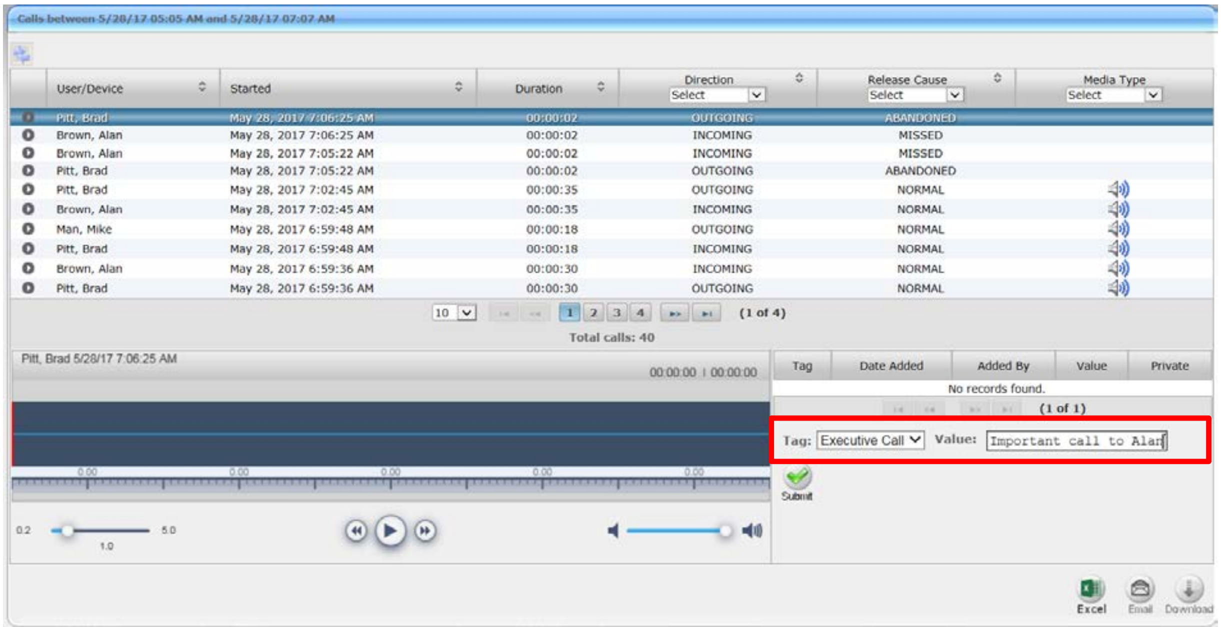
6.7.3 Assigning Values to a Call Tag and Applying to Call

This section describes how to apply a call tag to a call.

➢ **To apply a call tag:**

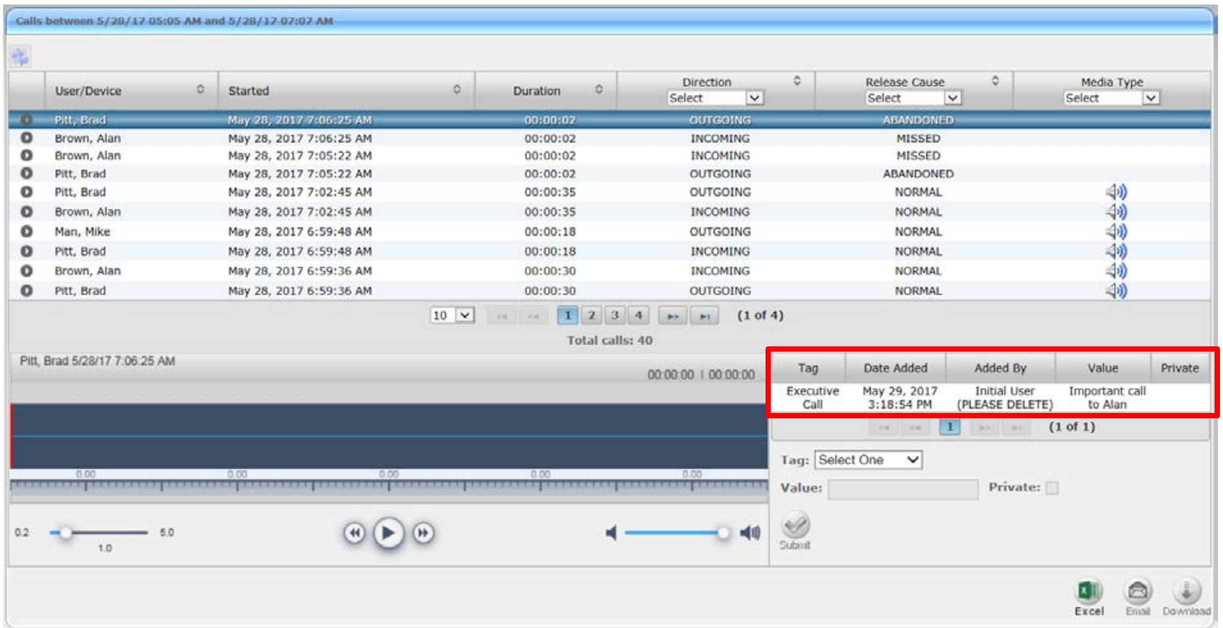
1. Search for call records (as described in Section 6.12.1)
2. Select the call record to tag.
3. From the Tags drop-down list, select the tag that you wish to assign.
4. In the Value field, enter the text note that you wish to assign to the tag. In the example below “Important call to Alan” (see highlighted in the figure below).
5. Click  .

Figure 6-13: Assigning Value to Call Tag



You can now view the assigned call tag (highlighted below):

Figure 6-14: Assigned Call Tag



6.8 Generating and Loading HTTPS Certificates

SmartTAP server by default operates in non-secure (HTTP) mode. This section describes how to optionally implement SSL/TLS (HTTPS) for the following:

- Securing the connection between your Web browser and the SmartTAP server
- Digitally signing audio files

6.8.1 Browser Connection Certificate Requirements

The certificate issued should contain the SAN (Subject Alternative Name) extension field, populated with all the correct URLs used to refer to the AS server:

- The FQDN (Fully Qualified Domain Name) of the AS server
- The Hostname (short server name, sans domain)
- The public IP of the AS server
- Any other CNAME used to refer to the AS server

In addition, ensure the following:

- All SAN entries are resolvable via the DNS configured on participating servers/workstations. Make sure the “DNS Suffixes” IPv4 setting is configured correctly.
- Whenever the network is installed with ***Microsoft Enterprise CA*** (as opposed to ***Microsoft Standalone CA***), the Domain’s root CA certificate is automatically distributed to all domain member servers and workstations. No further action is required.
- Servers/Workstations that <u>are not members</u> of the forest where ***Microsoft Enterprise CA*** is installed, and house SmartTAP components or used to manage SmartTAP via browser, should have the root CA certificate imported into Windows’ *“Trusted Root Certificates”* store.

- When using 3rd party Certificate Management Suite to self-issue a private certificate chain (as opposed to using a Global CA to issue a Global Certificate), the root CA certificate should be imported into Windows' "*Trusted Root Certificates*" store on all servers where SmartTAP components reside, and all computers used to manage SmartTAP via its web based UI.

6.8.2 Step 1: Generate Certificate Signing Request (CSR)

To obtain a certificate, first generate a CSR (Certificate Signing Request) from the SmartTAP server. A CSR is an encoded file that provides you with a standardized way to send the necessary details to a trusted authority in order to have the certificate created. When you generate a CSR, the software prompts for the following information - common name (e.g., www.example.com), organization name, location (country, state/province, city/town).

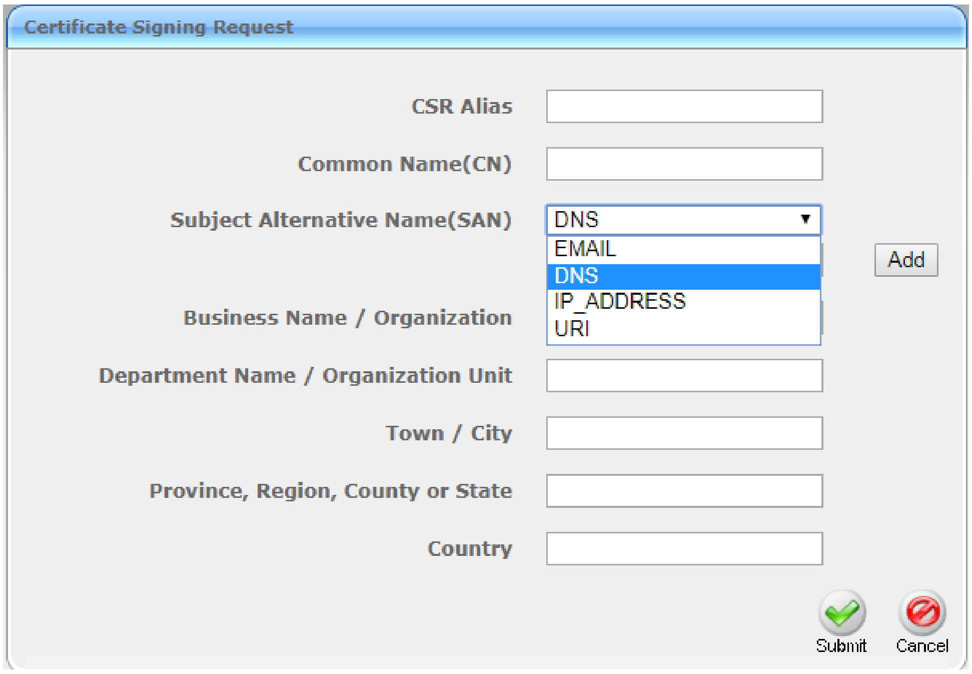
Note:

- The CSR is listed in the Certificate list as a self-signed certificate if you choose not to get a signed certificate from a trusted authority.
- To create a CSR, SmartTAP will automatically use Key type = RSA, Key size = 2048 and Cryptographic Hash = SHA-256.

➢ **This section shows how to generate a CSR. To generate a CSR:**

1. Under the System tab, select **Create Signing Request**.

Figure 6-15: Certificate Signing Request Screen



2. Use the table below as reference when defining the fields.

Table 6-9: Certificate Signing Request Screen

Field	Description
CSR Alias	Internal name associated with the CSR request.

Field	Description
Common Name (CN)	Full hostname=FQDN (consists of hostname + domain name).
Subject Alternative Name (SAN)	• **Email:** Indicates the email address of the organization • **DNS:** Indicates the name of the organization's DNS server • **IP_ADDRESS:** Indicates the IP address of the organization • **URL:** Indicates the URL of the organization's host server
Business Name / Organization	The legally registered name of your organization/company.
Department Name/ Organization Unit	The name of your department within the organization (frequently this entry will be 'IT', 'Web Security', etc.).
Town / City	The city in which your organization is located.
Province, Region, County or State	The Province, Region, County or State in which your organization is located.
Country	The country in which your organization is located. The following list of country codes is provided as a reference: http://www.digicert.com/ssl-certificate-country-codes.htm
Email	This field is optional..
Public Key	Created automatically by SmartTAP.

Note: It's inadvisable to abbreviate any information except for the country codes (i.e., enter New Jersey rather than NJ), to make sure there are no issues when you send the CSR to a trusted authority in order to generate the certificate, else it may be rejected.

3. Click **Submit**; the CSR is automatically available for download from the browser.
4. Save the 'filename.csr' file and send it to the trusted authority.

Note: Go to the View/Modify Certificate List to upload the official certificate from the trusted authority, in order to continue.

6.8.2.1 Viewing/Modifying the Certificate List

Figure 6-16: Viewing/Modifying the Certificate List

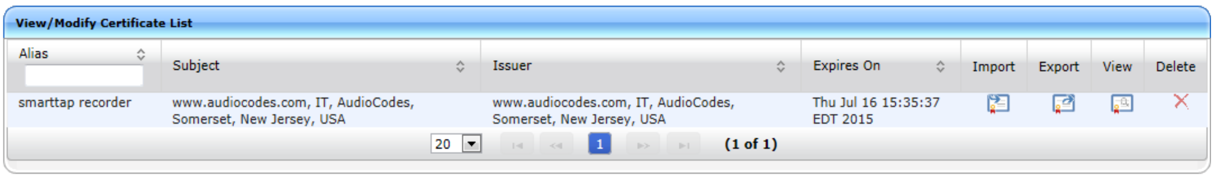


Table 6-10: Viewing/Modifying the Certificate List

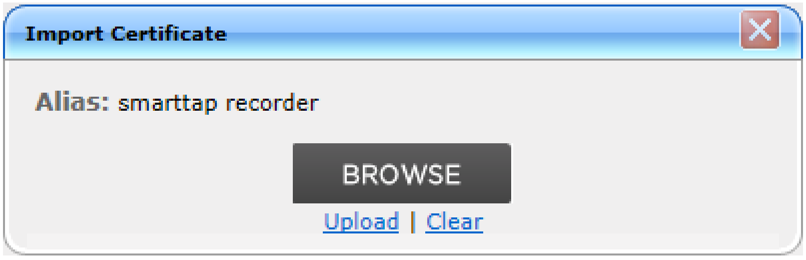
Field	Description
	Import signed Certificate 'filename.cer' from trusted authority

Field	Description
	Export Certificate to file to the local machine 'filename.cer'
	View Certificate

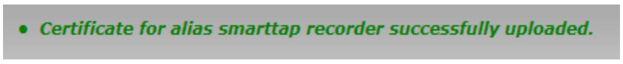
➢ To import a certificate:

- From the View/Modify Certificate List, click the **Import** icon.
- Click the **Browse** button and navigate to the location of the appropriate certificate file: 'filename.cer'

Figure 6-17: Import Certificate



- Once selected, click the **Upload** link.
- Once the upload completes, you should see a success message in the 'Command Execution Results' area.



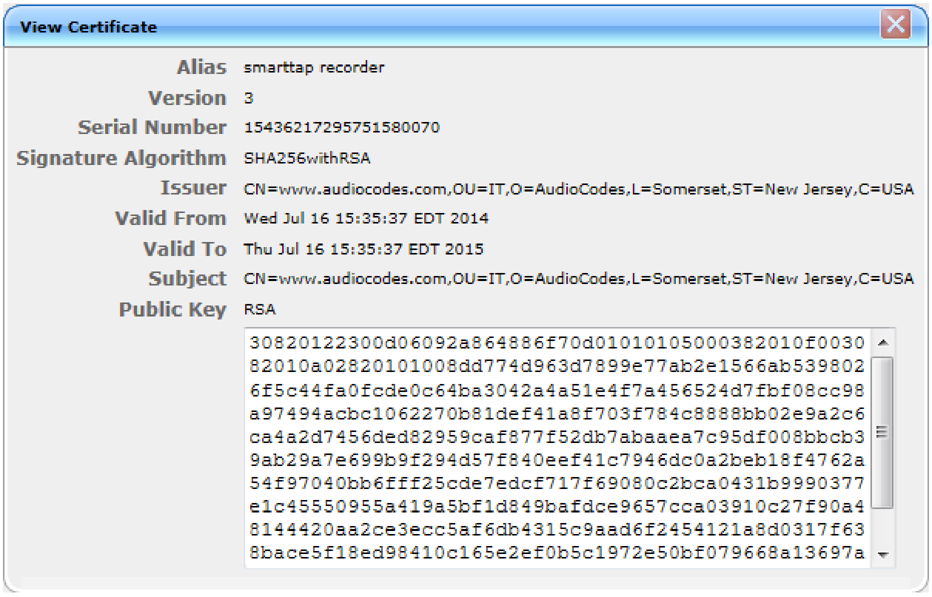
➢ To export a certificate:

- From the View/Modify Certificate List, click the Export icon
- The Certificate should now be available for download to the local PC.

➢ To view a certificate:

- From the View/Modify Certificate List, click the View icon.

Figure 6-18: View Certificate



6.8.3 Step 2: Load Certificates

Once a certificates are available, load them to secure the connection between a Web browser and the SmartTAP server and for securing digital files.

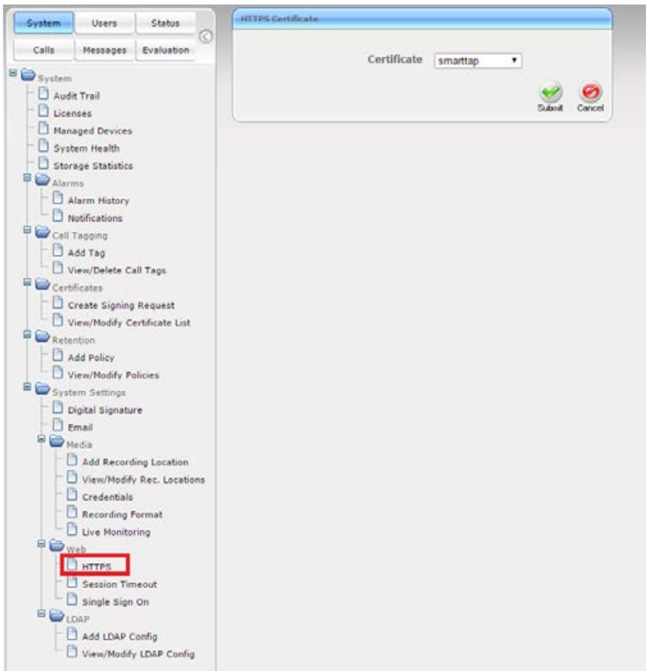
6.8.3.1 Loading Web Browser Certificate

This section describes how to load the certificate to secure the connection between your Web browser and the SmartTAP server.

➢ **To load the Web browser certificate:**

1. Open the HTTPS page (**System** tab > **Web** folder > **HTTPS**).

Figure 6-19: HTTPS Certificate



2. From the Certificate drop-down list, select the certificate that you wish to load and click 

.

3. Restart the SmartTAP server

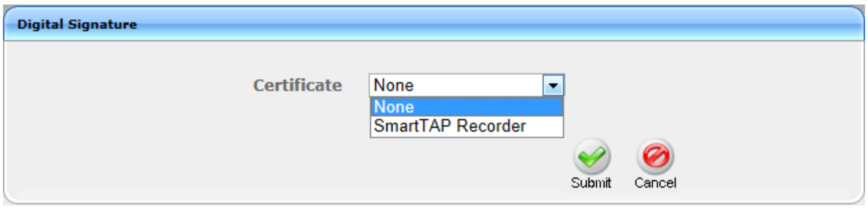
6.8.3.2 Loading Digital Files Certificate

This section describes how to load to certificate that you wish to secure digital recording files.

➢ **To load the digital files certificate:**

1. From the **System** tab, go to the System Settings section and select **Digital Signature**.
2. Select the appropriate certificate from the Certificate list box.
3. Click **Submit**.

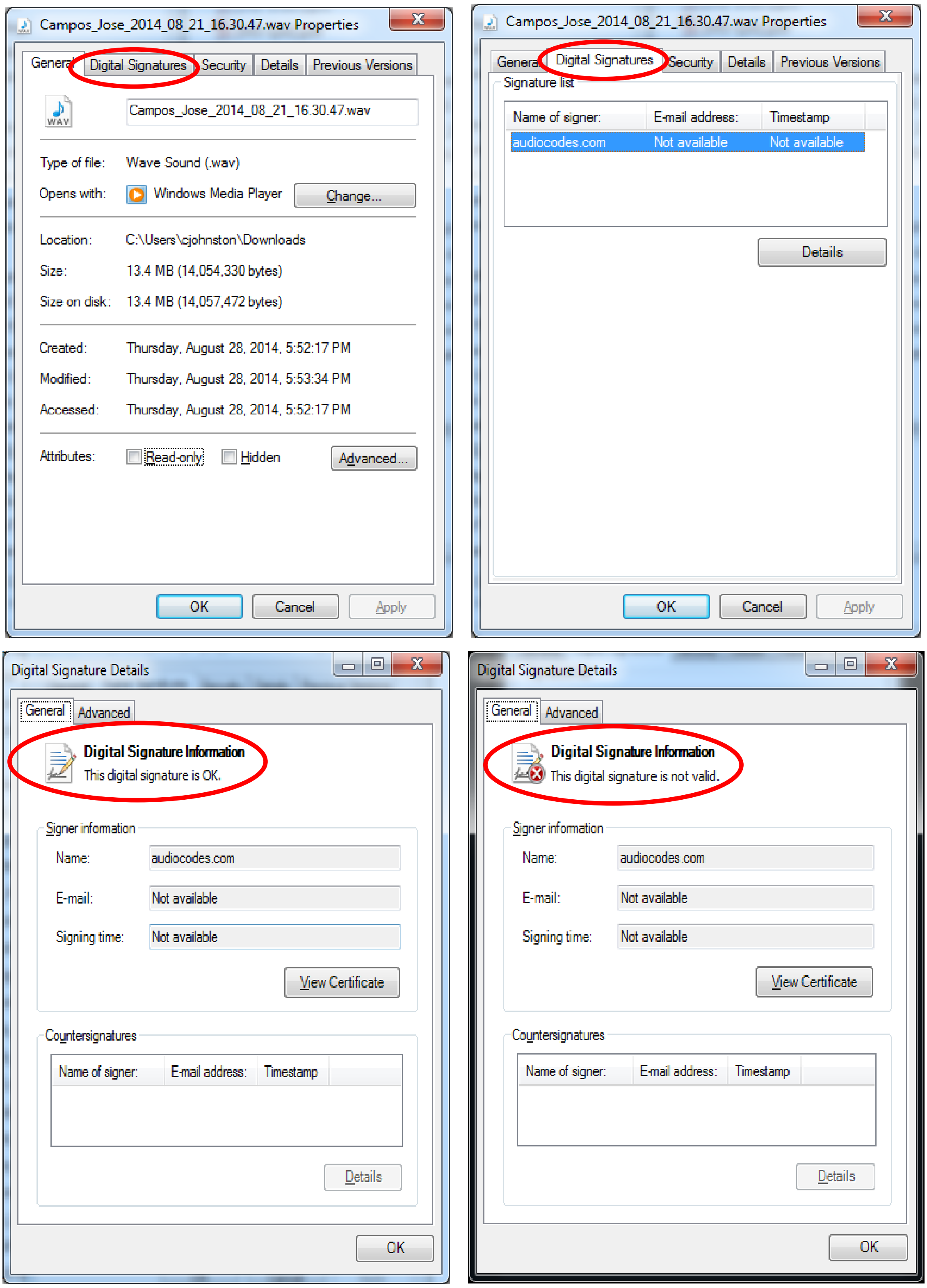
Figure 6-20: Digital Signature



If a user 'optionally' chooses to add a Digital Signature during the download process, the configured certificate is used to digitally sign the audio file. The SmartTAP Digital Signature file properties add-on must be installed on the local user PC to properly view the digital signature in the downloaded audio file.

Once installed, the **Digital Signatures** tab appears in the file properties of the downloaded audio recording. Click it to view the certificate and make sure it's from a trusted source. The certificate must be installed on the local PC in the Trusted Root authority.

Figure 6-21: Digital Signature Details



Note: Refer to the *SmartTAP Installation Guide* for instructions on how to install the add-on.

6.9 Configuring Call Retention

Call retention is the number of days to keep recordings in storage. Default: **0** indicates that recordings are never deleted. Use the default with caution since eventually the storage location will be completely consumed. To meet business requirements, it's highly recommended to set the retention value to a positive number.

SmartTAP deletes calls that exceed the retention period once a day. A network administrator with appropriate security profile credentials has the option to add / modify retention policies.

Figure 6-22: Call Retention Screen – Add Retention Policy

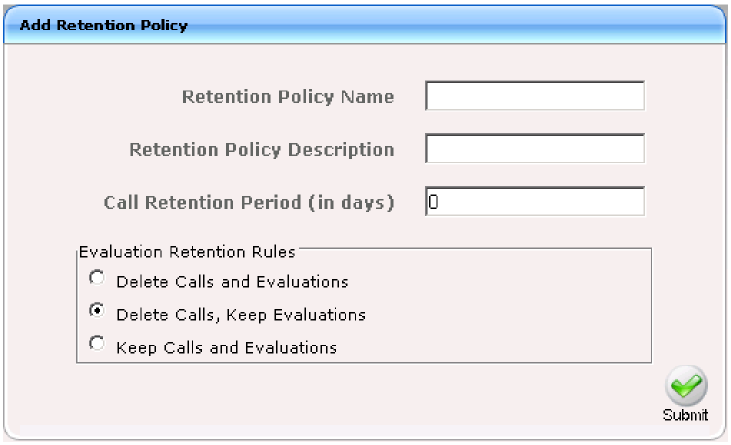


Table 6-11: Call Retention Screen

Field	Description
Call Retention Period (in days)	The number of days before automatically deleting recordings. A value of zero (**0**) indicates that recordings are never deleted.
Evaluation Retention Rules	Deletion rules for recordings with associated evaluations that exceed the Call Retention Period.
	Applies the changes.

The Evaluation Retention Rules determine whether recordings older than the retention period are deleted, based on whether there are evaluations associated with the recordings to delete.

Table 6-12: Evaluation Retention Rules

Rule	Description
Call Retention Evaluation Rules	The Retention Evaluation options set the rules for keeping and/or deleting calls used in evaluations, as well as evaluations themselves.
Delete Calls and Evaluations	Evaluations based on calls subject to retention will be deleted along with the calls.
Delete Calls, Keep Evaluations	Evaluations will be kept but calls will be deleted. Evaluation-call relationship will no longer exist.
Keep Calls and Evaluations	If an evaluation is associated with a call, both the call and the evaluation will be permanently kept.

➢ **To add a new retention policy:**

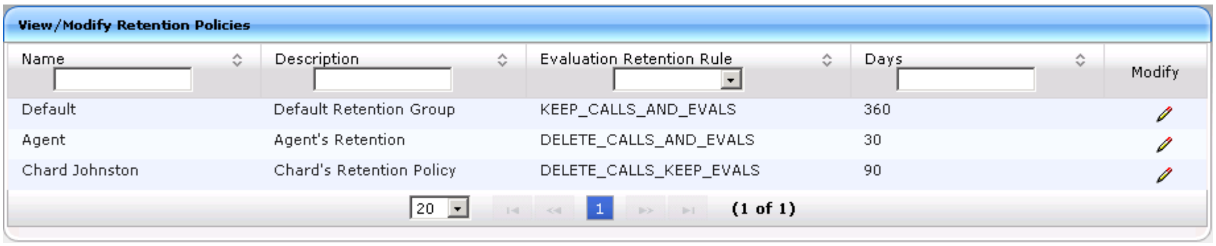
1. Open the Call Retention screen (**System** tab > **Retention** > **Add Policy**).
2. Enter the policy name (i.e., Agent, Sales, etc.).

3. Enter a description to describe who / what the policy applies to.
4. Enter the value for the Call Retention Period.
5. Select the appropriate 'Evaluation Retention Rule' assuming Evaluation is enabled.
6. Click Submit to submit changes.

➢ To view / modify a retention policy:

1. Open the Call Retention screen (**System** tab > **Retention** > **View** / **Modify Policies**).
2. Click the **Modify** ( ) for a specific policy and modify the necessary fields.
3. Click Submit to apply changes.

Figure 6-23: View / Modify Retention Screen



6.10 Configuring System Settings

Under 'System Settings', the administrator can configure interfaces pertaining to services or devices that are external to the system. From this folder, the administrator can configure the following:

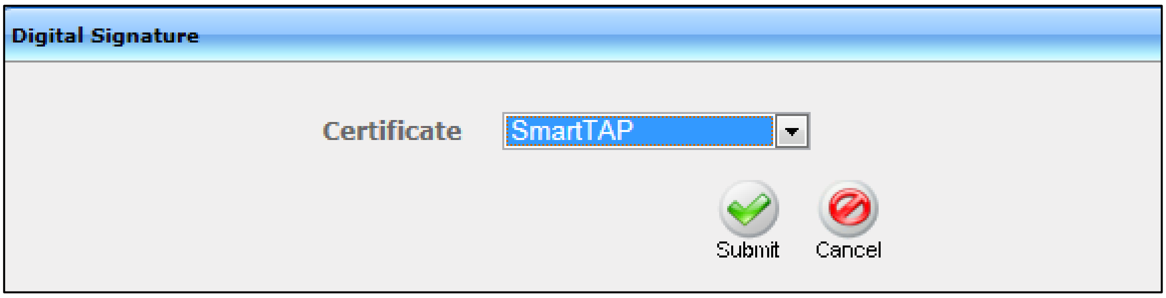
- Digital Signature to ensure that an electronic document (e-mail, spreadsheet, audio file, etc.) is authentic.
- SMTP interface to allow the SmartTAP server to send outbound emails
- LDAP interface to allow SmartTAP to use Active Directory users, groups, and security profiles
- Media storage location which may be stored on a network device
- End-user Web timeout

6.10.1 Configuring a Digital Signature

A digital signature is a way to make sure that an electronic document (e-mail, spreadsheet, audio file, etc.) is authentic. Authentic means that you know who created the document and that it was not altered in any way since that person or system downloaded it.

Select the appropriate certificate to use from the dropdown list. To generate a valid certificate, see Section 6.8.

Figure 6-24: Digital Signature



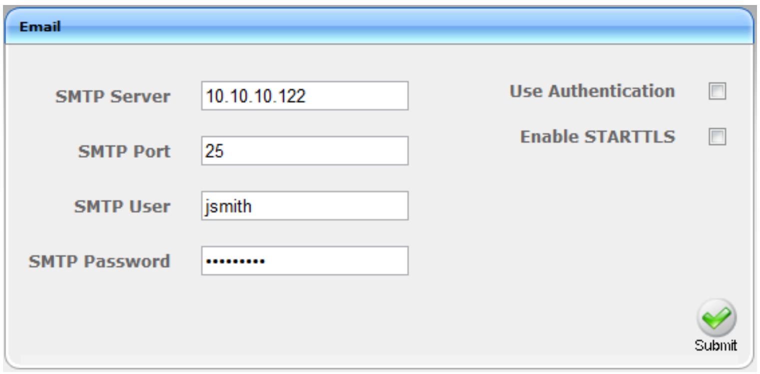
6.10.2 Configuring Email

SmartTAP sends automated email notifications and allows users to send emails directly from the user interface. The Email menu configures access to the SMTP server required to send outbound email from within SmartTAP.

➢ **To configure email:**

1. Open the Email screen (**System** tab > **System Settings** folder > **Email**).

Figure 6-25: Email



2. Enter the SMTP server information (provided by the SMTP administrator).

3. By default, SmartTAP will send email from username@audiocodes.com if the @domain.com is not included in the email account specified in the SMTP User field. To make sure an email is sent from your domain, set the SMTP User to username@YourDomain.com. Use the table below as reference.

Table 6-13: Email Screen

Field	Description
SMTP Server	Hostname or IP address of the email server.
SMTP Port	TCP port of the email server.
SMTP User	Email user for authentication.
SMTP Password	Email user password.
Use Authentication	Select the option if the SMTP server requires authentication.
Enable STARTTLS	Select the option when the SMTP server requires TLS.
Submit	Applies the changes.

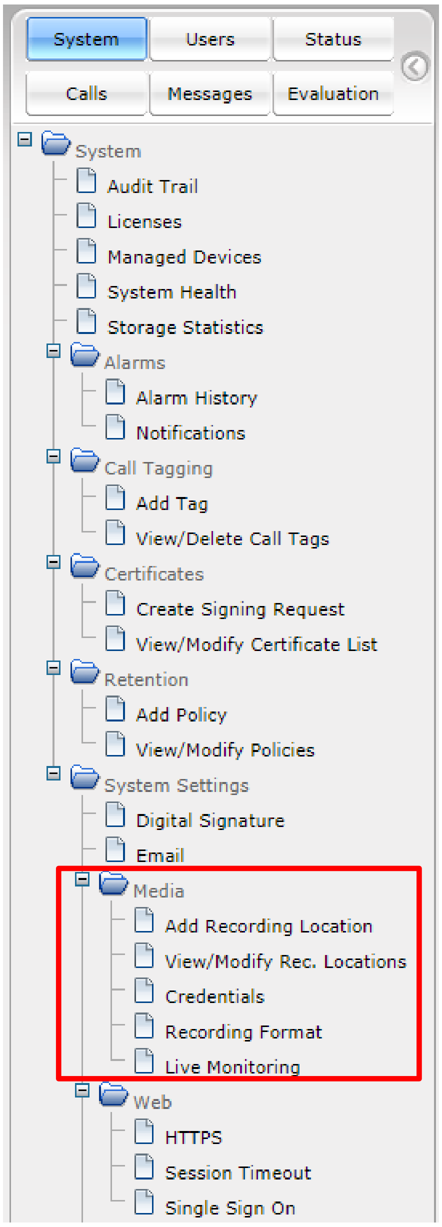
4. Apply changes (SmartTAP tests the Email interface when the user clicks the **Submit** button to apply the changes).
   - A successful configuration results in a message in **green** font in the command execution Results area.
   - A failed configuration results in a failure message and code in **red** font in the command execution Results area.

> **Note:** Email must be set up for SmartTAP to send email notifications, new user passwords, reset passwords, email recordings, email messages, etc.

6.10.3 Configuring Media

This section shows how to configure the items under the 'Media' folder shown in the figure below.

Figure 6-26: Media Folder



- Use the table below as a reference when accessing the items in the Media folder.

Table 6-14: Media Folder

Item	Description
Add Recording Location	Defines and adds a new media storage location. See Section 6.10.3.1.
View/Modify Rec. Locations	Allows viewing and modifying an existing media location. SmartTAP is shipped with a default local media storage location. A new location must be defined when media is not stored on the local drive. See Section 6.10.3.1.2.

Item	Description
Credentials	Sets the credentials to access the media recording locations. The credentials should be valid for all defined locations. See Section 6.10.3.3.
Recording Format	Defines a recording format, e.g., encryption and compression. See Section 6.10.3.4.
Live Monitoring Location	The Live monitoring feature allows users to listen to calls in real time. See Section 6.10.3.5.

6.10.3.1 Configure the Locations on the Call Delivery Server

Media configuration identifies the type and location of the storage for the recordings. The recordings may be stored on a local disk on the SmartTAP server, or on an SMB network accessible drive, i.e., Windows shared drive.

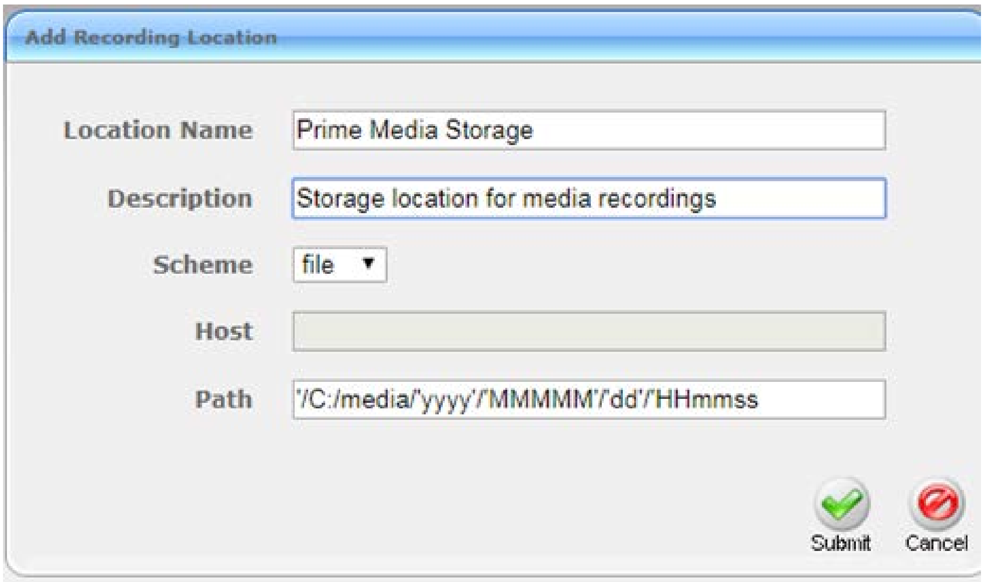
6.10.3.1.1 Configuring Media Storage on a Local Drive

This section shows how to configure media storage on a local drive.

➢ **To configure media storage on a local drive:**

1. Open the Media Storage Location screen (**System** tab > **Media** folder > **Add Recording Location**).
2. Select the **file** Scheme.
3. Default media path for **file** Scheme is **'/C:/media/'yyyy'/'MMMMM'/'dd'/'HHmmss** Where **C:** represents the drive letter, **media** represents the root directory to store the recordings, and **'yyyy'/'MMMMM'/'dd'/'HHmmss** is the subdirectory mask for the storage locations automatically created by the system.
4. Submit the changes.

Figure 6-27: Media Storage



6.10.3.1.2 Configuring Media Storage on a Network Drive

This section shows how to configure media storage on a network drive. Use the table below as a reference.

➢ **To configure media storage on a network drive:**

1. Open the Media Storage Location screen (**System** tab > **Media** folder > **Add Recording Location**).`
2. Select the **smb** Scheme.
3. Enter the path. The default media path for the **smb** Scheme is **mediaShare/yyyy/MMMMM/dd/HHmmss** where **mediaShare** is the name of the shared network drive.
4. Submit the changes.

Table 6-15: Add Recording Location

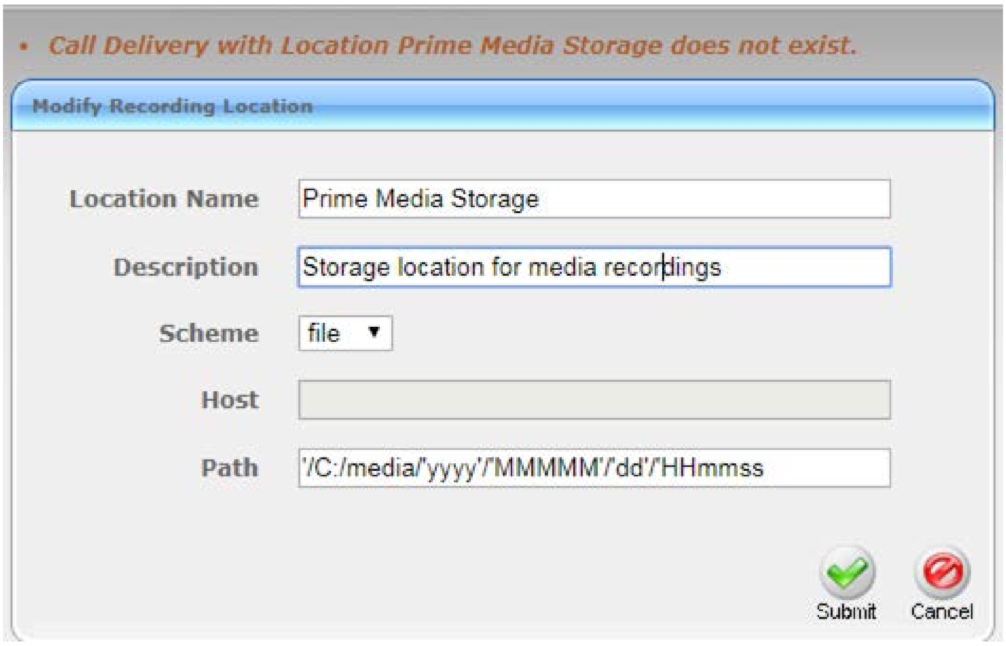
Parameter	Description
Location Name	Assign a name to the media location. The name serves to associate a media storage location with a location attribute defined in CallDelivery.
Description	Provide a description of the media location in order to facilitate intuitive management later.
Schema	Protocol to use when storing and retrieving recorded files. Either **file** or **smb**. • **file** is selected when recordings are to be stored on the same server as the Application and Media Server. • **smb** (Server Message Block, also known as CIFS) is used to remotely access shared files and directories on SMB file servers.
Host	Host name or IP address where the media files will be stored. Allowed only with **smb** Schema.
Path	Sets the media path pattern for recorded files.

Important: In machines with a locale other than English change **MMMMM** to **MM** in order to switch from lettered month presentation to numerical, or else SmartTAP will not play or download recordings.

6.10.3.1.3 Troubleshooting

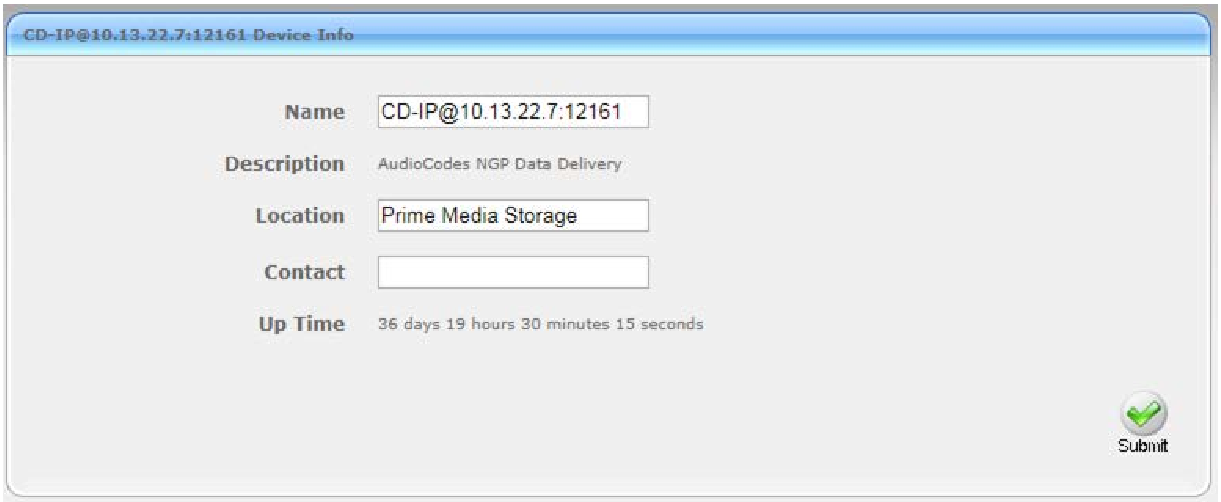
If the above message is displayed, this implies that the Location was defined, however, CallDelivery was not associated to this location name (Prime Media Storage).

Figure 6-28: Location does not Exist



To associate the CD, navigate to **System** > **Managed Devices**, select required Call delivery and define the location in the Device Info (for more information, see Section **Error! Reference source not found.**).

Figure 6-29: Device Info



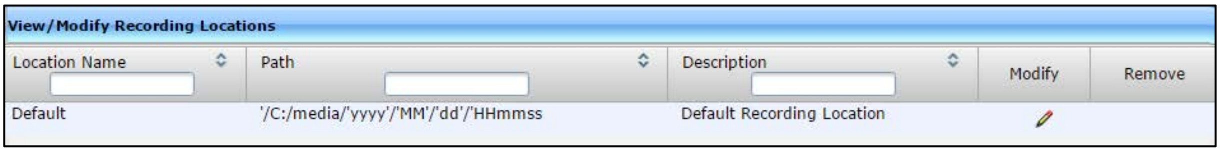
6.10.3.2 Modifying a Recording Location

This section shows how to modify a recording location.

➢ **To modify a recording location:**

1. Open the View/Modify Rec. Locations screen (**System** tab > **Media** folder > **View/Modify Rec. Locations**).

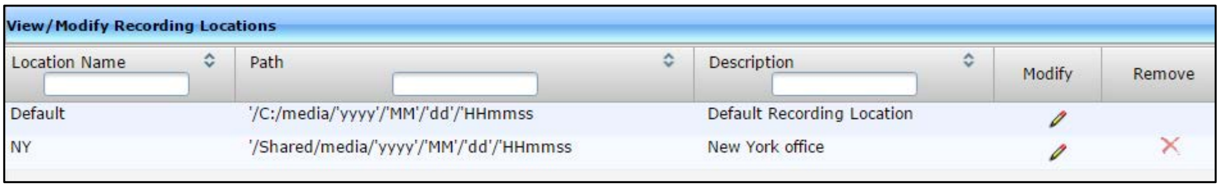
Figure 6-30: View/Modify Recording Locations - with Default Location Only



View/Modify Recording Locations

Location Name	Path	Description	Modify	Remove
Default	'/C:/media/'yyyy'/'MM'/'dd'/'HHmmss	Default Recording Location		

Figure 6-31: View/Modify Recording Locations - with Additional Recording Locations



View/Modify Recording Locations

Location Name	Path	Description	Modify	Remove
Default	'/C:/media/'yyyy'/'MM'/'dd'/'HHmmss	Default Recording Location		
NY	'/Shared/media/'yyyy'/'MM'/'dd'/'HHmmss	New York office		

2. Press the **Modify** button; this screen is displayed:

Figure 6-32: Modify Recording Location – Unmodifiable Location Name of 'Default'

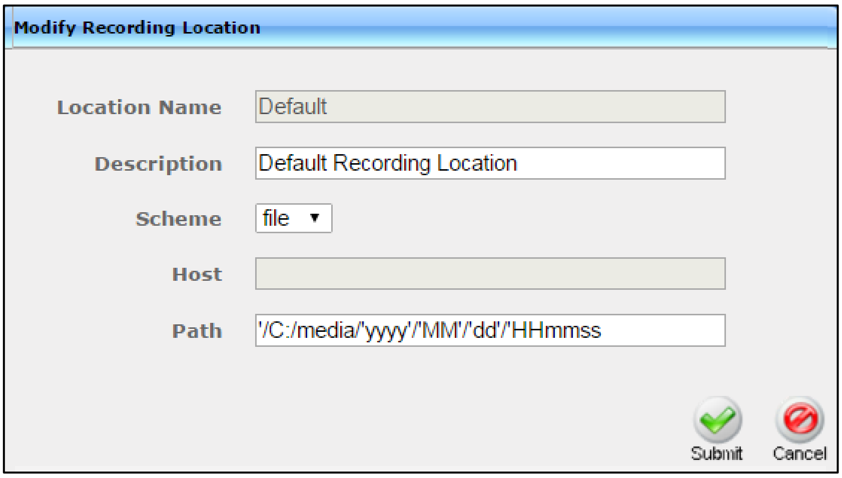
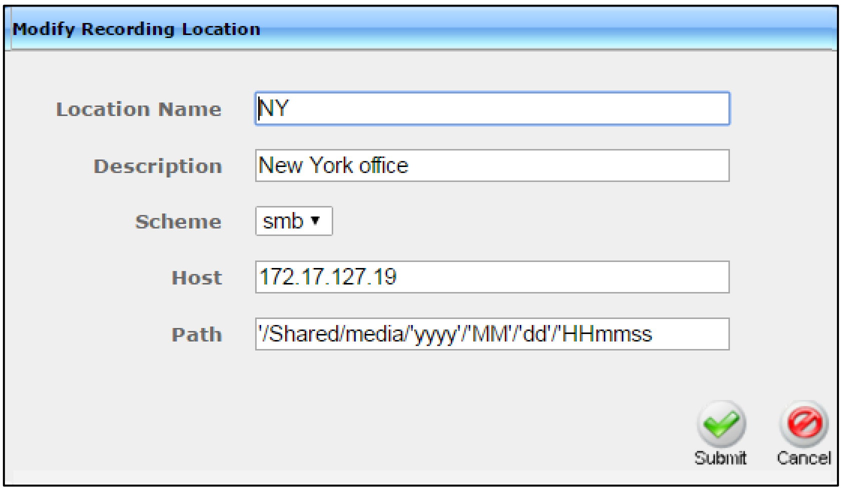


Figure 6-33: Modify Recording Location – Modifiable Location Name



Use the table below as a reference when viewing/modifying recording location.

Table 6-16: Modify Recording Location

Parameter	Description
Location Name	Define a name for the media location. The Location Name of **Default** cannot be modified.
Path	Define the media path pattern.
Description	Provide a description of the media location in order to facilitate intuitive management later.
Modify ( )	Click to modify the location.
Delete ( )	Click to delete the location.

6.10.3.3 Configuring User Credentials

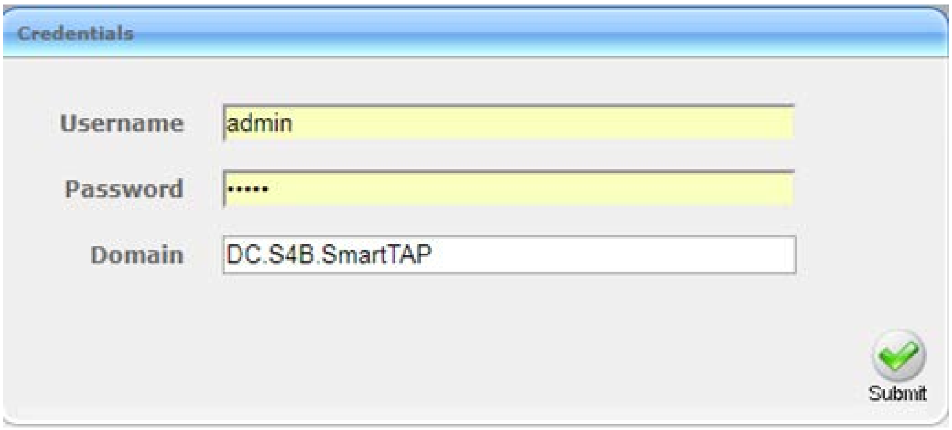
This section shows how to define credentials for accessing shared resources. Whenever you add or modify the location for saving recording or live monitoring files, SmartTAP verifies whether this location is accessible to the user defined in this procedure.

Note: You must define credentials before adding an SMB recording location (as described in Section 6.10.3.1) else the attempt to add the location will fail and you'll need to exit the screen, set the credentials, and then try to add the recording location again.

➤ **To define credentials:**

1. Open the credentials page (**System** tab > **Media** folder > **Credentials**).

Figure 6-34: Credentials



Use the table below as a reference when defining credentials.

Table 6-17: Credentials

Parameter	Description
Username	Specify a Username to use for accessing shared resources.
Password	Specify a Password to use for accessing shared resources.
Domain	Specify the authentication domain used to authenticate the username and password for accessing shared resources.

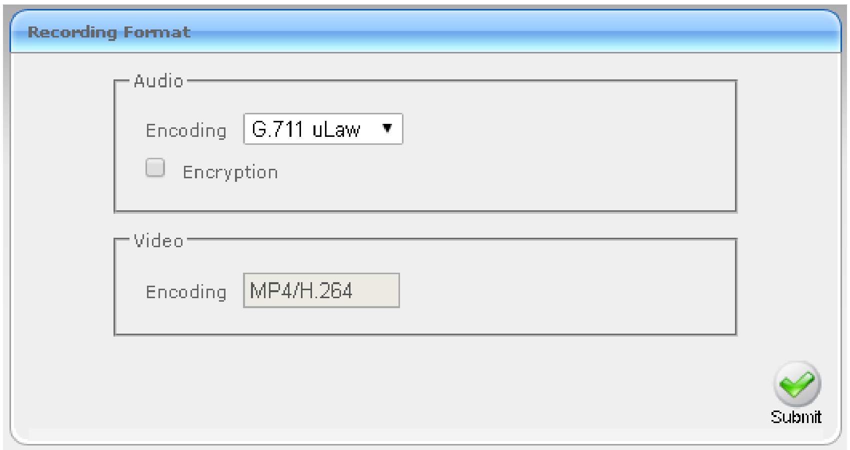
6.10.3.4 Defining a Recording Format

This section shows how to define a recording format.

➢ **To define a recording format:**

1. Open the Media Storage Location screen (**System** tab > **Media** folder > **Recording Format**.

Figure 6-35: Recording Format



2. Use the table below as a reference when defining a recording format.

Table 6-18: Recording Format

Parameter	Description
Audio Encoding	From the dropdown choose either: ▪ **g711Ulaw** (uncompressed storage) ▪ **g711Alaw** (uncompressed storage) ▪ **g729** (compressed storage)
	Encryption Select this option to encrypt media files as they are recorded.
Video Encoding	Video recordings are by default saved in MP4/H.264 format (not configurable).

3. Click 

to submit changes.

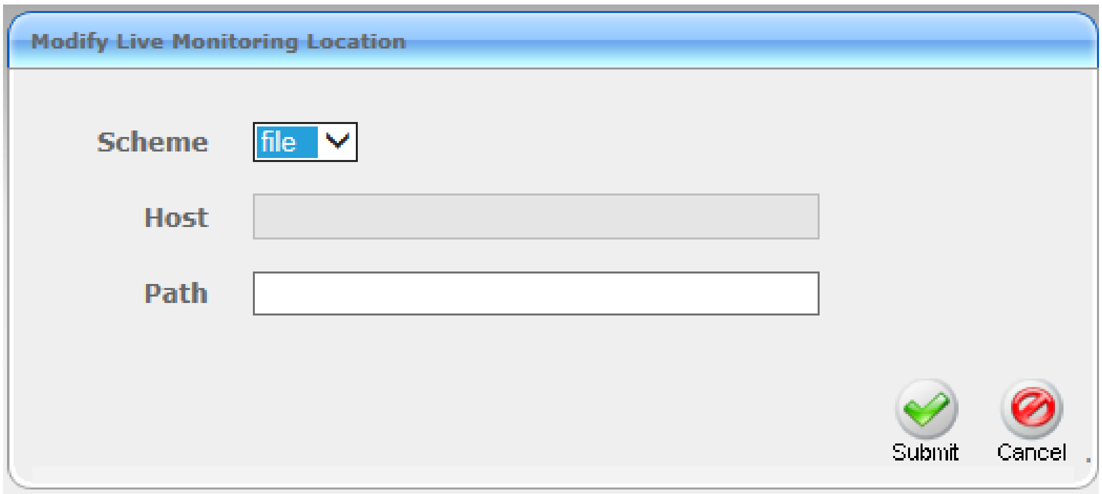
6.10.3.5 Configure Live Monitoring Location

The Live monitoring feature allows users to listen to calls in real time. When this feature is enabled for a site, Live monitoring media files are buffered to a playlist. The playlist and files are stored in the “Live Monitoring Location” which can be configured using this procedure. The live monitoring content is constantly refreshed by the SmartTAP client and can be played back by the user by clicking the **Live Monitor** microphone button (see Section 3.1).

➢ **To configure Live Monitoring file location:**

- Open the Live Monitoring page (**System** tab > **Media** folder> **Live Monitoring**).

Figure 6-36: Modify Live Monitoring Location



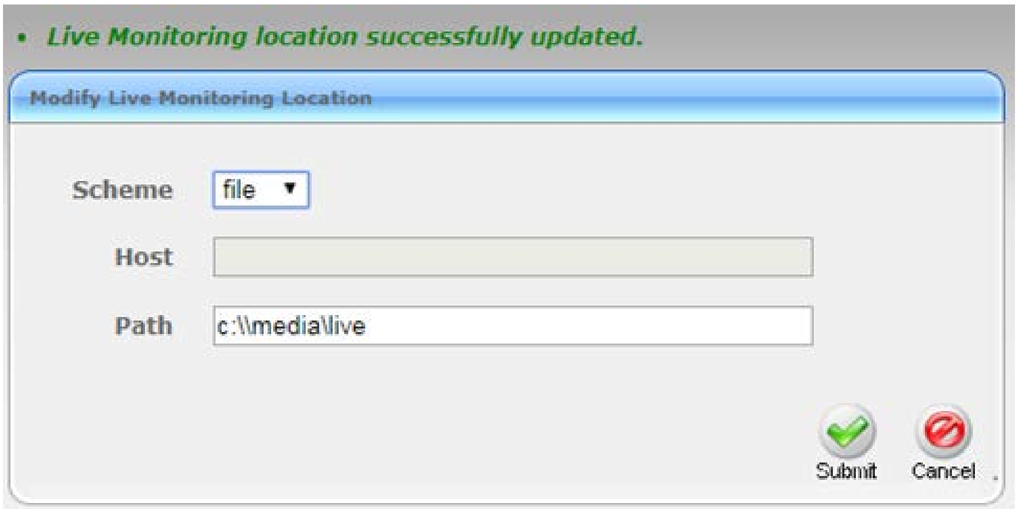
In this page, the following can be configured:

- **Scheme:** A protocol for storing and retrieving live monitoring files. Two options for scheme are available:
  - **File:** Used when recordings are stored on the same server as the Application Server.
  - **Smb:** Server Message Block (SMB) also known as CIFS, is used to remotely access shared files and directories on SMB file servers (i.e. a Microsoft Windows "share”).
- **Host:** Media files are stored on the host.
- **Path:** Sets the media path for recorded files. The path input is a plain path e.g., C:\Media (no string pattern is available).

Note: When the changes are submitted, the target folder path is verified for read/write access according to the credentials defined in the Credentials page (see Section 6.10.3.3).

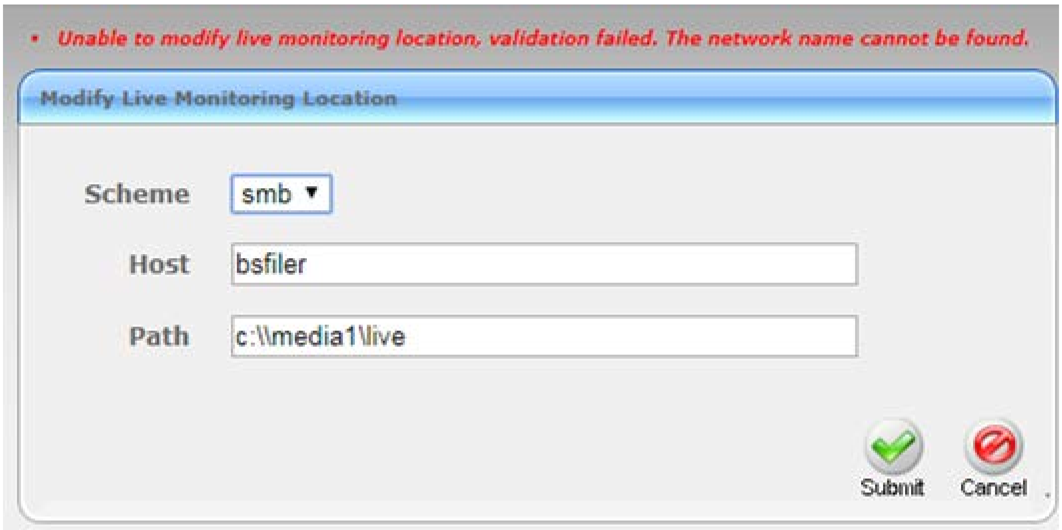
When the Live Monitoring Location has been successfully updated, a confirmation message is displayed at the top of the dialog:

Figure 6-37: Modify Live Monitoring Location-Successfully Update



In the case of failure, an error message describing the problem is displayed at the top of the dialog:

Figure 6-38: Modify Live Monitoring Location-Update Error



6.10.4 Configuring Single Sign-On

Single Sign-on (SSO) simplifies the login process for domain administrators. The administrator logs into their machine using domain credentials. The user then attempts to access the Application Server's Web service via a Web browser such as IE, Chrome or Firefox. *Without* SSO, the administrator is directed to a login form where Username and Password are entered and sent to SmartTAP to authenticate. *With* SSO enabled, the administrator is authenticated in the background through Active Directory using the same domain credentials that were used to log into the machine. This bypasses the login page and immediately opens the Welcome page.

Important: The SmartTAP server must be added to the Domain.

➢ To configure Single Sign-On:

1. Open the Single Sign-On page (**System** tab > **Web** folder > **Single Sign-On**).

   Initially, SSO is disabled, therefore the login form must be used. Log in under any account, with permissions to make SmartTAP system changes such as the default administrative user, 'admin'.
2. Configure the following parameters:
   - **Enable SSO** – select this option to enable Single Sign-On.
   - **KDC** – The Key Distribution Center, likely located on the Active Directory Server. Enter the hostname for your KDC (**ad.myDomain.local**).
   - **Principal** – Enter {principal} here. Note that the principal name must include the security realm (**HTTP/smarttap.myDomain.local@MYDOMAIN.LOCAL**).
   - **Password** – Enter the password for the defined Service Principal name.
3. **Submit** the changes when you have completed the configuration; a status notification indicates that the entries were validated and applied; a popup warns that the Application Server must be restarted for the changes to take effect. Restart the Application Server's Web service for the changes to take effect.

Figure 6-39: Single Sign-On

6.10.4.1 Validating SSO

The validation page validates some of the parameters entered and validates that SSO is functioning correctly.

- The KDC hostname is resolved to an IP address. If the name cannot be resolved, an error is given indicating that the KDC is invalid.
- The Principal name is parsed to ensure it contains the service, hostname and realm, i.e., there is some text for the service (HTTP), followed by a '/' followed by more text for the principal name and a '@' followed by the text for the realm. Each individual piece of this name is not checked and will be used as given.
- The password is not validated in anyway and is taken as entered.

Note: Refer to Appendix A for other necessary steps to configure SSO.

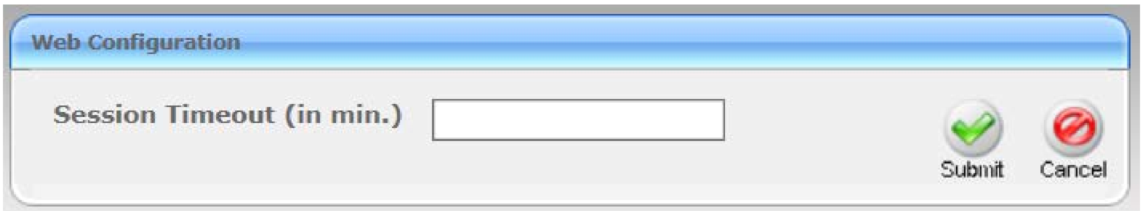
6.10.5 Configuring Web Session Timeout

You can configure the Web Session Timeout (in minutes) using the Web Configuration screen. The Web configuration screen shows the current Web Session Timeout in minutes. Changes to this value will only affect logins after the change takes place. Valid range is 1 to 60 minutes. The time a user session may be left idle before the system automatically logs the user off is configurable. The default is 20 minutes and may be changed by someone with the appropriate security profile credentials.

➢ **To configure Web Session Timeout:**

1. Open the Session Timeout page (**System** tab > **System Settings** folder > **Session Timeout**).

Figure 6-40: Session Timeout



2. Specify the appropriate Session Timeout.
3. Click 

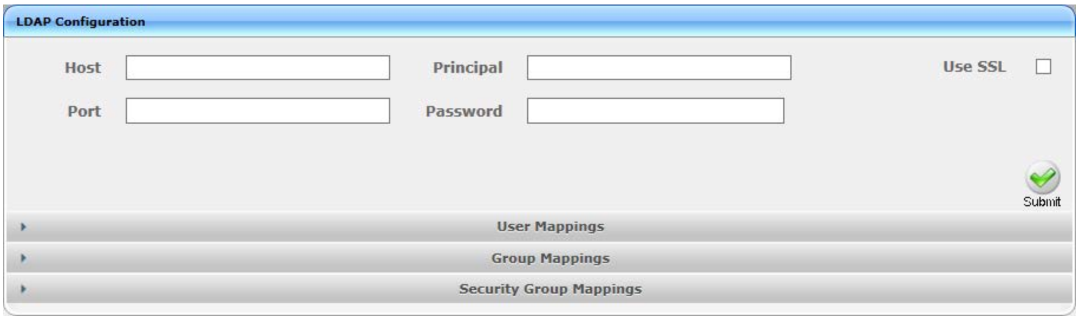
to accept changes.

6.10.6 Configuring an LDAP Connection

The LDAP Configuration page shown below allows configuration of an LDAP Provider. The information required to connect to the LDAP server, along with the user, group, and security group attribute mappings, are all configured from this page. Once the connection information is correctly entered and submitted, the list of object classes and attributes for mapping the various user, group, and security group properties will be obtained from the LDAP server.

Note: SmartTAP existing local users that match LDAP-obtained users are treated as the same unique user.

Figure 6-41: LDAP Connection Configuration



Use the table as reference to the screen parameters.

Table 6-19: LDAP Connection Configuration Screen

Field	Description
Host	Hostname of LDAP provider. Sorted ascending/descending by clicking header up/down arrows. Dropdown displays only matching entries.
Port	The Port on which the LDAP server is listening on. This is typically **389** for plain connections and **636** when using SSL. Sorted ascending/descending by clicking header up/down arrows. Dropdown displays only matching entries.
Principal	The Principal user's distinguished name, to use when connecting to the LDAP Server. This user must at least have search privileges.
Password	The password of the principal user to use for connecting to the LDAP server.
Use SSL	Click if required by the LDAP host.

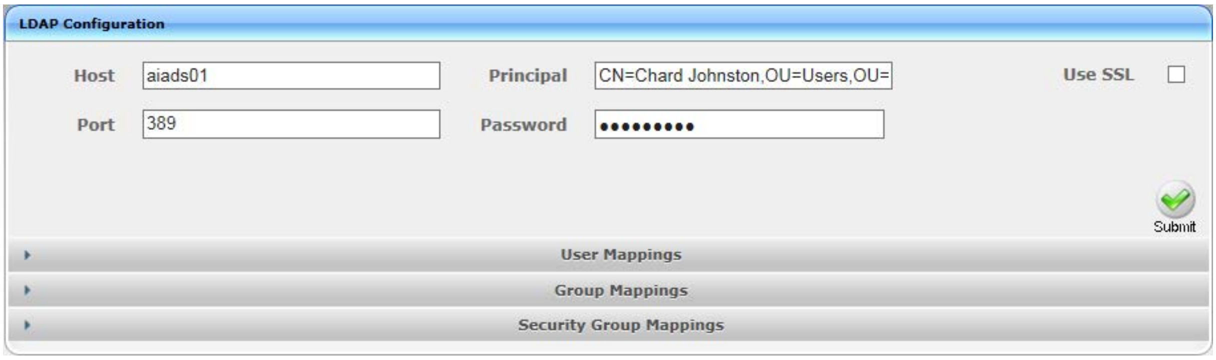
➢ **To configure an LDAP connection from the Domain Controller:**

1. Run Active Directory Explorer on the domain controller
2. Find the distinguishedName of the Administrator account (or whatever account has full read access to the entire LDAP database). (i.e. CN=Administrator,CN=Users,DC=qalabEE,DC=local)

➢ To configure an LDAP connection from SmartTAP:

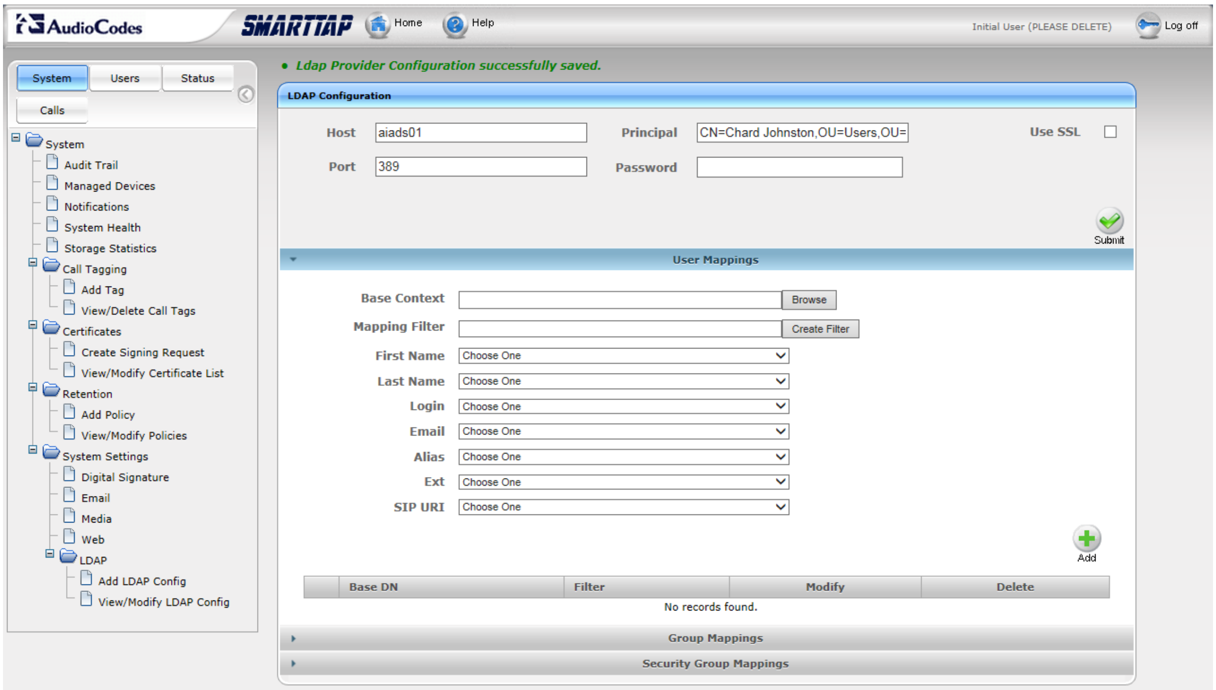
1. Open LDAP Providers screen (**System** tab > **System Setting** folder > **Add LDAP Config**).
2. Enter the IP or Name of the domain controller in the 'Host' field.
3. Enter distinguishedName in the 'Principal' field.
4. Enter the Port number in the 'Port' field.
5. Provide the password for the distinguishedName account used.
6. Check 'Use SSL' if required (see the next section for more information).

Figure 6-42: LDAP Connection Configuration



- Click  to apply changes; 'LDAP Provider Configuration successfully saved.' is displayed above the LDAP Configuration screen title bar.

Figure 6-43: LDAP Configuration



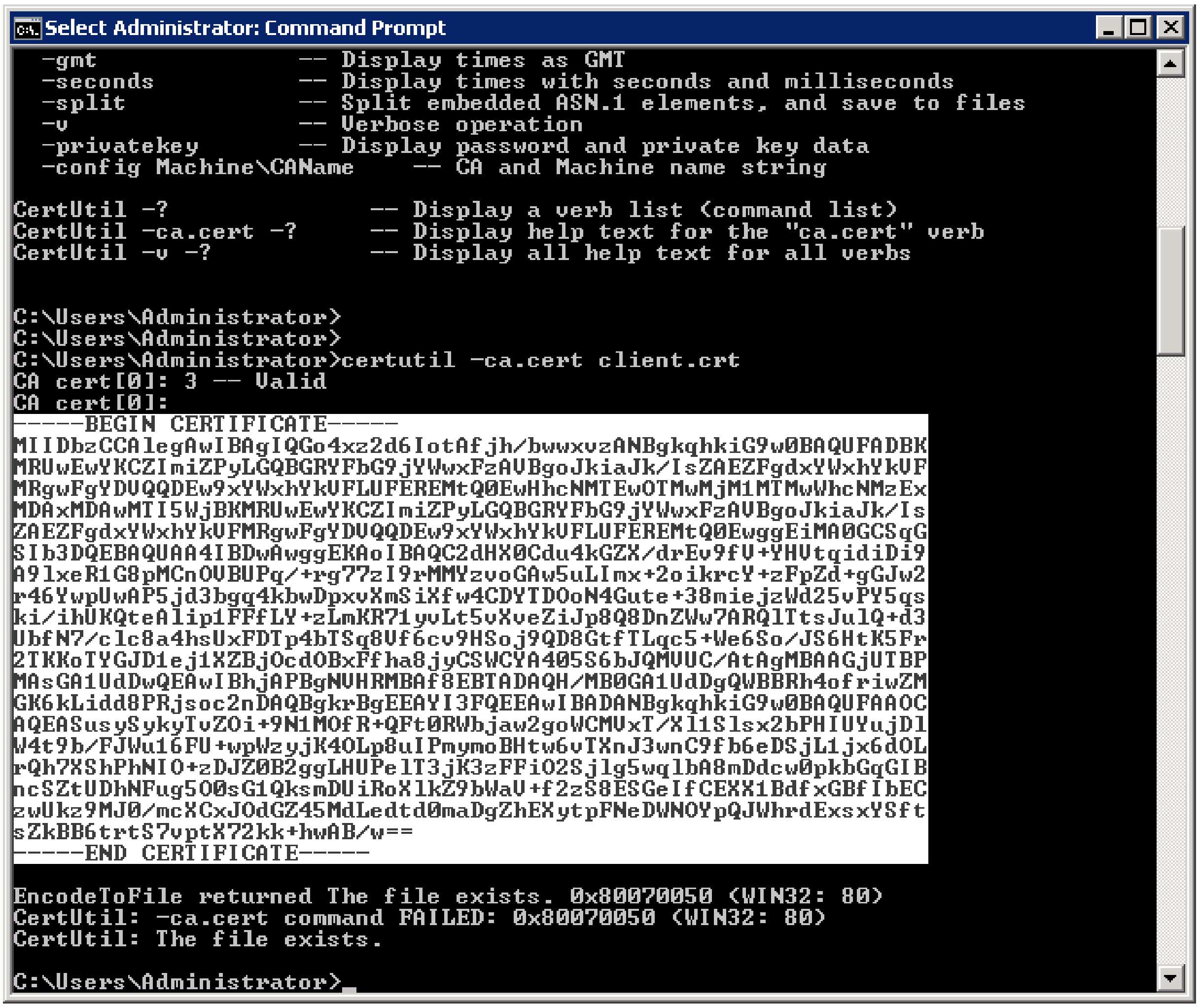
6.10.7 Configuring SSL

This section shows how to enable SSL encryption between SmartTAP and AD for all LDAP transactions.

➢ **To enable encryption between SmartTAP and AD for all LDAP transactions:**

1. On the server that houses the certificate authority (typically, the domain's active directory server), run from a command prompt:
   `certutil -ca.cert client.crt`
2. Copy `client.crt` from the Active Directory server to the SmartTAP server, copy from ------BEGIN CERTIFICATE----- to -----END CERTIFICATE----.

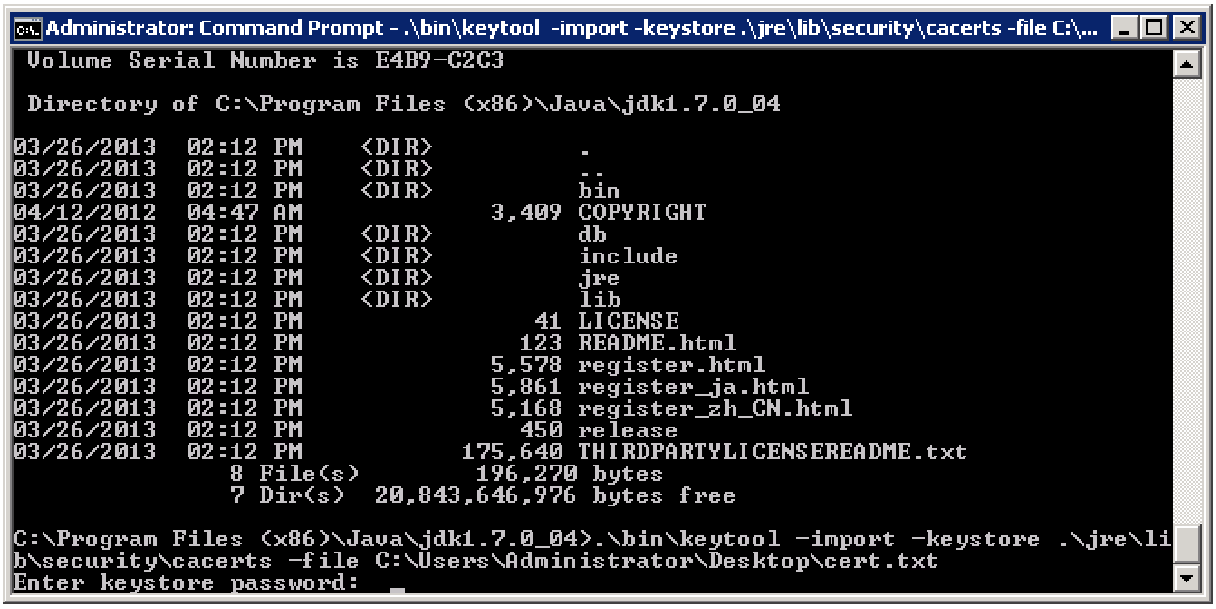
Figure 6-44: SSL



3. Copy the certificate to the SmartTAP machine. From the Java directory (C:\Program Files\Java\<jre_version>\ on SmartTAP) run the following:

```
\bin\keytool -import -keystore .\jre\lib\security\cacerts -file
c:\YOURPATHHERE\client.crt
```

Figure 6-45: SSL

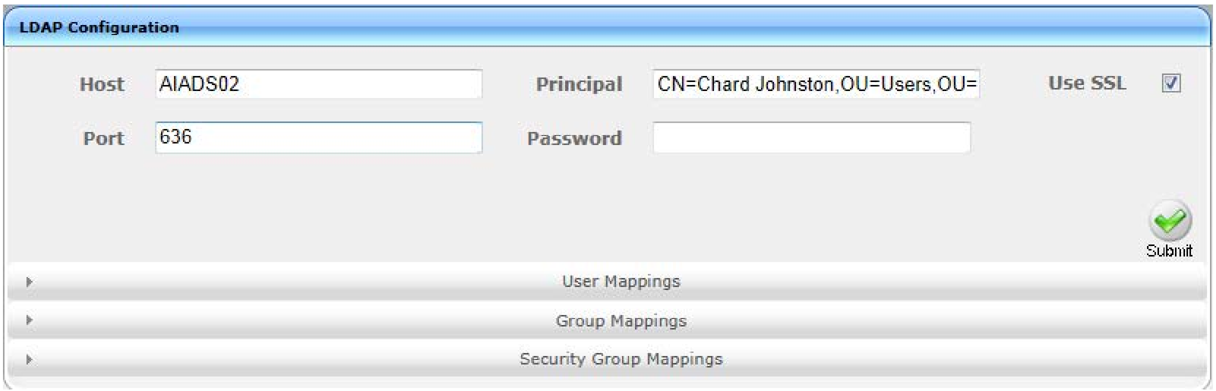


Note:

- The keytool will prompt you for a password. The default keystore password is **changeit**.
- Make sure you replace YOURPATHHERE with the actual path to where the **client.crt** file is.
- When prompted *Trust this certificate? [no]:* enter **yes** to confirm the key import.

4. The default port for LDAPS (LDAP with SSL support) is **636** (see the figure below).
5. Check the 'Use SSL' checkbox (see the figure below).
6. Click **Submit** to continue (see the figure below).

Figure 6-46: LDAPS



6.10.8 Configuring an LDAP User

This section shows how to configure an LDAP user. The following entities need to be configured:

- User Mappings
- Group Mappings
- Security Group Mappings.

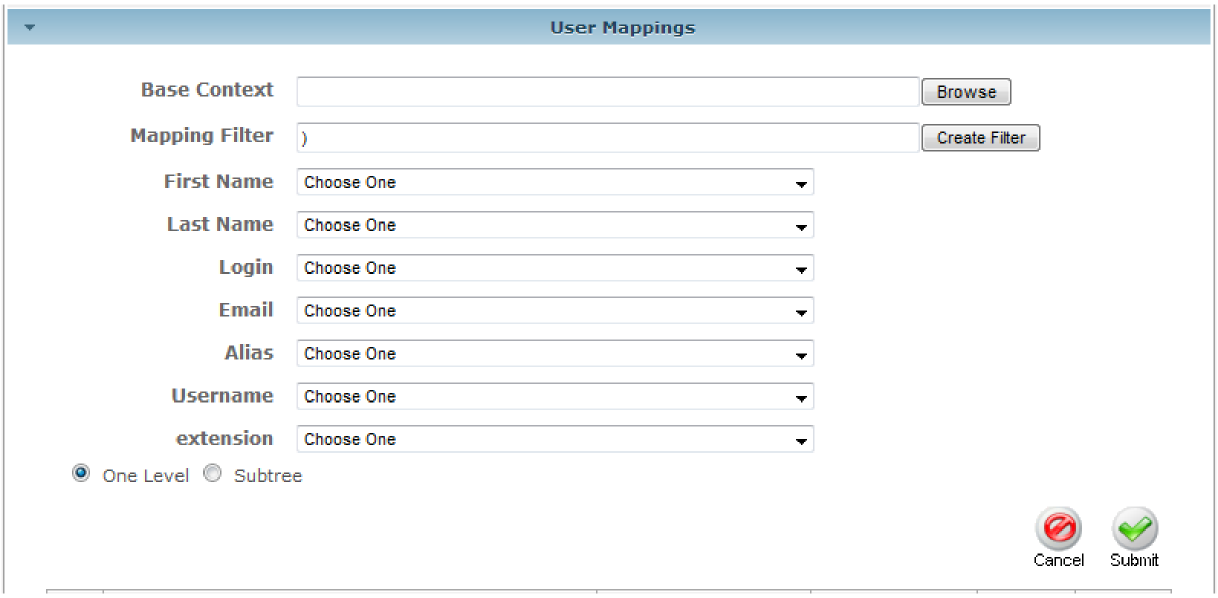
6.10.8.1 Configuring User Mappings

The procedure below describes how to configure User Mappings.

➢ **To configure User Mappings:**

1. Open the User Mappings screen shown below.

Figure 6-47: User Mappings



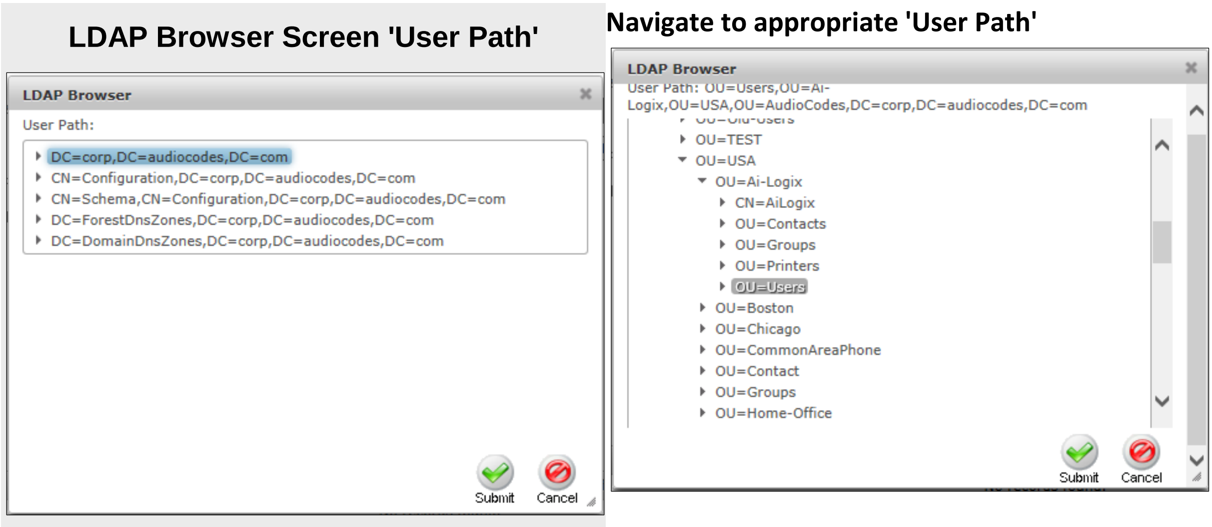
Use the table below as reference.

Table 6-20: User Mappings – Field Descriptions

Field	Description
User Mappings	▪ **User Base Context** (LDAP path for users). ▪ **User Filter** (Create / Manage User filter). ▪ **First Name** (LDAP Attribute that maps to the user first name). ▪ **Last Name** (LDAP Attribute that maps to the user last name). ▪ **Login** (LDAP Attribute that maps to the user login. The login should map to an attribute that contains a unique value across all LDAP providers, else users with the same login value will be considered the same user). ▪ **Alias** (LDAP Attribute that maps to the user alias, nickname, or employee ID). ▪ **One Level** – Retrieves LDAP attributes for the selected node. ▪ **Subtree** – Retrieves LDAP attributes for the selected node and all its child nodes in the LDAP directory tree. = expand screen = shrink screen

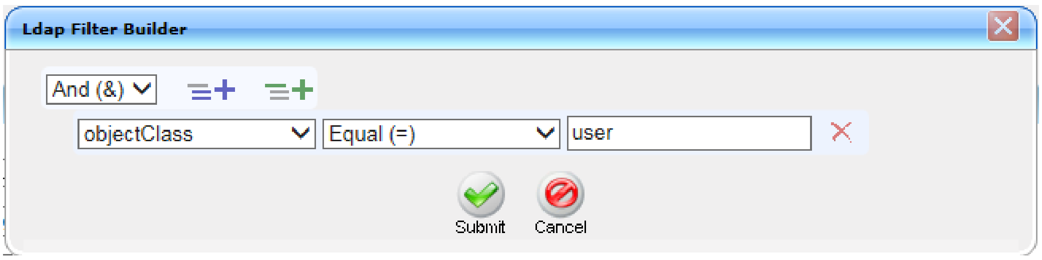
2. Enter the User Mappings Information in the 'User Mappings' screen (click if necessary to expand the screen).
3. The default user location in Windows is displayed as follows:

   OU=Ai-Logix,OU=USA,OU=AudioCodes,DC=corp,DC=audiocodes,DC=com
4. Click **Browse** and navigate to the appropriate OU.



5. Navigate to the appropriate 'User Path' and then click **Submit**.
6. Use filtering if you prefer not to add all users.

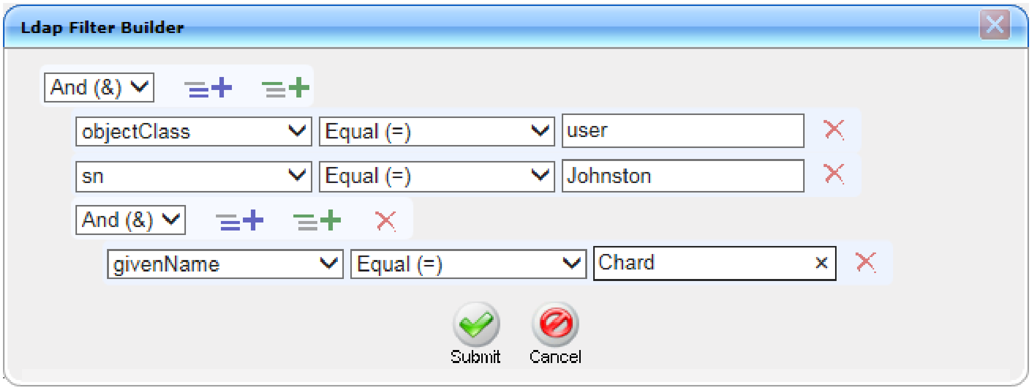
Figure 6-48: User Filtering Screen



■ To add a filter:

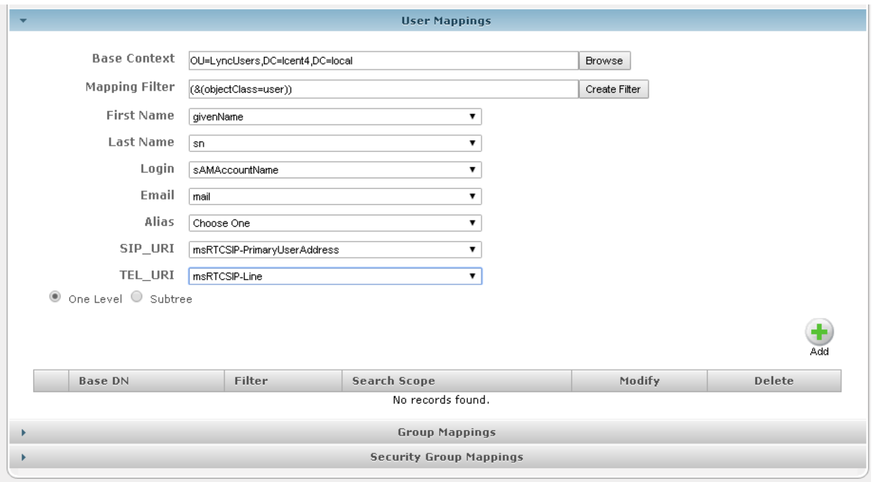
a. Select the appropriate Conditional Operator (And, Or, Not)
b. Select the appropriate Attribute
c. Select the appropriate Equality Operator (>=, =, ~=, <=)
d. Specify value = **(objectClass = user)** recommended
e. Click Submit to apply changes
f. Click the icon to add an additional filter and repeat above filter steps
g. Click the icon to add a Sub filter and repeat above filter steps

Figure 6-49: LDAP Filter Builder Example



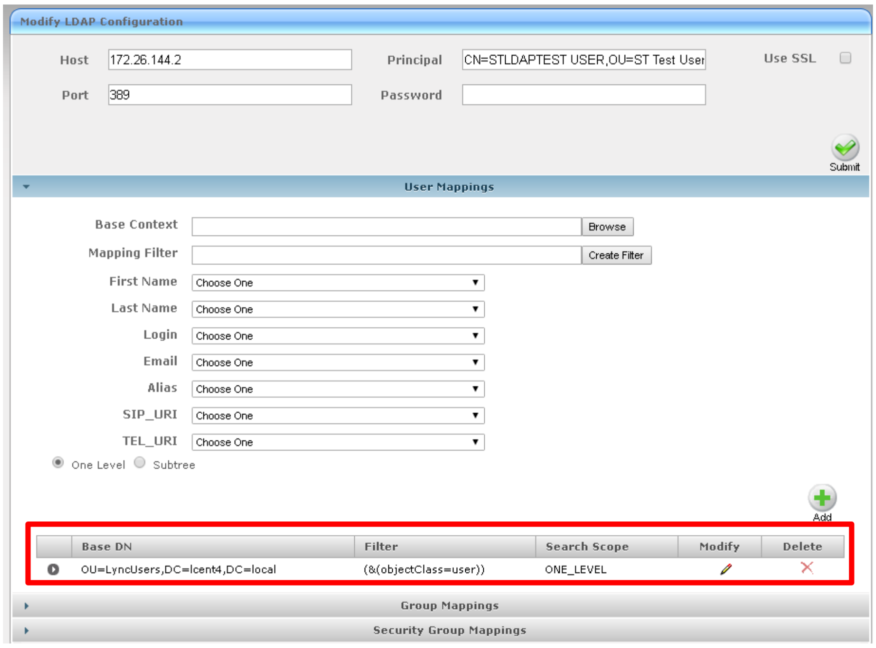
7. Scroll through the list and select the First Name, Last Name, Login, Email and Alias user attributes:
   - If you created any SmartTAP Attributes, they will appear in the list of user attributes as well.
   - Those attributes that were created with 'Network Mapping' defined will be used to trigger recording.
   - 'Ext' and 'SIP URI' in the image above are examples of SmartTAP User attributes added for recording purposes.
8. Map SmartTAP attributes to appropriate AD user attributes.

Figure 6-50: User Mappings



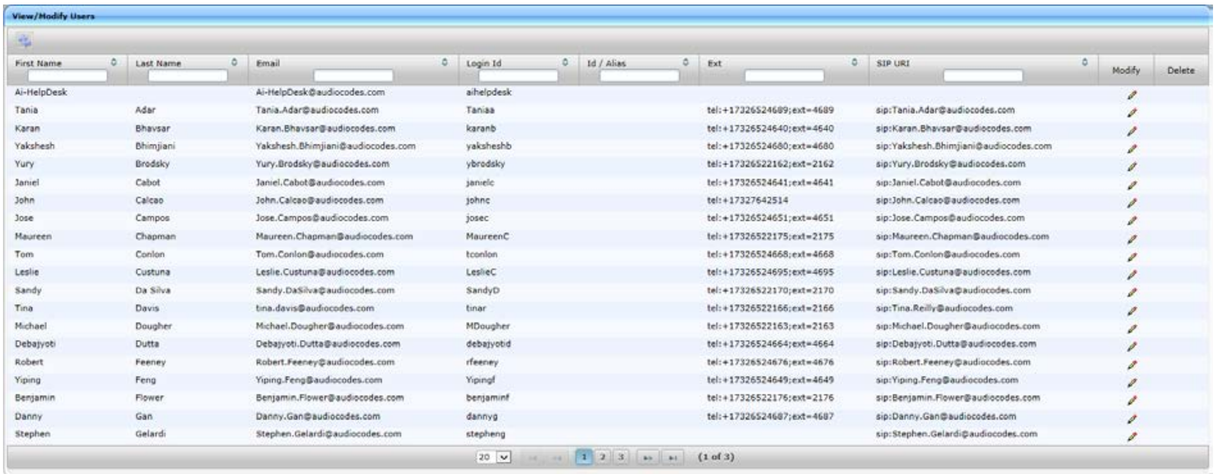
9. Click Submit to apply changes; the added User Mapping should be listed in the table as shown in the figure below.

Figure 6-51: LDAP Configuration – Added User Mapping



10. Add additional User Mappings as needed.
11. Go to the **User** tab (**Users** > **View/Modify Users**) to see the list of users added from the Active Directory.

Figure 6-52: View/Modify Users



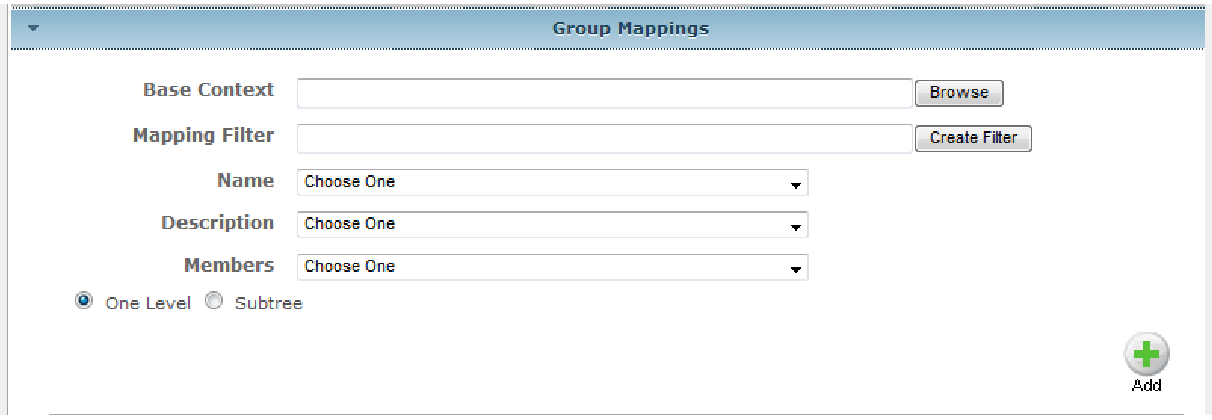
6.10.8.2 Configuring Group Mappings

The procedure below describes how to configure Group Mappings.

➢ **To configure Group Mappings:**

1. Open LDAP Providers screen (**System** tab > **System Setting** folder > **Add LDAP Config**).
2. Open the Group Mappings screen (click ▸ if necessary to expand screen).

Figure 6-53: Group Mappings



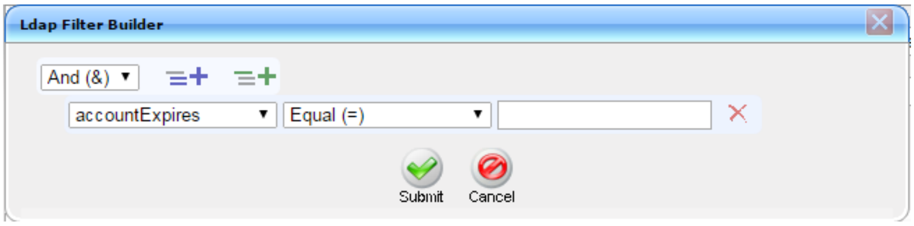
3. Use the table below as reference.

Table 6-21: Group Mappings - Field Descriptions

Field	Description
Group Mappings	▪ **Group Base Context** (LDAP path for groups) ▪ **Group Filter** (Create / Manage Group filter) ▪ **Name** (LDAP Attribute that maps to the group name) ▪ **Description** (LDAP Attribute that maps to the group description) ▪ **Members** (LDAP Attribute that maps to the group members. The members attribute should contain a collection of distinguished names of users that belong to the group). ▪ **One Level** – Retrieves LDAP attributes for the selected node. ▪ **Subtree** – Retrieves LDAP attributes for the selected node and all its child nodes in the LDAP directory tree. = expand screen  = shrink screen

4. Enter the Group Mappings Information in the 'Group Mappings' screen (i.e. (Groups,DC=qalabEE,DC=local)
5. Navigate to appropriate 'Group Path' and then click **Submit**.
6. Use filtering if you prefer not to add all groups.

Figure 6-54: Group Filter



- To add a Group Filter:
  a. Select the appropriate Conditional Operator (And, Or, Not).
  b. Select the appropriate Attribute.
  c. Select the appropriate Equality Operator (>=, =, ~=, <=).
  d. Specify a value.
  e. Click  to apply changes.

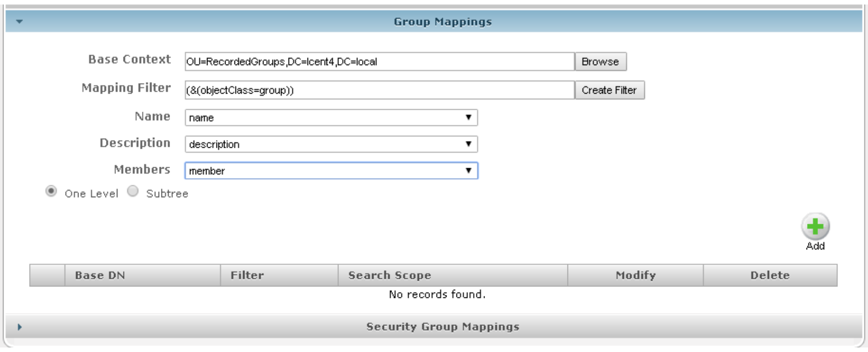
f. Click the  icon to add an additional filter and repeat the above filter steps.

g. Click the  icon to add a Sub filter and repeat the above filter steps.

7. Click  to apply changes.

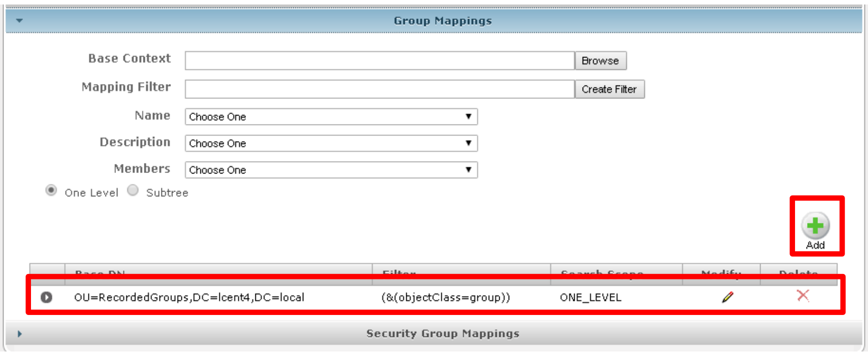
8. Scroll through the list and select the Name, Description and Members attributes.

Figure 6-55: User Mappings - Group Mappings



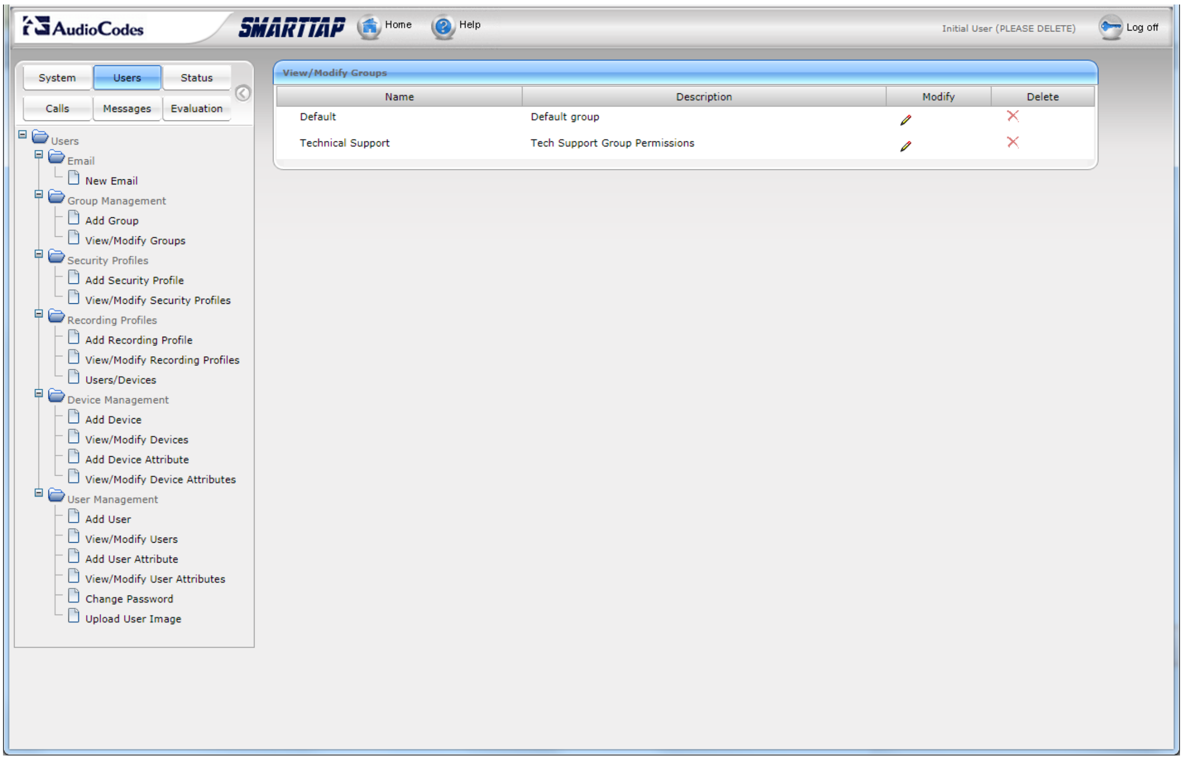
9. Click  to apply changes; view the listed group in the table as shown in the figure below.

Figure 6-56: User Mappings - Group Mappings



10. Click the **Users** tab (**Group Management** > **View/Modify Groups**) to see the list of groups added from the Active Directory. If you only see the 'Default' group listed in the table, the group mapping is incorrect.

Figure 6-57: View/Modify Groups



6.10.8.3 Configuring Security Group Mappings

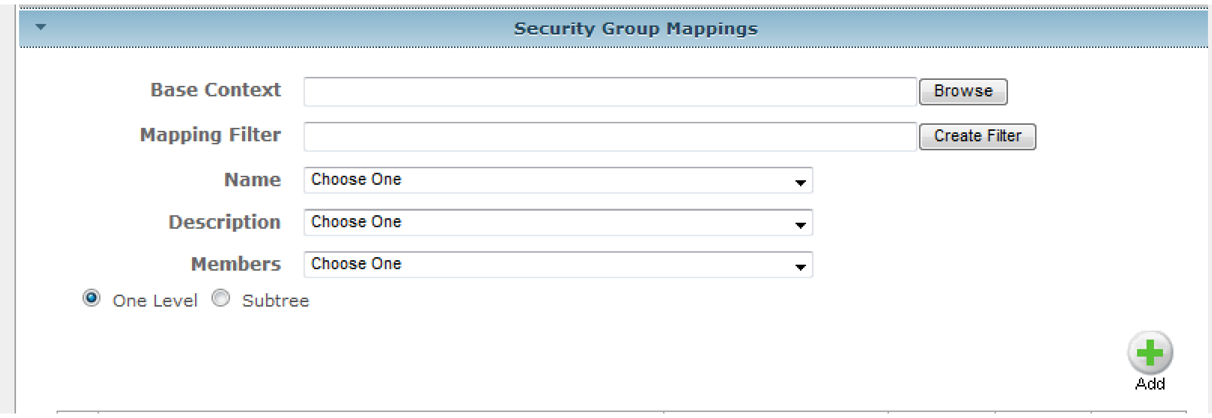
This section shows how to configure Security Group Mappings. All mapped Active Directory security groups automatically become SmartTAP Security Profiles.

Note: By default, new security profiles are granted *no* SmartTAP permissions.

➢ **To configure Security Group Mappings:**

1. Open the LDAP Providers screen (**System** tab > **System Setting** > **LDAP Providers**).
2. Open the Security Group Mappings screen (click if necessary to expand the screen).

Figure 6-58: Security Group Mappings



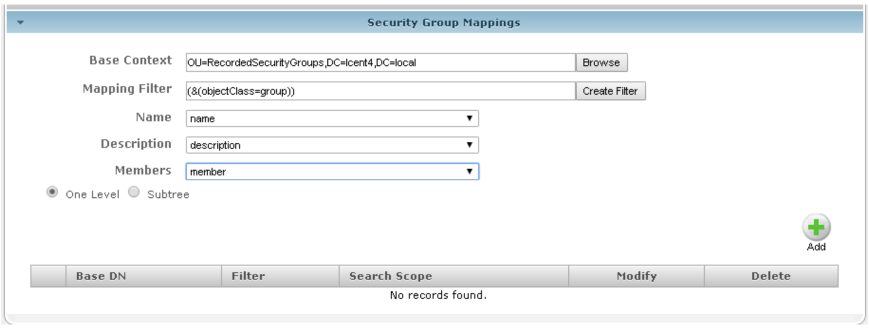
3. Enter the Security Group Mappings Information in the Security Group Mappings screen. Use the table below as reference.

Table 6-22: Security Group Mapping – Field Descriptions

Field	Description
Security Group Mappings	▪ **Security Groups Base Context** (LDAP path for security groups) ▪ **Group Filter** (Create / Manage Security Group filter) ▪ **Name** (LDAP Attribute that maps to the security group name) ▪ **Description** (LDAP Attribute that maps to the security group description) ▪ **Members** (LDAP Attribute that maps to the security group members. The members attribute should contain a collection of distinguished names of users that belong to the group.) ▪ **One Level** -Retrieves LDAP attributes for the selected node. ▪ **Subtree** – Retrieves LDAP attributes for the selected node and all its child nodes in the LDAP directory tree. Expand screen Shrink screen

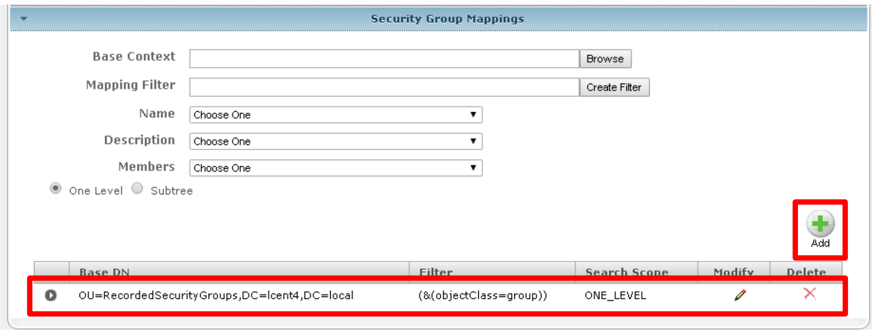
4. Use filtering if you prefer not to add all security groups.

Figure 6-59: Security Group Mappings



5. Click  to apply changes.

Figure 6-60: Security Group Mappings



6. Click the **Add** button to easily add additional Security Group Mappings.

6.11 Managing Users

This section describes how to access features and subfolders for User/Device Provisioning, Email, Group Management, Security Profiles, Recording Device Management, and User Management.

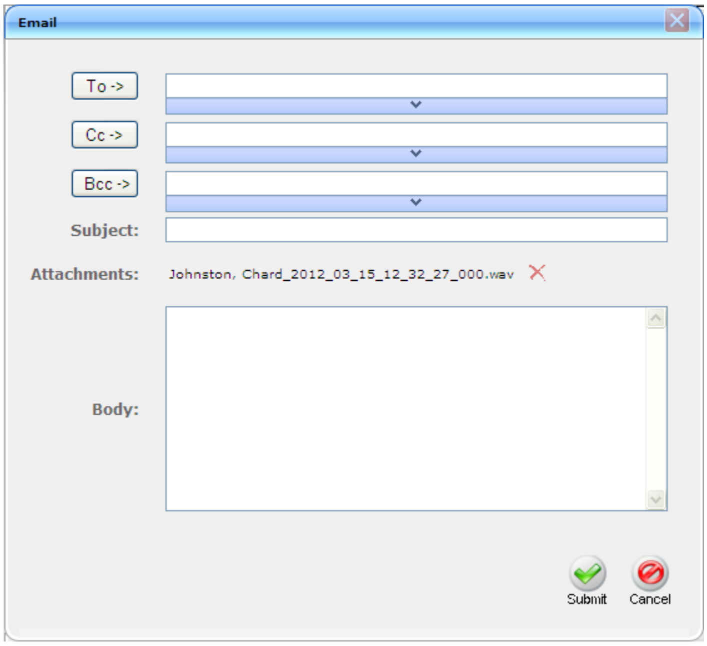
6.11.1 Configuring Email

The Email screen allows the network administrator to send emails directly from the SmartTAP GUI.

➢ **To configure Email:**

1. Open the Email screen.

Figure 6-61: Email



2. Configure the fields using the table below as reference.

Table 6-23: Email Field Descriptions

Field	Description
To > Cc > Bcc >	Clicking the **To>**, **Cc>**, **Bcc>** buttons will expand and collapse the list of users within the current user's group(s). Selecting/deselecting users from this list will add/remove them from the recipient list is a comma separated list of email addresses of the format 'jsmith@example.com'. The recipient list may also include the display name of the recipient. To add a display name for a recipient, the recipient's email address should be surrounded by angle brackets; for example: 'John Smith <jsmith@example.com>'
Subject	Subject of the email.
Attachments	List of attachments to be included with the email. Clicking **X** adjacent to the attachment removes the attachment from the email.
Body	Body of the email.
 Submit	Sends the email.

Field	Description
 Cancel	Cancels the email.

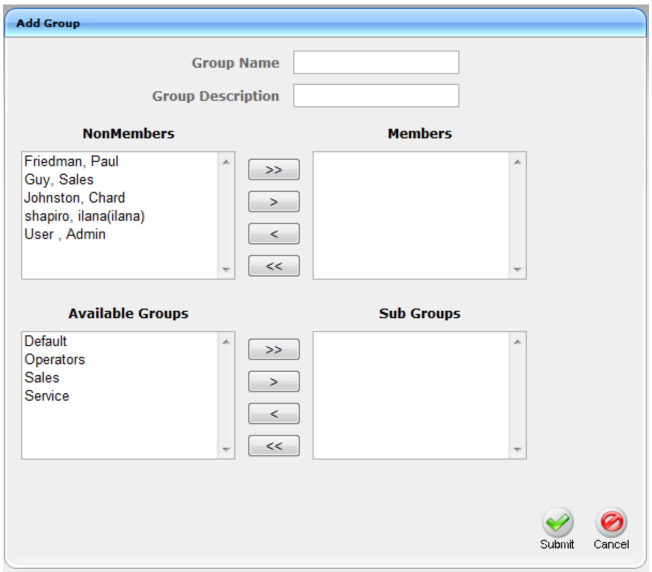
6.11.2 Managing Groups

This section describes how to create, modify and delete groups and sub groups.

➢ **To add a Group and associated sub groups:**

1. Open the **Add Group** screen.

Figure 6-62: Add Group



Use the table below as reference.

Table 6-24: Group Screen Settings

Field	Description
Group Name	Name of group to add.
Group Description	Description of the group to add.
NonMembers	Users that are not group members. Select users by clicking the user name; multiple users while holding <ctrl>; or all within a range by clicking top user and bottom user while holding <shift>
>>	Add all NonMembers to the Members group.
>	Add selected NonMembers to the Members group.
<	Remove selected Members from the Members group.
<<	Remove all Members from the Members group.
Available Groups	List of existing groups. Select groups by clicking the group name; multiple groups while holding <ctrl>; or all within a range by clicking top group and bottom group while holding <shift>
Sub Groups	List of Sub Groups of the group to add.

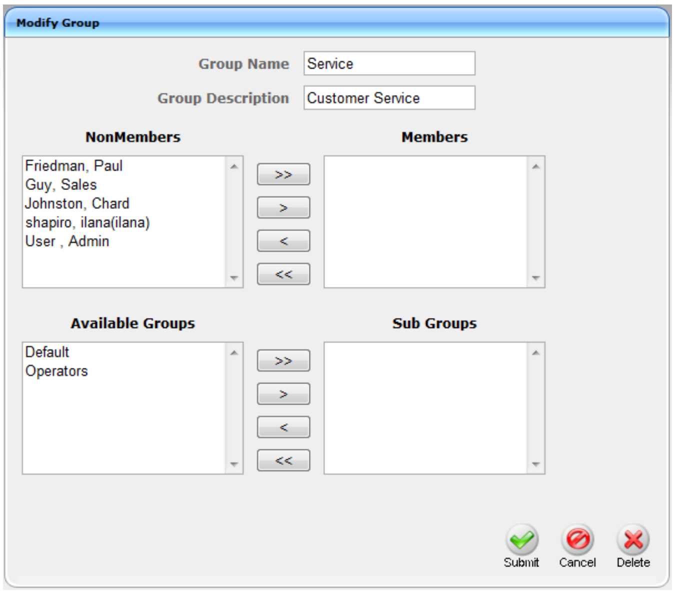
Field	Description
Members	Users that are members of the group. Select users by clicking the user name; multiple users while holding <ctrl>; or all within a range by clicking top user and bottom user while holding <shift>
Submit	Apply the changes.
Cancel	Cancel changes
Delete	Delete Group – displayed only when you modify an existing group.

2. Enter the **Group Name**.
3. Enter the **Group Description**.
4. From the list of NonMembers select the users and move them to the Members side by clicking the buttons in between the NonMembers and Members windows.
5. (Optionally, Sub Groups for the Group just being added can be entered from the Add Group screen).
6. Click **Submit**.

➢ To view/modify a Group:

1. Open the screen View/Modify Group screen as shown in the figure below.

Figure 6-63: View/Modify Group



- In this screen you can change or delete existing groups. Use the table below as reference.

Table 6-25: View/Modify Groups – Field Descriptions

Field	Description
Name	Group name displayed. Clicking ▶ to the left of the Name expands the group to show the sub groups.
Description	Description of the group displayed
Modify ( )	Click to modify the group.
Delete ( )	Click to delete the group.

➢ To modify/delete a group:

1. In the Modify Group screen, change the Membership by moving users to/from the Members window.
2. Change the Sub Groups by moving Groups to/from the Sub Groups window.
3. Click the **Submit** button to apply changes, or click the **Delete** button to delete the group.

6.11.3 Managing Security Profiles

This section describes how to create, view, modify and delete security profiles.

➢ To add a Security Profile:

1. Open the Add Security Profile screen.

Figure 6-64: Add Security Profile

2. Use the table below as reference.

Table 6-26: Security Profile Settings

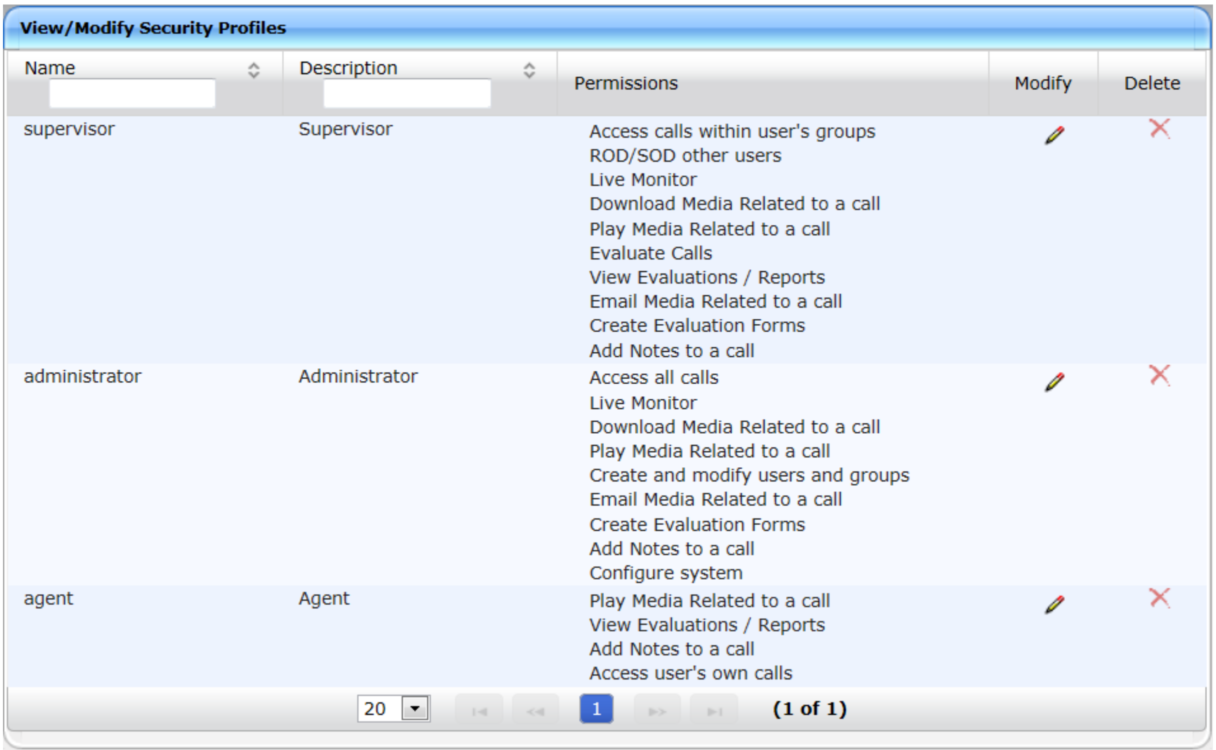
Field	Description
Security Profile Name	The name of the new security profile.
Security Profile Description	Description of the new security profile.
No Call Access	Select this option to prevent users with this security profile from accessing call data.
Access all calls	Select this option to allow users with this security profile to access calls for all users and devices.
Access calls within user's groups	Select this option to allow users with this security profile to access calls for all users within all the groups and sub groups of the group hierarchy to which they are a member.
Access user's own calls	Select this option to allow users with this security profile to access their calls.
Play Media Related to a call	Check this option to allow users with this security profile to play calls to which they have access.
Download Media Related to a call	Check this option to allow users with this security profile to download media for calls to which they have access.
Email Media Related to a call	Check this option to allow users with this security profile to email media for calls to which they have access.
Tag Calls	Check this option to allow users with this security profile to add Call Tags to calls to which they have access.
Live Monitor	Check this option to allow users with this security profile to live monitor calls to which they have access.
Evaluate Calls	Check this option to allow users with this security profile to evaluate calls to which they have access. Perform evaluation of another user or their own call
View Evaluations / Reports	Check this option to allow users with this security profile view completed evaluations or run reports for evaluations to which they have access.
ROD/SOD other users	Check this option to allow a user to Record or Save on Demand another user's calls. The user to be recorded must be in the same group as the initiator
Configure System	Check this option to allow users with this security profile to view and modify system configuration settings.
Create and modify users and groups	Check this option to allow users with this security profile to create and modify users, groups, and security profiles.
Create Evaluation Forms	Check this option to allow users with this security profile access to the SmartTAP Web interface.
Submit	Apply changes.
Cancel	Cancel changes.
Delete	Delete Security Profile – displayed only when you modify an existing profile.

3. Enter the Security Profile Name.
4. Enter the Security Profile Description.
5. Select the **Call Permissions** option.
6. Selecting 'No Call Access' disables the permissions on the right side of the Call Permissions.
7. Select the configuration permissions at the bottom of the form.
8. Click **Submit**.

➢ To view/modify Security Profiles:

1. Open the View/Modify Security Profiles screen.

Figure 6-65: View/Modify Security Profiles



2. Use the table below as reference.

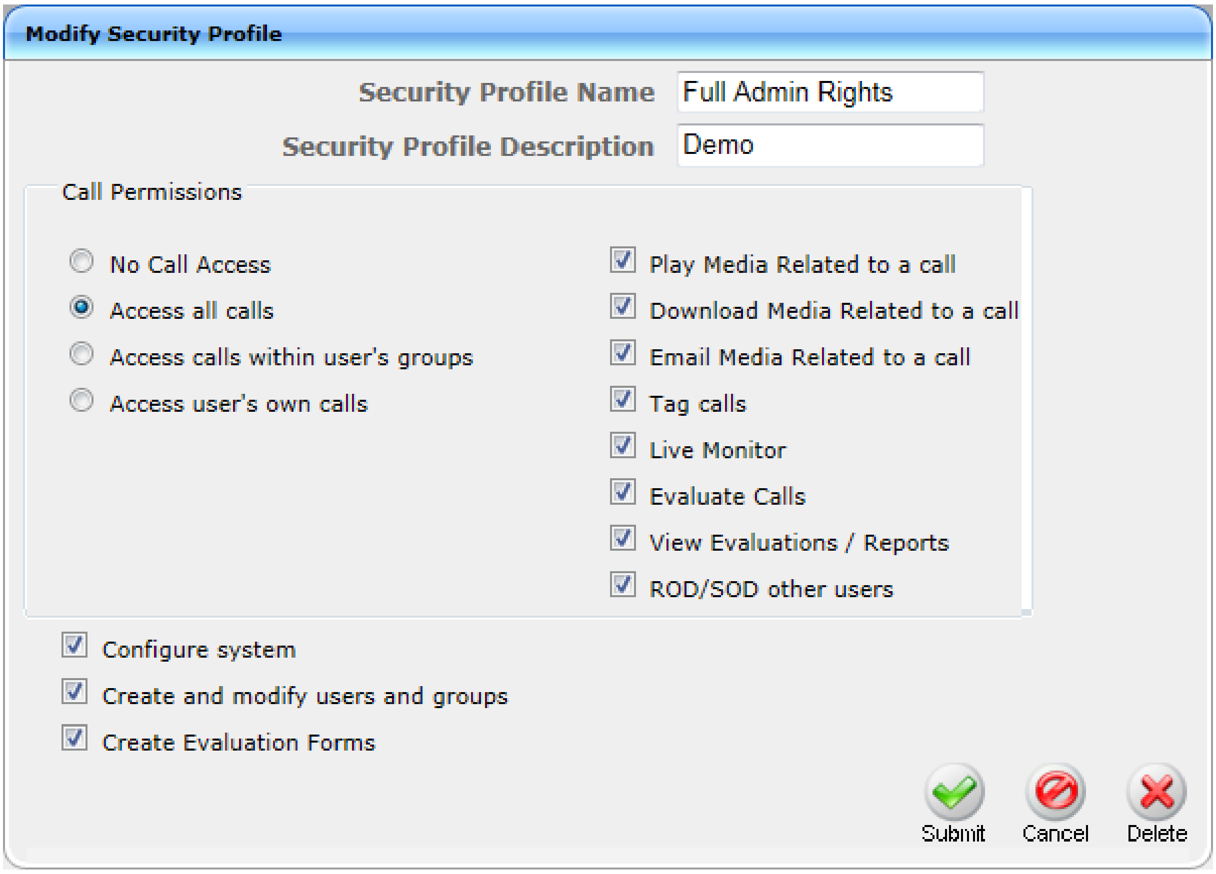
Table 6-27: View/Modify Security Profiles Main Screen

Field	Description
Name	Security Profile name sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.
Description	Security Profile description sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.
Permissions	List of permissions enabled for the Security Profile.
Modify ( )	Click to modify the Security Profile.
Delete ( )	Click to delete the Security Profile.

➢ To modify a Security Profile:

- Open the Modify Security Profile screen.

Figure 6-66: Modify Security Profile



The screen allows the administrator to control system access and permissions. The security profiles assigned to users allow a flexible means to manage access to SmartTAP resources.

6.11.4 Managing Recording Profiles

Recording profiles determine the method by which a user or device is recorded.
A profile may be assigned to one or more users or devices.

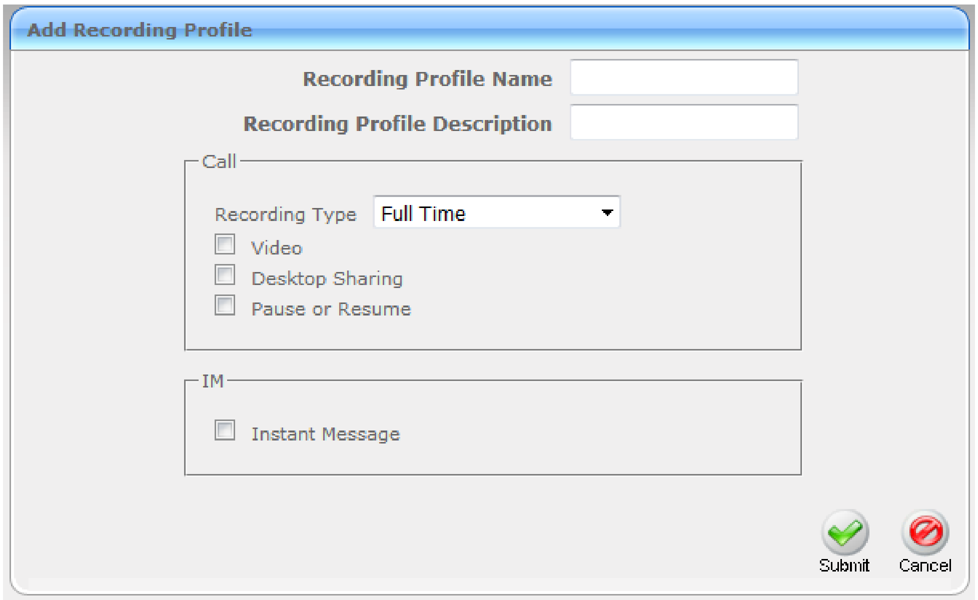
- **None** (default) – User is not recorded. Do not assign a recording profile to a user or device if you do not want to record them.
- **Full Time Recording** – Automatic Audio and/or Video recording
- **Record on Demand** – Audio recording is Manually Triggered from the GUI Status page or from the S4B / Lync CWE toolbar
- **Save on Demand** – Audio and/or Video recording is Manually Triggered from the GUI Status page or from the S4B / Lync CWE toolbar

For more information, see Appendix B

➢ **To add a Recording Profile:**

1. Under the User’s tab, Select 'Add Recording Profile'.

Figure 6-67: Add Recording Profile



2. Fill in the required fields using the table below as a reference.

Table 6-28: Recording Profiles

Field	Description
Profile Name	Enter a name for the new recording profile.
Profile Description	Enter a description of the new recording profile.
Recording Type	Select either: ▪ **Full Time** (supported for audio, video, instant messages and desktop sharing) automatic recording of complete call will begin from start of call with no user action required. ▪ **Record on Demand** (supported for audio) recording will commence from a specific point in the call that the user decided to record. ▪ **Save on Demand** (supported for audio, video, and desktop sharing) recording will contain audio and/or video from beginning of call, if the user decides to record the call.

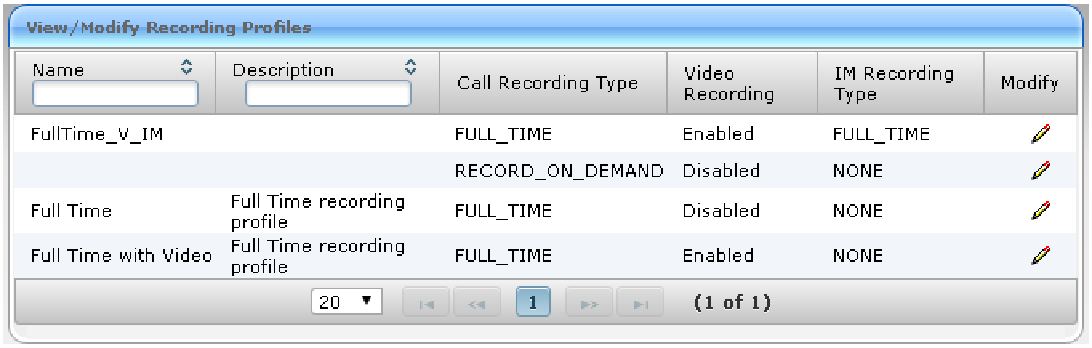
Field	Description
Video	Record a video call (Full Time or Save on Demand.)
Pause / Resume	[Optional] Select Pause / Resume audio recording during sensitive areas of the conversation with a customer, for example, when Credit Card details are given. The process is manual and executed from the Status page.
Instant Message	Automatic Instant Message recording.
Desktop Sharing Recording–	Recording of Desktop Sharing sessions
Submit	Apply the changes.
Cancel	Cancel the changes.

3. Click **Submit**.

➢ **To view/modify Recording Profiles:**

1. Open the View/Modify Recording Profiles screen as shown in the figure below.

Figure 6-68: View/Modify Recording Profiles



View/Modify Recording Profiles

Name	Description	Call Recording Type	Video Recording	IM Recording Type	Modify
FullTime_V_IM		FULL_TIME	Enabled	FULL_TIME	
		RECORD_ON_DEMAND	Disabled	NONE	
Full Time	Full Time recording profile	FULL_TIME	Disabled	NONE	
Full Time with Video	Full Time recording profile	FULL_TIME	Enabled	NONE	

20 ▼ 1 (1 of 1)

2. Use the table below as reference.

Table 6-29: View/Modify Recording Profiles – Field Descriptions

Field	Description
Name	Recording Profile name, sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.
Description	Recording Profile description sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.
Audio Recording Type	Full Time, Record on Demand or Save on Demand.
Video Recording Type	Full Time or Save on Demand.
IM Recording Type	Full Time or None
Desktop Sharing Recording	Full Time or Save on Demand
Modify ( )	Click to modify the Recording Profile.

➢ **To assign a recording profile to a User / Device account:**

- **Option method #1**:
  Add the recording profile to the account manually when the user account is created in SmartTAP. To create a new user account and assign a Recording Profile:
  1. Under the **User** tab, select **View/Modify Users**.
  2. Click the **Modify** icon.
  3. From the 'Recording Profile' dropdown, select the required profile (i.e., R.O.D).
  4. Click **Submit** to apply the changes.
- **Optional method #2**:
  Under the **User** tab, select **Recording Profiles | Users / Devices** to assign a single or bulk list of users / devices their recording profile.
  To manage a single or bulk assignment of recording profiles for existing user / device accounts:
  1. Under the **User** tab, select **Recording Profile | User / Devices**.
  2. Using the arrows, move single or bulk list of user / devices from the left screen to one of the recording profiles available.
  3. Click **Submit** to apply changes.

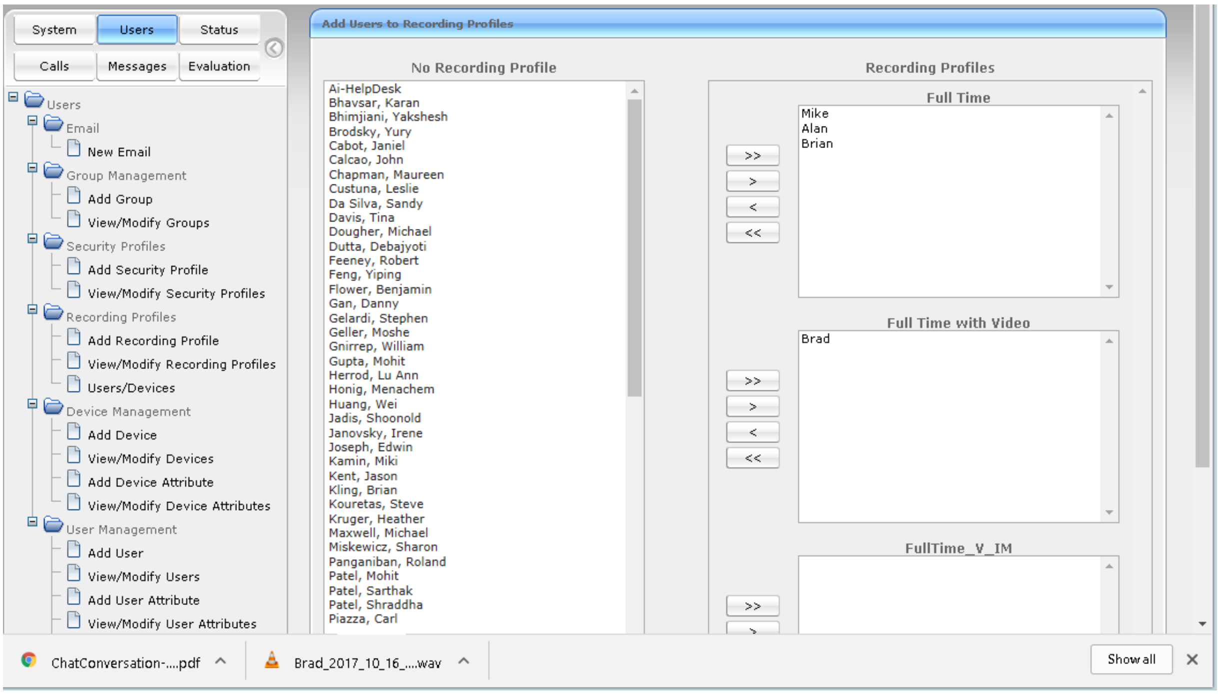
Note:

- By default, SmartTAP includes the 'Full Time' recording profile.
- All users imported from Active Directory will not have a recording profile assigned. Use optional method # 2 above to quickly assign multiple users the appropriate recording profile.

➢ To assign a single/multiple user(s)/device(s) to the appropriate recording profile:

1. Open the Add Users to Recording Profiles screen shown below.

Figure 6-69: Add Users to Recording Profiles



2. Use the table below as reference.

Table 6-30: Add Users to Recording Profiles Screen

Field	Description
No Recording Profile	List of available Users / Devices in SmartTAP unassigned to a specific recording profile.
Recording Profiles	Choose from one of the available recording profiles that were defined above to assign a User / Device (Full Time is the default profile)
>>	Add all available users / devices to a specific recording profile.
>	Add a user / device to a specific recording profile.
<	Remove a selected user / device from a specific recording profile.
<<	Remove a selected user / device from a specific recording profile.
Submit	Apply changes.
Cancel	Cancel changes.

Important:

- In addition to assigning a user / device with a recording profile, you must add a recording attribute and a targeting value.
- SmartTAP will use the added targeting value to trigger recording once detected in the call signaling.

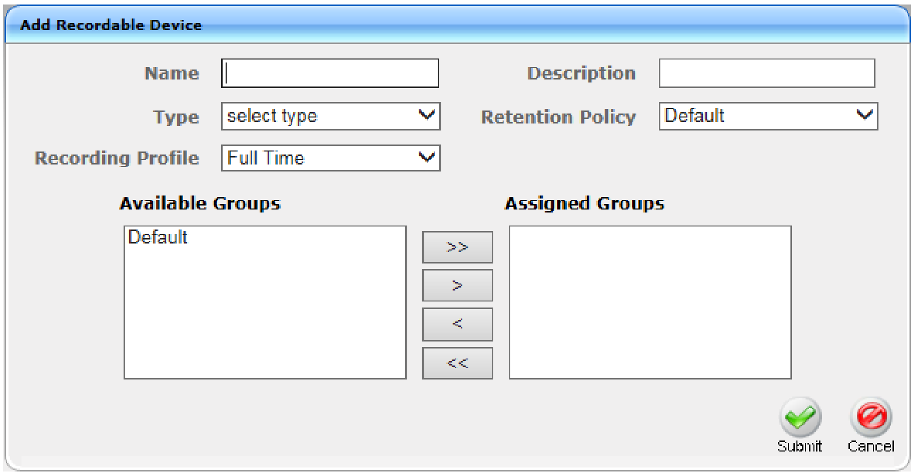
6.11.5 Managing Recordable Devices

This section shows how to manage recordable devices.

➢ **To add a Recordable Device:**

1. Open the Add Recordable Device screen as shown in the figure below.

Figure 6-70: Add Recordable Device



2. [Use the table below as reference] Enter a Name for the device.
3. Enter a Description for the device.
4. Select the Type from the dropdown menu.
5. From the list of Available Groups, select the groups and move them to the Assigned Groups by clicking the > / >> buttons.
6. Click **Submit** to apply changes.

Table 6-31: Recordable Device – Settings Descriptions

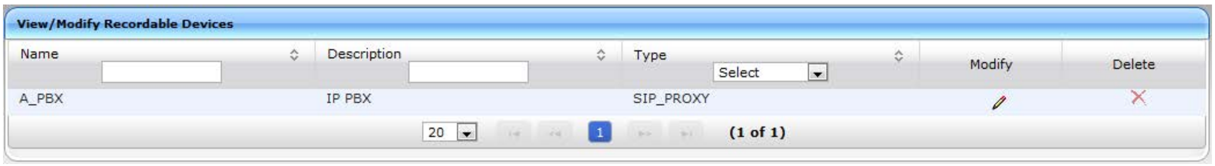
Field	Description
Name	Name of the new recordable device.
Description	Description of the new recordable device.
Type	Type of recordable device. Dropdown menu shows valid entries.
Retention Policy	Select an appropriate retention policy for the device.
Recording Profile	Select an appropriate recording profile for the device.
Available Groups	User groups available to assign to this device. Select groups by clicking the group name; multiple groups while holding <ctrl>; or all within a range by clicking top group and bottom group while holding <shift>.
Assigned Groups	User groups assigned to this device. Select group by clicking the group name; multiple groups while holding <ctrl>; or all within a range by clicking top group and bottom group while holding <shift>.
>>	Add all Available Groups to the Assigned groups.
>	Add selected Available Groups to the Assigned groups.
<	Remove selected Groups from the Assigned group.
<<	Remove all Groups from the Assigned group.

Field	Description
Submit	Apply the changes.
Cancel	Cancel the changes.
Delete	Delete Device – displayed only when you modify an existing profile.

➢ **To view/modify a Recordable Device:**

1. Open the View/Modify Recordable Device screen as shown in the figure below.

Figure 6-71: View/Modify Recordable Devices



2. Use the table below as reference.

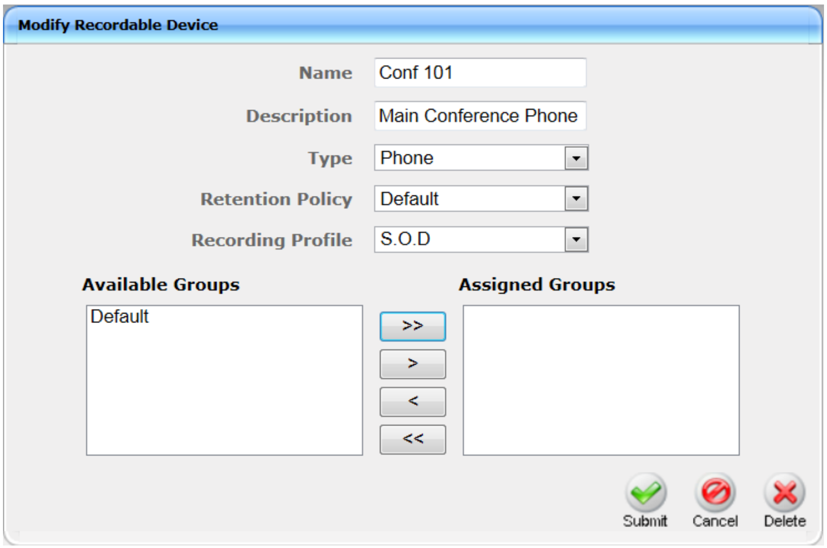
Table 6-32: View/Modify Recordable Devices – Field Descriptions

Field	Description
Name	Recordable device name sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.
Description	Recordable device description sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.
Type	Type of recordable device sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.
Modify ( )	Click to modify the Security Profile.
Delete ( )	Click to delete the Security Profile.

➢ **To modify a Recordable Device:**

■ Open the Modify Recordable Device screen. Use the table above as reference.

Figure 6-72: Modify Recordable Device



6.11.6 Adding a Device Attribute

This section shows how to add a SmartTAP device attribute. A device attribute has two purposes:

Table 6-33: SmartTAP Device Attribute's Two Purposes

Attribute Purpose	Priority	Description
Trigger Recording	Critical	To designate to SmartTAP what to use to trigger recording. (i.e., Add SIP_URI attribute and provide a value to be assigned to the device. If the device makes a SIP call, SmartTAP will trigger a recording based on the SIP_URI). See also below.
Provide Additional device Info	Optional	Add additional information to the device account within SmartTAP. (i.e. Ext, Tel URI, Mobile, etc.) for information purposes only. See also 'To add a general device attribute' below.

Enhance the integration by mapping SmartTAP attributes to Active Directory attributes to auto populate device information within SmartTAP. To map a device attribute to an Active Directory device attribute, see Section 6.10.60.

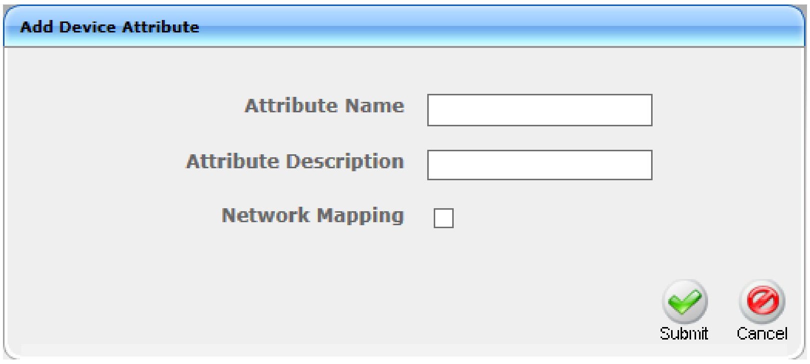
Table 6-34: User Attributes

User Attribute	Description
Name	Assign a unique easily identifiable name to the attribute.
Description	Include a brief description to explain the meaning of the attribute.
Network Mapping	Select the option in order to instruct SmartTAP to use the attribute for the purpose of recording any device.
Network Mapping Type	Instructs SmartTAP what type of attribute has been defined.

➢ To add a general device attribute:

1. [A general device attribute will not be used for recording purposes]. Under **Device Management** under the **User** tab, select **Add Device Attribute**.

Figure 6-73: Add Device Attribute



2. Enter the Attribute Name.
3. Enter the Attribute Description.
4. Leave the **Network Mapping** option cleared.
5. Click **Submit** to apply new device attribute or **Cancel** to exit.

➢ To add a device attribute for recording purposes:

1. Under Device Management under the **User** tab, select **Add Device Attribute**.
2. Enter the Attribute Name.
3. Enter the Attribute Description.
4. Check the **Network Mapping** option.
5. Select the appropriate Network Mapping type.
6. Click **Submit** to apply new device attribute or **Cancel** to exit.

Following are examples of device attributes created for recording purposes:

Figure 6-74: Add Device Attribute - Example 1

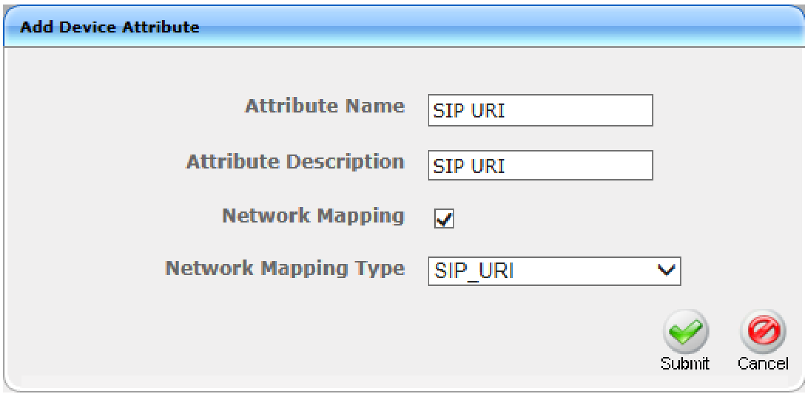
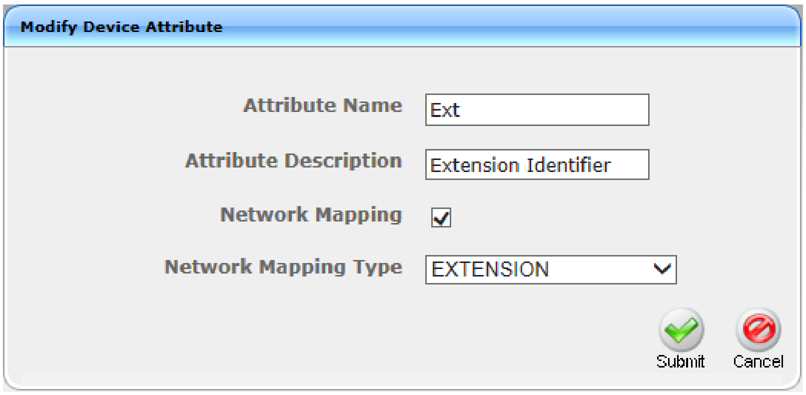


Figure 6-75: Add Device Attribute - Example 2



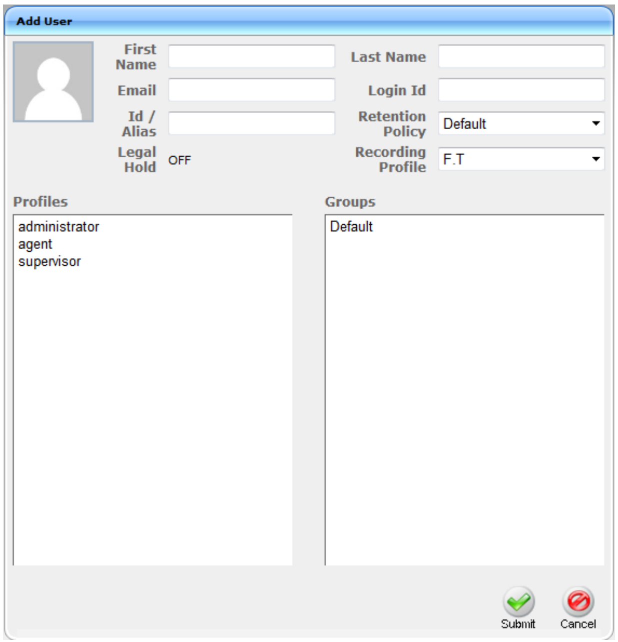
6.11.7 Managing Users

This section shows how to perform user management.

➢ **To add a user:**

1. Open the Add User screen.

Figure 6-76: Adding a User



2. Use the table below as reference.

Table 6-35: Adding a User

Field	Description
First Name	First name of the user.
Last Name	Last name of the user.
Email	Email of the user (must be valid as a new password is sent to this email).
Login Id	User login name.
Id / Alias	Free text (can be anything).
Retention Policy	Select an appropriate retention policy for the user.

Field	Description
Recording Profile	Select an appropriate recording profile for the user.
Security Profiles	Lists the Security Profiles that can be assigned to the user. Highlighted items indicate the Security Profiles that have been assigned to the user. To assign/or remove Security Profiles from the user, hold down the <crtl> key and click the Security Profiles name(s) to be added/or removed. To select a range of Security Profiles, hold down the <shift> key and click the Security Profile at the top of the range and then the Security profile at the bottom of the range.
Groups	Lists the groups that the user can be a member of. Highlighted items indicate the groups that the user is a member of. To assign/or remove a user from a group, hold down the <crtl> key and click the Group name(s) to add/or remove the user from. To select a range of Groups, hold down the <shift> key and click the Security Profile at the top of the range and then the Security profile at the bottom of the range.
	Reset Password – displayed only when modifying a user.
	Legal hold – the retention process will not delete a user's calls when the user is on legal hold. Available only when modifying a user.
 Submit	Apply the changes.
 Cancel	Cancel the changes.

- **To update an Admin User (optional):**

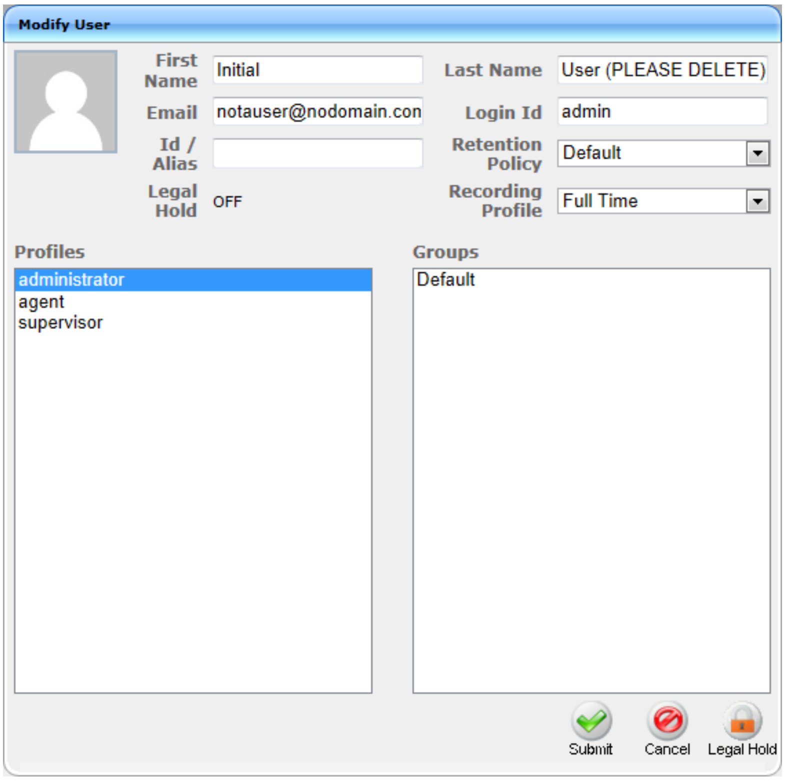
- After logging in, the 'admin' user can create a new administrator account or just edit the information and modify the password for this account.

Note: Configure SMTP before proceeding.

- **To modify / update an Admin User:**

1. Log in as user 'admin'.
2. Open the 'View/Modify Users' screen (**Users** tab > **User Management** folder > **View/Modify Users**).

Figure 6-77: Modify User



3. Update the user information (First name, Last name, Email, Login Id).
4. Make sure the email is a valid email.
5. Id/Alias is an optional text field that can be used to enter any data. For example, employee ID or nickname to help identify the user if there are multiple users with the same first & last name.

➢ To change the Password:

- Click the **Reset password** button  An email is sent to the Email address for this user with a new internally generated password.

Important:

- Make sure the new user successfully receives an email with password and logs into SmartTAP before modifying or deleting the default **admin** user account.
- Make sure the email with the new password is received before logging off. Resetting the admin user password prevents the user from logging into the system. In addition, it is recommended to add at least one other user with administrative privileges to avoid being locked out of the system.

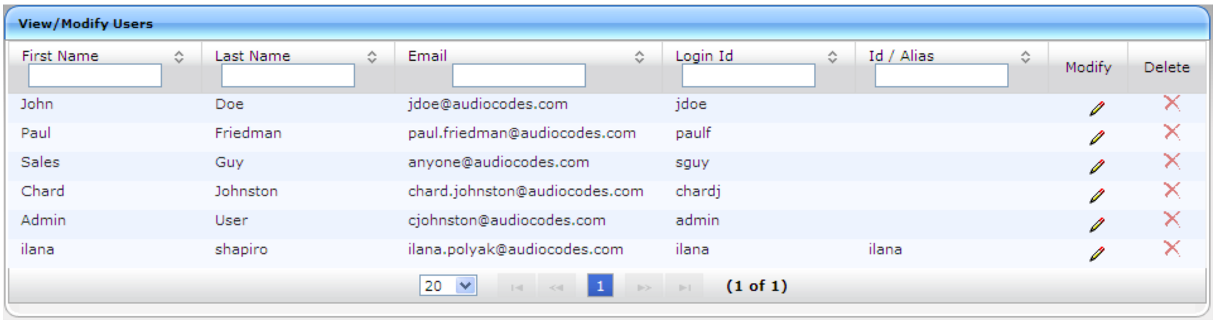
➢ **To add a new user:**

1. Open the Add User screen (**Users** tab > **Users** folder > **User Management** > **Add User**).
2. Enter the user's First Name.
3. Enter the user's Last Name.
4. Optionally enter the user's email (SmartTAP sends initial password to this email address).
5. Optionally enter ID / Alias (this is free-form text that can be used to enter the employee ID or any other data).
6. Select an appropriate retention policy for the user (Default: 'default').
7. Select an appropriate recording profile for the user (Default: 'None').
8. Select the security profile or profiles by highlighting them (see the notes on the Add User screen field descriptions, above, for how to select more than one profile).
9. Select the group or groups to which the new user is to be added.
10. Add the appropriate value to any attribute fields that are designated for recording.
11. If SmartTAP is configured for LDAP, any SmartTAP attributes mapped to AD attributes will be auto populated.
12. Click **Submit** to apply changes; a successful configuration results in a message in **green** font in the command execution Results area; a failed configuration results in a failure message encoded in **red** font in the command execution Results area.
    SmartTAP sends an email to the user with their login and initial password, assuming that an email was provided.

➢ To view/modify users:

1. Open the View/Modify Users screen.

Figure 6-78: View/Modify Users



2. Use the table below as reference.

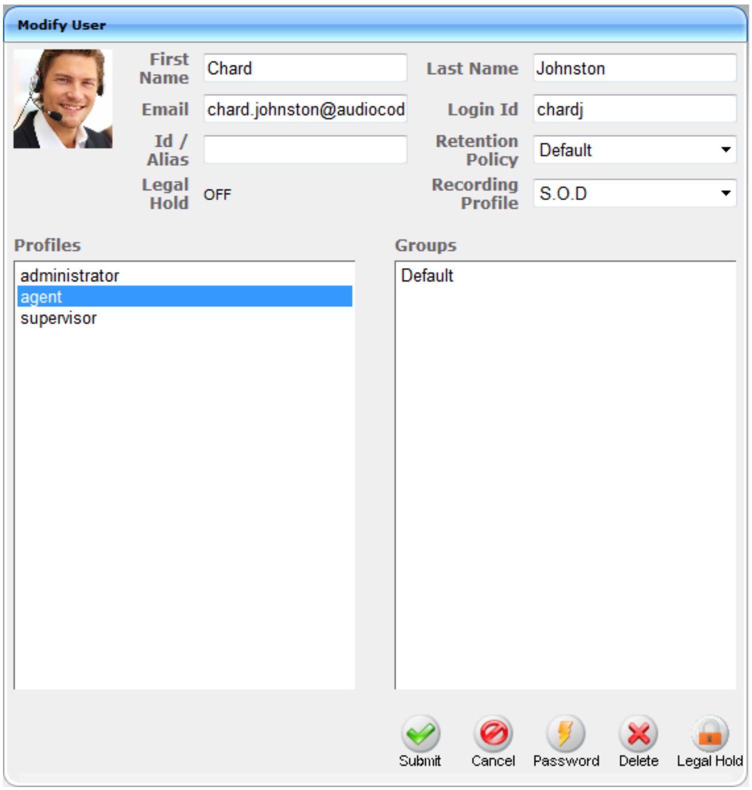
Table 6-36: View/Modify Users

Field	Description
First Name	User first name sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.
Last Name	User last name sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.
Email	User email address sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.
Login Id	User login ID sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.
Id / Alias	User ID / Alias sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.
Modify ( )	Click to modify the user.
Delete ( )	Click to delete the user.
Page Navigation buttons	Buttons are shortcuts to the beginning/end, previous/next page of displayed entries. The dropdown allows changing the number of entries per page.

➢ To modify a user:

1. Navigate to the **Users** tab > **Users** folder > **User Management** > **View/Modify Users**.
2. Open the Modify User screen by clicking **Modify** ( ) in the View/Modify User main screen display for the user to change.

Figure 6-79: View/Modify User



3. Modify the fields to change.
4. Click **Submit** to apply changes.

➢ To reset a user password:

Note: Only users who belong to profiles with 'Create and modify users and groups' privileges are allowed to reset other users' passwords. All users can reset their own passwords.

1. Open the View/Modify Users screen (**Users** tab > **Users** folder > **User Management** > **View/Modify Users**).
2. Open the Modify User screen by clicking **Modify** ( ) in the View/Modify User main screen display for the user to reset password.
3. Click the **Reset Password** button.

➢ To add a User Attribute:

A SmartTAP User attribute has two purposes:

Table 6-37: SmartTAP User Attribute's Two Purposes

Attribute Purpose	Priority	Description
Trigger Recording	Critical	To designate to SmartTAP what to use to trigger recording. (i.e., add a SIP_URI attribute and provide the value assigned to the user. If the User makes a SIP call, SmartTAP will trigger a recording based on SIP_URI). See 'To add a user attribute for recording purposes' below.
Provide Additional User Info	Optional	Add additional information to the User account within SmartTAP. (i.e., Ext, Tel URI, Mobile, etc.) for information purposes only. See 'To add a general user attribute' below.

Enhance the integration by mapping SmartTAP attributes to Active Directory attributes to auto populate user information within SmartTAP. To map a user attribute to an Active Directory user attribute, see Section 6.10.8.

Table 6-38: User Attributes

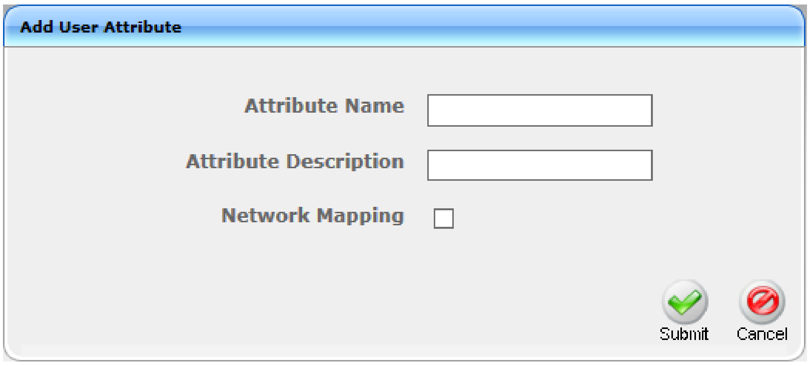
User Attribute	Description
Name	Assign a unique easily identifiable name to the attribute.
Description	Include a brief description to explain the meaning of the attribute.
Network Mapping	When checked, instructs SmartTAP to use the attribute for the purposes of recording. All users will be targeted for recording that have this attribute assigned with a value.
Network Mapping Type	Instructs SmartTAP what type of attribute has been defined.

➢ To add a general user attribute:

[A general user attribute will not be used for recording purposes].

1. Under User Management within the User's tab, select **Add User Attribute**.

Figure 6-80: Add User Attribute



2. Enter the Attribute Name.
3. Enter the Attribute Description.
4. Leave the **Network Mapping** option cleared.
5. Click **Submit** to apply new user attribute or **Cancel** to exit.

➢ To add a user attribute for recording purposes:

1. Under 'User Management' under the **User** tab, select **Add User Attribute**.
2. Enter the Attribute Name.
3. Enter the Attribute Description.
4. Select the **Network Mapping** option.
5. Select the appropriate Network Mapping type.
6. Click **Submit** to apply new user attribute or **Cancel** to exit.

The following are examples of user attributes created for recording purposes:

Figure 6-81: Example 1: Modify User Attribute

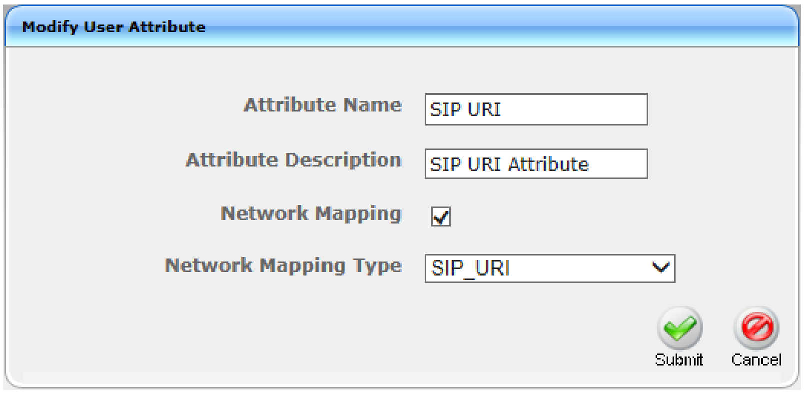
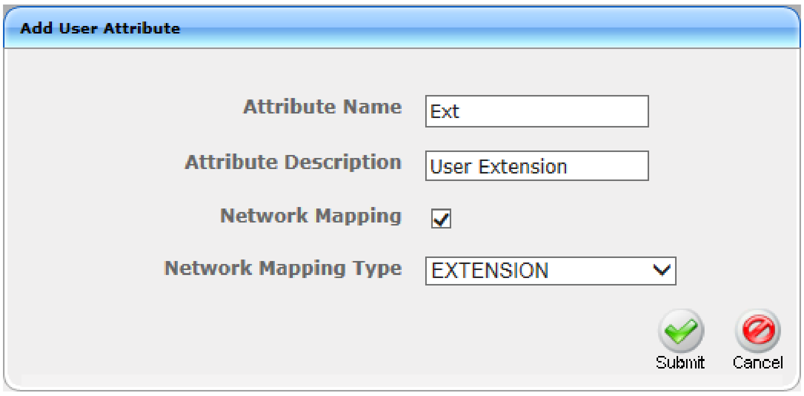


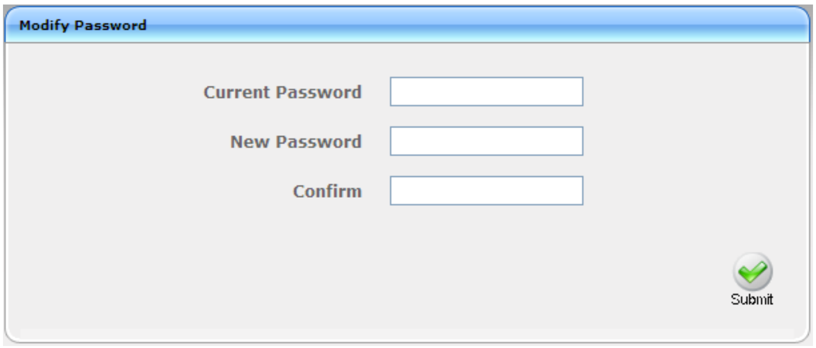
Figure 6-82: Example 2: Modify User Attribute



➢ To change your own password:

1. Open the Change Password screen (**Users** tab > **Users** folder > **User Management** > **Change Password**).

Figure 6-83: Change Password



2. [Use the table below as reference]. Enter the current password.
3. Enter the new password.
4. Confirm the new password.
5. Click **Submit** to change the password; the system automatically logs off and the user is required to log in with the new password.

Table 6-39: Change Password

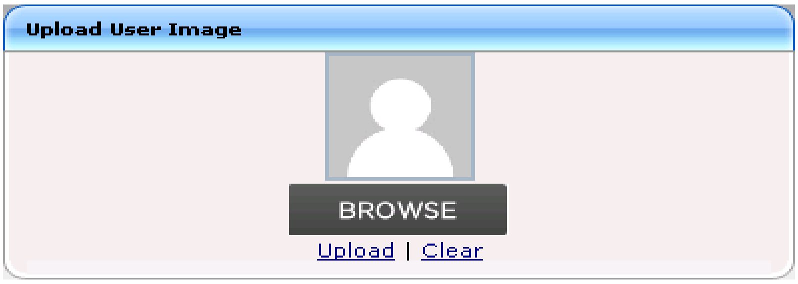
Field	Description
Current Password	Current password.
New Password	The password that will replace the current password.
Confirm	Reenter the new password.
Submit	Apply the changes.

Important: The only means to regain access to the SmartTAP system after a lost password, is by having a user with user Add/Modify privileges reset this user password.

➢ To upload an image:

Select this option to upload your own image.

Figure 6-84: Upload User Image



➢ To upload an image

1. Click the **Browse** button and navigate to the appropriate folder to select the image.
2. Click **Upload** to load the image or click **Clear** to select a different image.

Figure 6-85: Upload

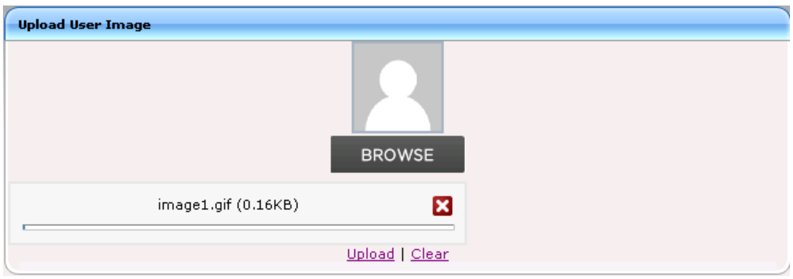


Figure 6-86: Upload Success

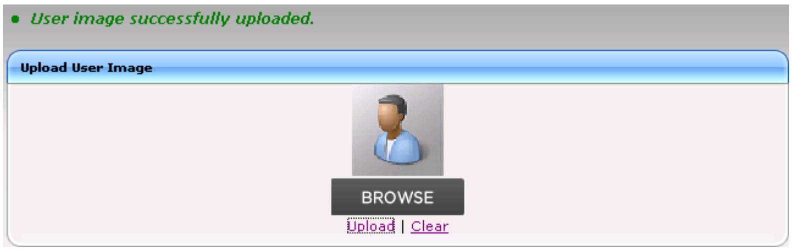
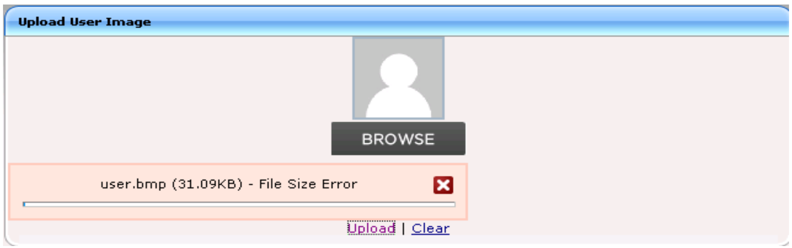


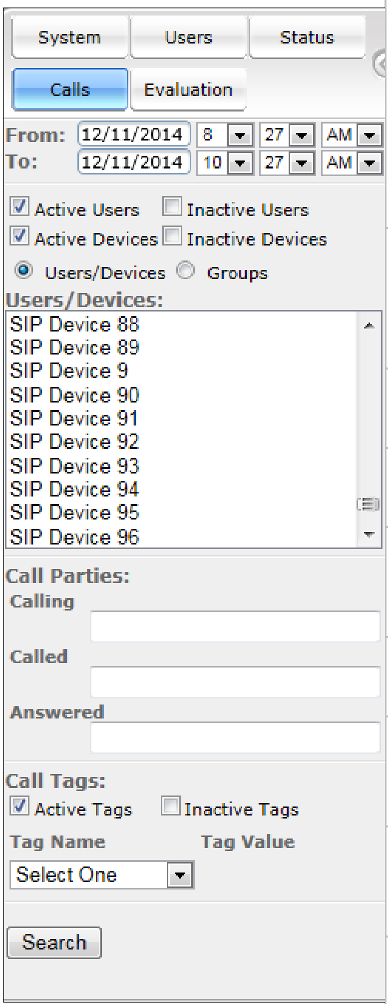
Figure 6-87: Upload Error



6.12 Managing Calls

This section shows how to manage calls. They're managed under the **Calls** tab in the Search Calls Navigation screen, shown and described below.

Table 6-40: Search Calls Navigation Screen - Calls Tab



Search Calls Navigation	Field	Description
	From:	Earliest date and time to search from. Click the date field for a calendar to pop up showing one month at a time. From the dropdown, change the time of day. **Note:** When searching for calls within a time range, only calls that start within the range are returned in the search results.
	To:	Latest date and time upon which to search. Click the date field for a calendar to pop up showing one month at a time. From the dropdown, change the time of day.
	Active Users	Users whose accounts are enabled in the SmartTAP system.
	Inactive Users	Users whose accounts have been deleted from the SmartTAP system.
	Active Devices	Devices that are not associated with users enabled in the SmartTAP system and can be targeted for recording.
	Inactive Devices	Devices that have been deleted from the SmartTAP system.
	Users/Devices	Only Users and Devices will be listed in the search list. Either the **Users/Devices** or the **Groups** option must be selected.
	Groups	Only Groups will be listed in the search list. Either the **Users/Devices** or the **Groups** option must be selected.
	User/Devices: (list)	To select multiple Users/Devices, highlight the name; multiple Users/Devices while holding <ctrl>; or all within a range by clicking top User/Device and bottom User/Device while holding <shift>.
	Call Parties: Calling Called Answered	Enhance the search by specifying the Calling (Caller ID), Called and/or Answering party. Use a wild card to broaden the search Example *732* will return all calls with 732 anywhere in the number 732* will return all calls that start with 732 *Bill will return all calls with a user participant with a name that contains the word 'Bill'.
	Call Tags	Select one or more Tags and provide a value to enhance search.
	Search	Click to search and display results.

6.12.1 Searching for Calls

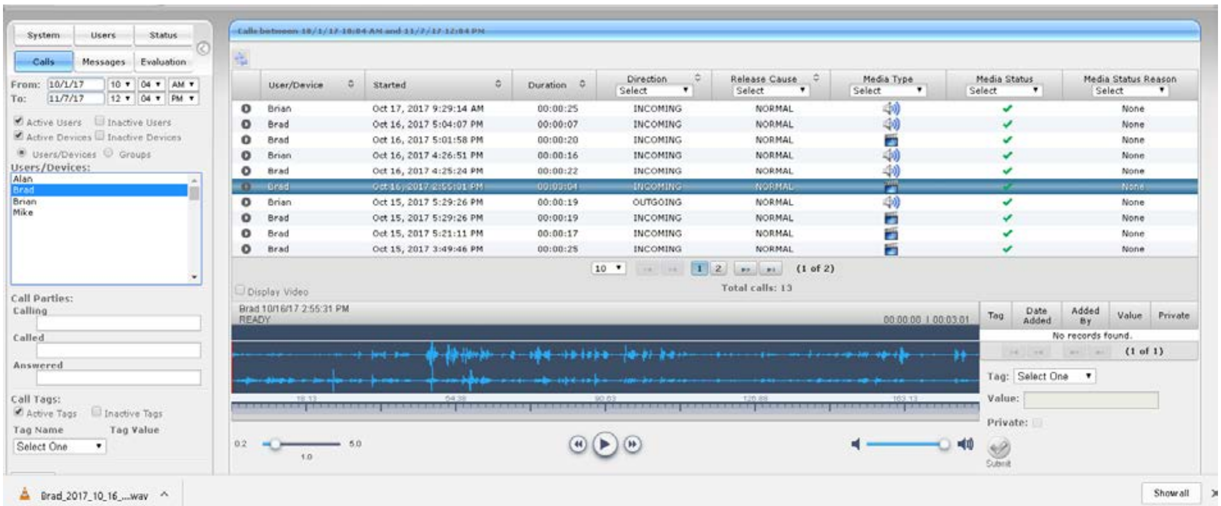
This section shows how to search for calls.

> **Note:** The search fields' logical operations are:
>
> Selected Users/Devices or Users/Devices within selected Groups
> **AND**
> Call Parties
> **AND**
> Call Tags
>
> where Call Parties Calling, Called, Answered are logically **OR**ed
> and Call Tags (Call Tag1 … Call TagN) are logically **OR**ed.

➢ **To search for calls:**

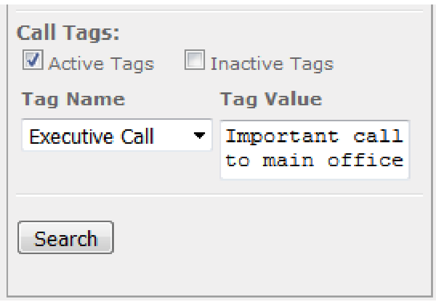
1. Open the Search Calls screen by clicking the **Calls** tab.
2. In the Search Navigation screen (left side of the screen), enter a time range; only calls that start within the time range will be returned in the search results.
3. Select the type of Users and Devices.
4. Select either the **Users/Devices** or **Groups Radio** button.
5. Selecting the **User/Devices** option changes the display below to show a list of Users/Devices.
6. Selecting the **Groups** option changes the display below to show a list of Groups and Sub Groups (if the **Search Sub Groups** option is selected).
7. Select one of more User/Devices or Groups by highlighting them in the list (see notes on Search Calls Navigation screen field descriptions above on how to select more than one User/Device or Group).
8. Optionally, specify a Calling, Called and/or Answered party.
9. Click Search to start the search for calls matching the search criteria; the Results are displayed in the Search Calls Results screen to the right. The figure below shows a list of retrieved calls for a specific users "Brad" and "Brian".

Figure 6-88: Retrieved Calls List for Specific User



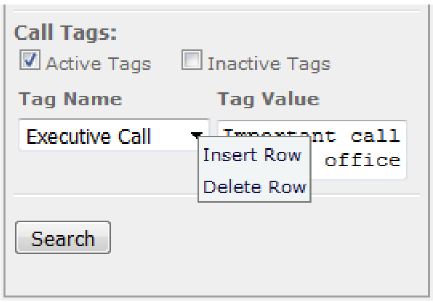
10. Optionally, specify a Call Tag & Value.

Figure 6-89: Call Tags



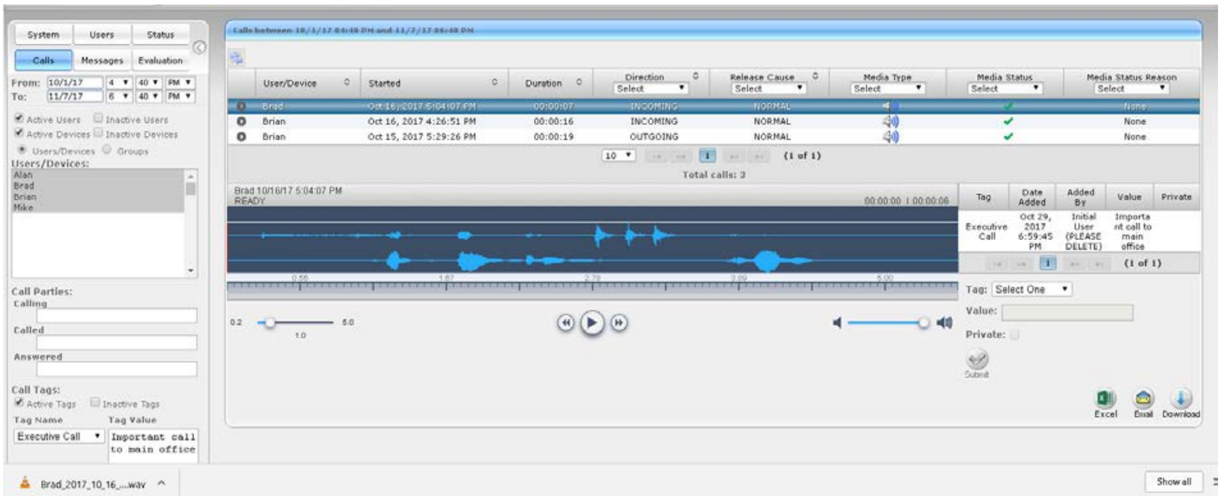
11. Right click the initial tag row to 'Insert' or 'Delete' an existing tag from the search. Add additional search tags as needed to fine tune the search.

Figure 6-90: Call Tags



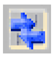
12. Click Search to start the search for calls matching the search criteria; the Results are displayed in the Search Calls Results screen to the right. Figure 6-91 below shows a Call Tag example of the Search Calls Results screen with Call Tag 'Executive Call' value * Important call to main office * for users “Brad” and “Brian”. Note that only calls with Call Tag 'Executive Call' with matching note value ' Important call to main office ' will meet the search conditions.

Figure 6-91: Search Calls Results



Important: Notice the difference in the search results displayed in Figure 6-91 and how wild cards can affect the results.

Table 6-41: Search Calls Results

Field	Description
	Launches the Add and Remove Columns dialog.
User/Device	User/Device name. Clicking this header sorts the search results in Ascending/Descending order alternating with each click.
Started	Date and time the call recording started. Clicking this header sorts the search results in Ascending/Descending order alternating with each click.
Duration	Call Duration. Clicking this header sorts the search results in Ascending/Descending order alternating with each click.
Direction	The column represents Call Direction (Incoming, Outgoing). Clicking this header sorts the search results in Ascending/Descending order alternating with each click. Dropdown entry shows only the matching results.
Release Cause	Release cause for the call. Clicking this header sorts the search results in Ascending/Descending order alternating with each click. Dropdown entry shows only the matching results.
Media Type	Indicates the media type. One of the following values: • **Audio:** the Speaker icon is displayed in this column for a recorded audio call. No icon is displayed for a non-answered call. • **Video:** the Video icon is displayed in this column for a recorded video call. No icon is displayed for a non-answered call. • **Skype for Business Desktop Application (Desktop SharingS):** the Desktop Sharing call icon is displayed. No icon is displayed for a non-answered call. • None
	Indicates that the call audio has been successfully recorded.
	Indicates that the call video has been successfully recorded.
	Indicates that the Desktop Sharin has been successfully recorded.
Expires	Call recording expiration date. The date after which the call recording is purged. The date is calculated based on the retention profile assigned to the call. If the call was put on legal hold or evaluated, the expiration date is presented along with a lock icon. The Expires field has a value only when during the call the associated user had retention policy assigned to it and the period of the policy was set to a larger than 0 value (0 is default implying that calls should never expire).
Notes	There are no notes associated with this call. There are notes associated with this call. Notes are displayed adjacent to the Player screen as highlighted in the figure above with the note example “Executive Call”.
Display Video	Displays the video screen. When you select the  button, the recorded video is replayed.
System Call ID	Indicates the Original Call ID. Applicable to Skype For Business and other SIP-related integrations. This ID can be used to correlate call records to the original calls.

Field	Description
Conversation ID	Indicates the Skype For Business Conversation ID. This ID can be used to correlate between audio/video and content sharing calls made by a user from SFB client as part of one conversation.
Conference ID	Indicates the Skype For Business Conference ID. This ID identifies the conference to which the call was connected. It can be used to correlate between audio/video and content sharing calls made by a user from a SFB client.
Media Status	**Corresponding Media Reason**
None	**None** - Indicated when there are no media files and the call was not answered i.e. Abandoned or Missed.
(OK)	**None –** There are no reasons.
(Warning	**Silent Media** – Indicated when media files associated with the call are silent as a result of not receiving RTP packets.
(Error)	• **No Media** – Indicated when there are no media files associated with the call; however, the call was answered. • **No License** - Indicated when the media cannot record as a result of no licenses being available.

➢ To filter search results:

- Click a column heading to sort A-Z or Z-A.
- To apply additional filters, type into the text box below the column heading where applicable.
- Use a * wild card to enhance the filter.
- Filter 'abc' will search the field for any string that starts with 'abc'.
- Filter '*abc' will search the field for any position within the string to match 'abc'.

➢ To add/remove columns from the Search Call Results:

Figure 6-92: Add/Remove Columns from the Search Call Results Screen

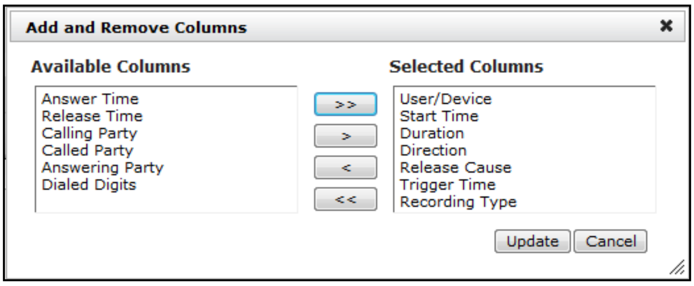


Table 6-42: Add and Remove Columns – Field Descriptions

Field	Description
Available Columns	List of columns that can be added to the search results table.
Selected Columns	List of columns that will be displayed in the search results table.
>>	Moves all items from the Available Columns list to the Selected Columns list.
>	Moves the selected item(s) from the Available Columns list to the Selected Columns list, effectively adding the column to the search results table.

Field	Description
<	Moves the selected item(s) from the Selected Columns list to the Available Columns list, effectively removing the column from the search results table.
<<	Moves all items from the Selected Columns list to the Available Columns list, effectively removing all columns from the search results table.
Update	Applies changes and closes the screen.
Cancel	Cancels changes and closes the screen.

➢ To add/remove columns from the Search Call Results

1. Click the button in the 'Search Calls' results screen to open the 'Add and Remove Columns' dialog.
2. Move the Columns to display to the 'Select Columns' side of the screen. Use Table 6-43 as reference.
3. Click **Update** to apply the changes and close the screen.

Table 6-43: Add and Remove Columns

<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td>User / Device</td><td colspan="2">Targeted User or Device.</td></tr>
<tr><td>Start Time</td><td colspan="2">Initial off-hook or offering of the call.</td></tr>
<tr><td>Answer Time</td><td colspan="2">The time at which the call was answered.</td></tr>
<tr><td>Release Time</td><td colspan="2">The time at which the call was disconnected.</td></tr>
<tr><td>Trigger Time</td><td colspan="2">The time at which the user manually initiated Record or Save on Demand.</td></tr>
<tr><td>Duration</td><td colspan="2">Total duration of the call, from the Start Time to the Release Time.</td></tr>
<tr><td>Calling Party</td><td colspan="2">The call initiator.</td></tr>
<tr><td>Called Party</td><td colspan="2">The intended recipient of the call.</td></tr>
<tr><td>Answering Party</td><td colspan="2">The party who ultimately answered the call.</td></tr>
<tr><td>Dialed Digits</td><td colspan="2">Any dialed digits to set up the call (not supported or required for SIP or Microsoft Lync).</td></tr>
<tr><td>Direction</td><td colspan="2">Inbound or Outbound.</td></tr>
<tr><td rowspan="5">Release Cause</td><td>Normal</td><td>Answered call.</td></tr>
<tr><td>Missed</td><td>Incoming call to targeted user that wasn’t answered.</td></tr>
<tr><td>Abandoned</td><td>Outgoing call from targeted user that wasn’t completed.</td></tr>
<tr><td>Conferenced *</td><td>Indicates the call leg was released as a result of the call being elevated to a conference call.</td></tr>
<tr><td>Transferred *</td><td>Indicates the call leg was released as a result of being transferred.</td></tr>
<tr><td>Recording Type</td><td colspan="2">▪ Full Time
▪ Record on Demand
▪ Save on Demand</td></tr>
<tr><td>Expires</td><td colspan="2">Call recording expiration date. The date after which the call recording is purged. The date is calculated based on the retention profile assigned to the call. If the call was put on legal hold or evaluated, the expiration date is presented along with a lock icon.</td></tr>
</table>

6.12.2 Playing Back Recorded Media

This section describes how to listen to call audio, view a call video and view a desktop application recording. Use the Player interface, available when a call is selected and shown below, to listen to, email, or download a call recording.

Note: The Web browser support for the SmartTAP HTML5 player is listed below:

- **Audio:**
  - √ **Audio Playback:** Google Chrome Ver. 58 and later, Mozilla Firefox Ver. 53 and later, Microsoft Internet Explorer 11
  - √ **Wave form rendering:** Google Chrome Ver. 58 and later, Mozilla Firefox Ver. 53 and later
  - √ **Stereo wave form rendering**: Google Chrome Ver. 58 and later
  - √ **Playing while loading**: Google Chrome Ver. 58 and later, Microsoft Internet Explorer 11
- **Video:**
  - √ **Video:** Google Chrome Ver. 58 and later, Mozilla Firefox Ver. 53 and later
  - √ Playback with 'Display Video' selected is limited to five concurrent sessions.
- **Skype for Business Desktop Application Recording (Desktop Sharing):** Skype for Business desktop sharing over VBSS (Video Based Screen Sharing) recording is supported. Refer to the link below for more information on Skype for Business VBSS client and server support:
  https://docs.microsoft.com/en-us/skypeforbusiness/manage/video-based-screen-sharing#clients-and-servers-support

Figure 6-93: Audio Player Screen

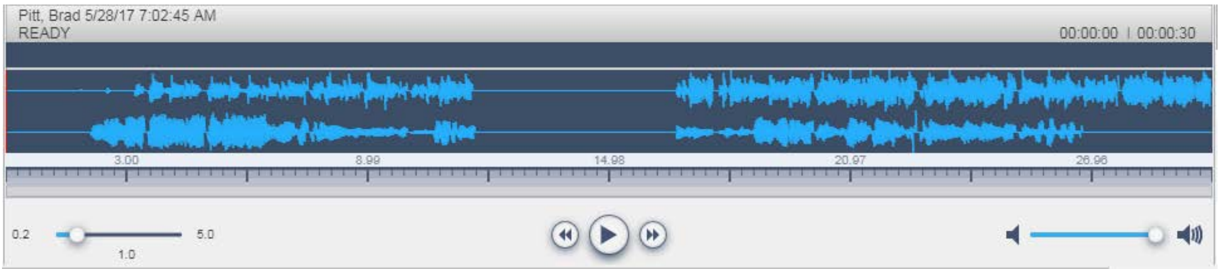
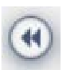
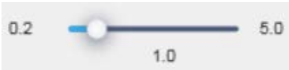
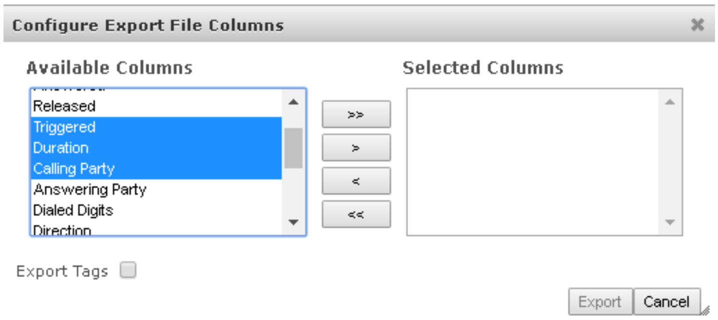


Table 6-44: Player Screen Overview

Field	Description
	Call details for the selected call
	Volume control
	Status and other information (see more information below).
	Playback the entire recording or a selected segment.
	Pause the playback of the recording.
	Rewind to immediately replay the selected segment of the recording from the start point of the segment.

Field	Description
	Return to the start point of the selected segment of the recording,. then click  to replay the segment.
	Playback speed in milliseconds.
	Send call information to an excel worksheet. When this option is selected, you can use the arrow keys to select those columns to include in your report. 
	Email call information.
	Download call information to your PC.

6.12.2.1 Listening to Call and Viewing Call Video

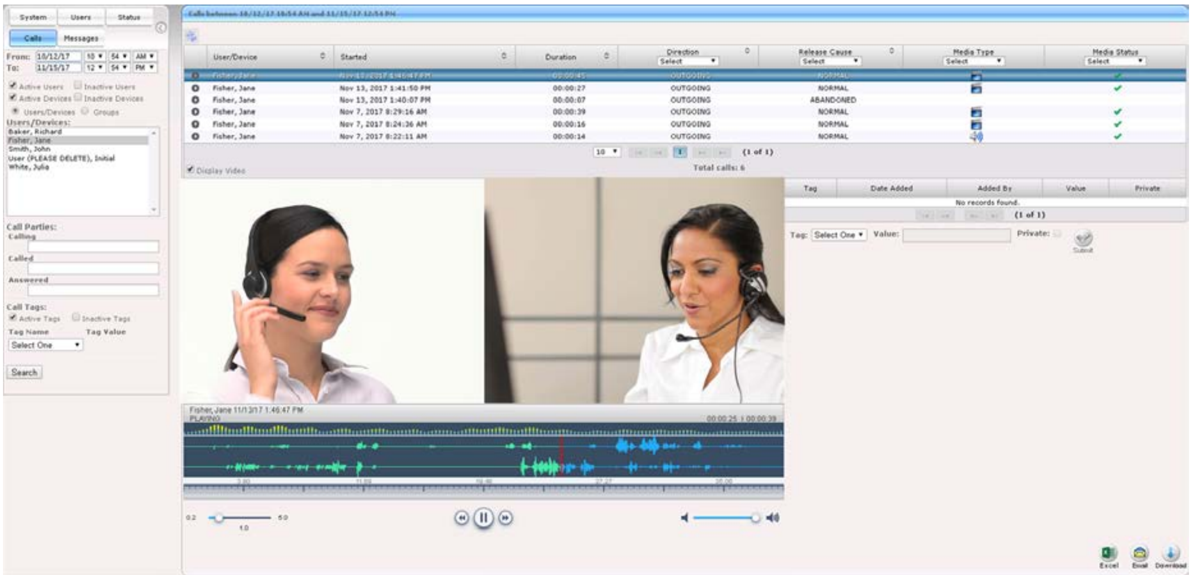
This section describes how to listen to a call and view a video.

➢ **To listen to a call and view call video:**

1. Follow the instructions described in Section 6.12.1 to search for calls.
2. If you wish to view call video, ensure that you have selected the “Display Video” check box.
3. In the retrieved calls list, select the desired call entry that you wish to listen.

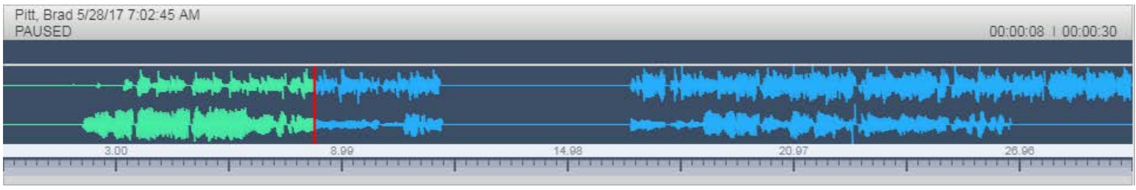
   The call recorder is displayed with the frequency spectrum of the call.
4. Click the  button to start listening to the call and/or view the video (if you selected “Display Video” check box); the button changes to  while the call is playing, to allow the administrator to pause the player while playing the audio or video.

Figure 6-94: Viewing Video



When the call is played back, the played back segments are colored green and the audio signaling playback data is displayed at the top of the dialog (shown by the yellow lines at the top of the dialog below).

Figure 6-95: Playback Audio Signaling Data

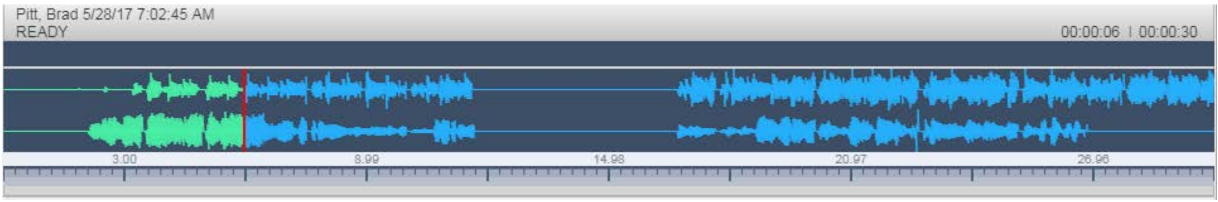


Information at the top-left hand side of the screen includes the user name, date and time and status e.g. “PLAYING”. On the top-right hand side of the screen includes the elapsed playback time and the total playing time.

The timeline of the recording segments (in minutes and seconds) is displayed below the recording signal data.

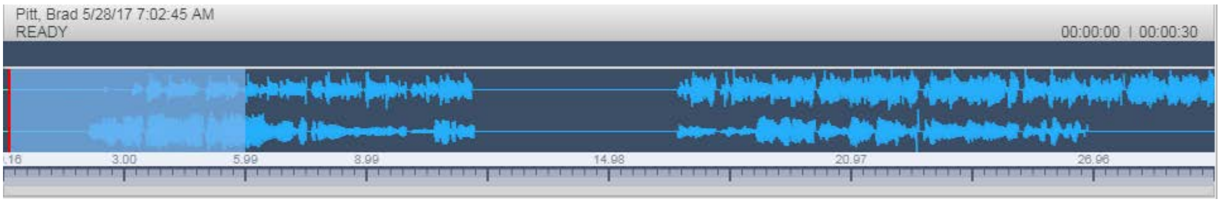
5. Manipulate the call recording in the following ways:
   - Move the cursor to any random point in the recording and left-click and release;
   - The selected segment is colored green. Click the button; the call recording is played from the left-click selection point forward (shown by the red line in the figure below).

Figure 6-96: Random Selection Point in Call Recording



   - Left-click and drag the mouse over the desired segment in the call recording and release; the selected segment is shaded blue. Click the button; the shaded segment of the call recording is played back.

Figure 6-97: Highlighted Segment in Call Recording



- Select the  button to return to the start point of the selection; the selected segment is immediately played back.
- Select the  button to return to the start point of the selection. You must then click the  button to playback the selected segment.

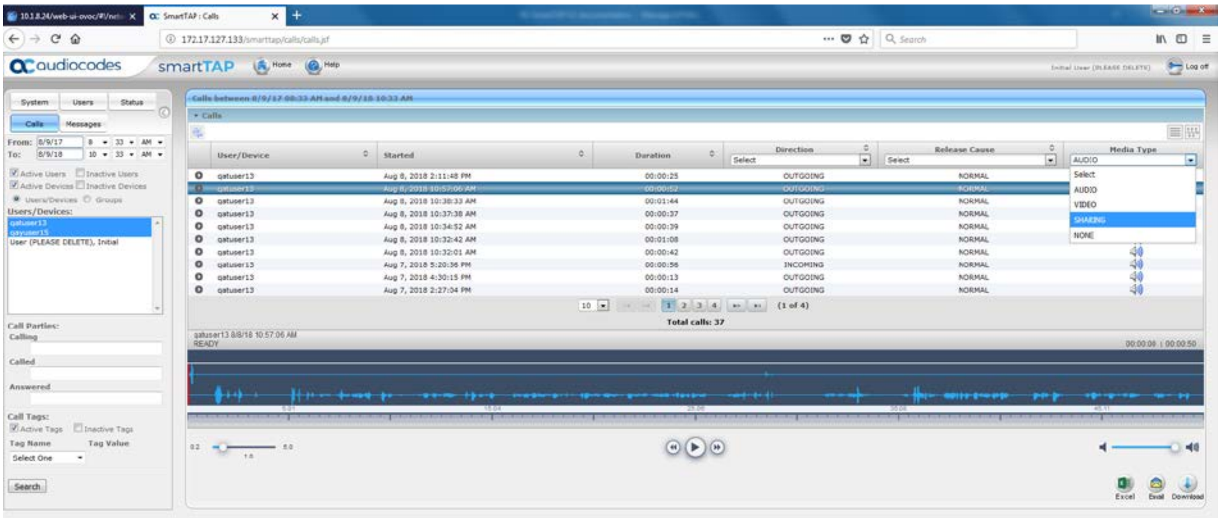
6.12.3 Skype for Business Desktop Sharing

This section describes how to playback a desktop sharing recording.

➢ **To playback desktop sharing recording :**

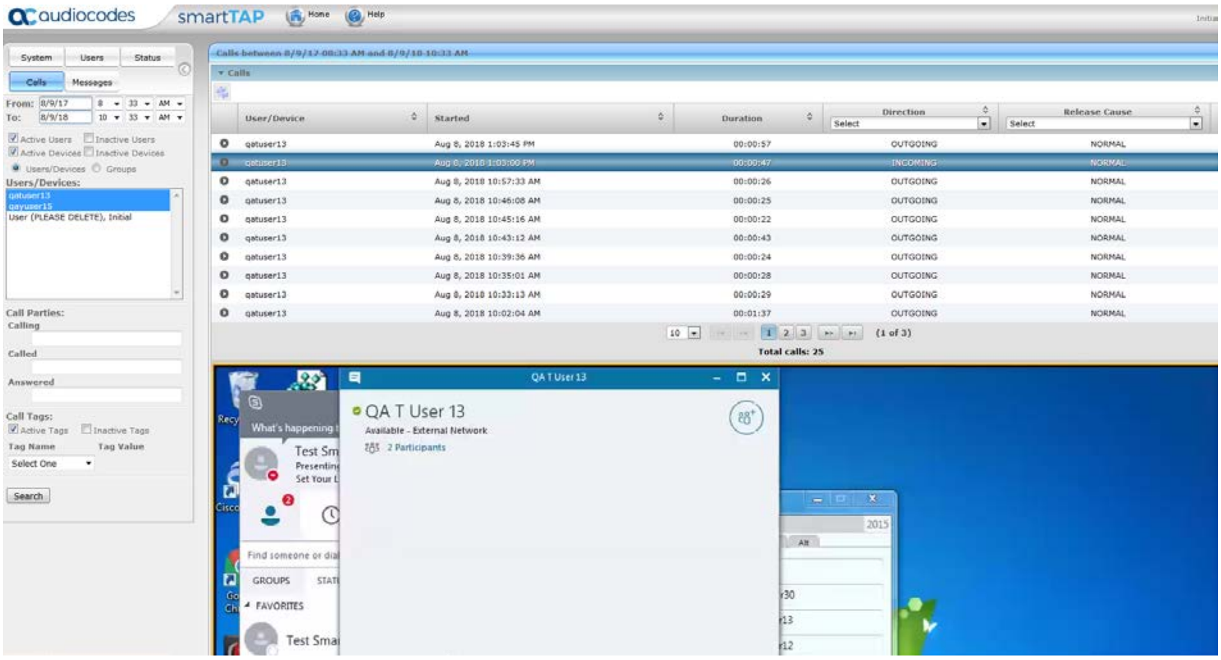
1. Follow the instructions described in Section 6.12.1 to search for calls.
2. From the Media Type drop-down list, select **Sharing** to filter the search results for the desktop sharing recordings.

Figure 6-98: Media Type-Sharing



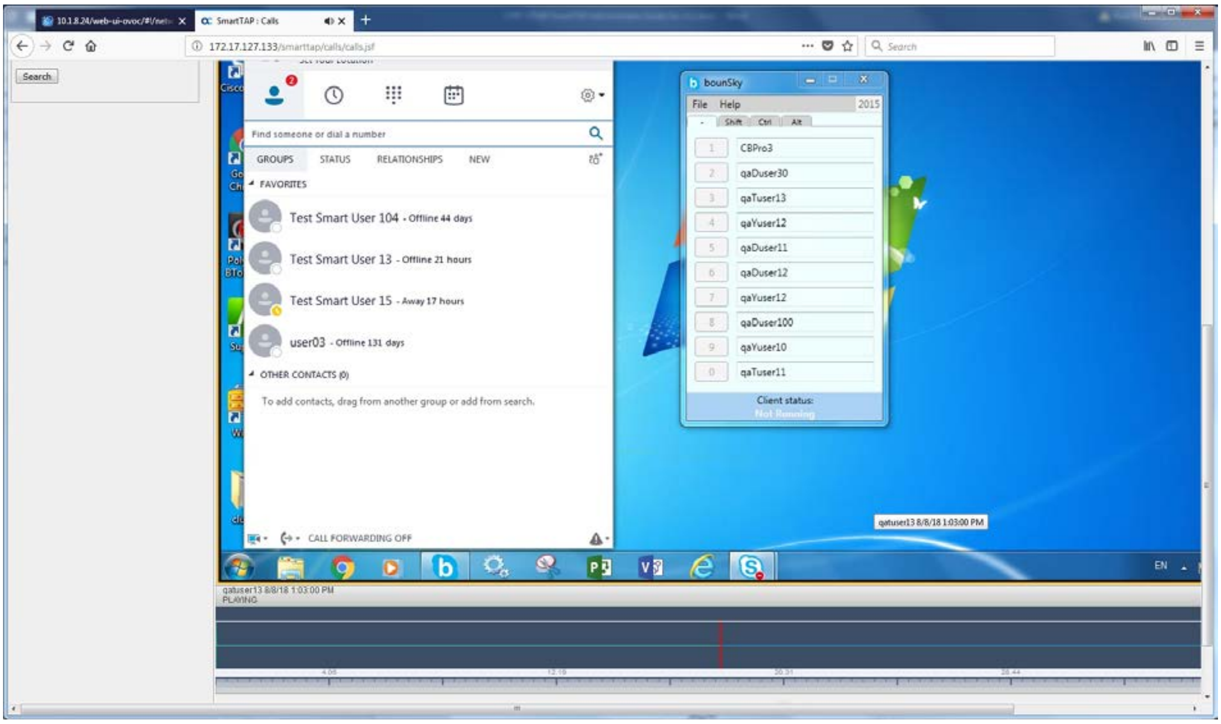
3. Double-click a row to display the desktop sharing recording.

Figure 6-99: Desktop Sharing Recording



4. Click the  button to playback the selected segment; view the keyboard and mouse actions of the user for the recorded application segment.

Figure 6-100: Playback Desktop Sharing Recording



5. Click the  button to return to the start point of the selection; the selected segment is immediately played back.

6. Click the button to return to the start point of the selection. You must then click the button to playback the selected segment.

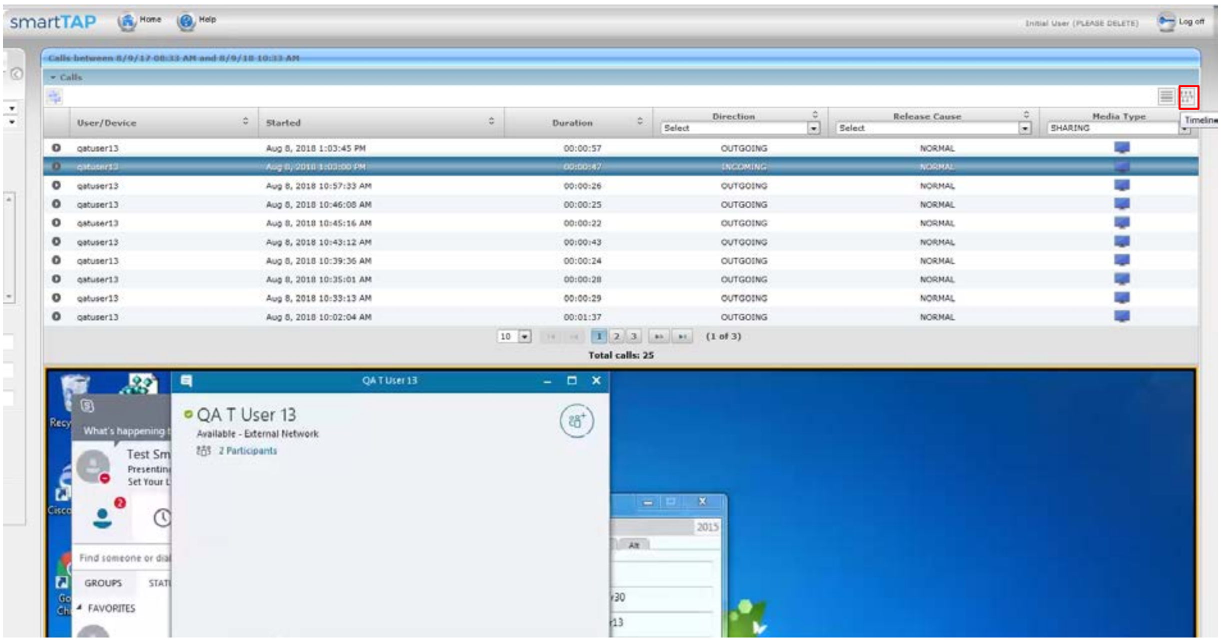
6.12.4 Time Line View

You can view call data for a specific user/device over a time line. Zooming in using the mouse roller or navigation buttons enables you to view the details of call.

➢ **To manage calls using the timeline feature:**

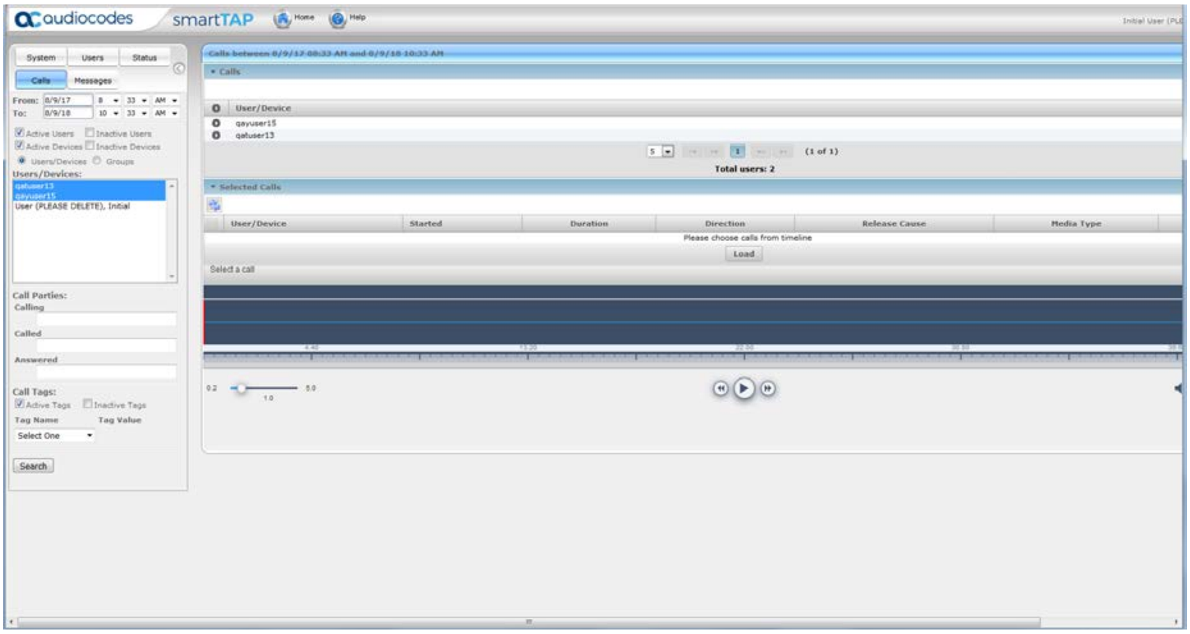
1. Follow the instructions described in Section 6.12.1 to search for calls.
2. Select the Timeline view icon as shown in the figure below.

Figure 6-101: Timeline View Icon



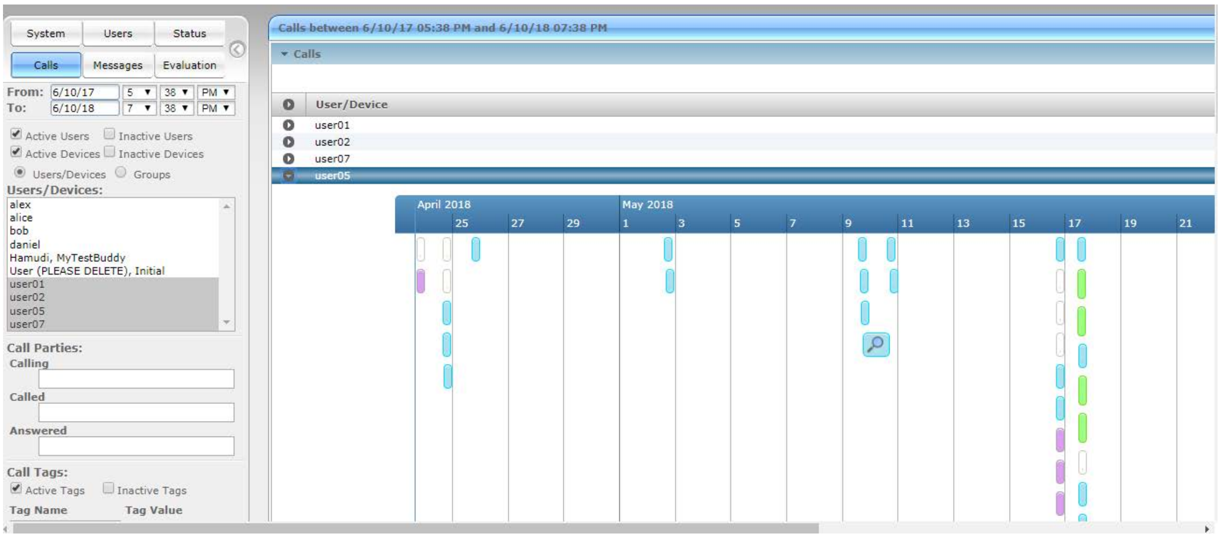
A screen similar to the following is displayed:

Figure 6-102: Choose Calls to View from the Timeline



3. In the Call Results screen, select the arrow adjacent to the entry whose timeline you wish to view. The timeline for the selected user is displayed:

Figure 6-103: User Timeline



4. Zoom in on a specific day to view the details using either the mouse roller or the navigation buttons that are highlighted below.

Figure 6-104: Zoom In

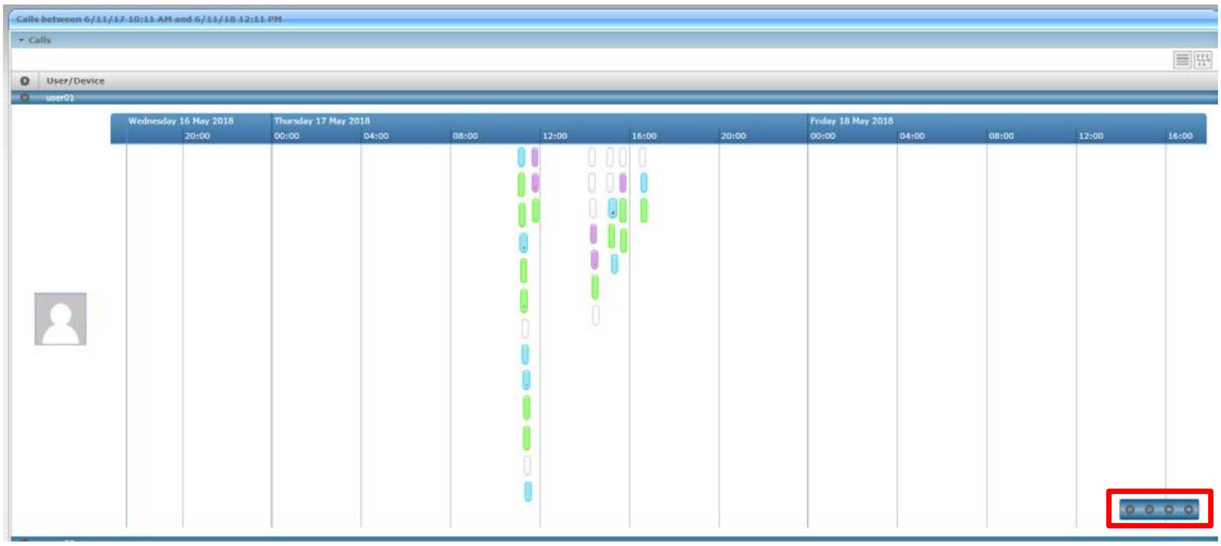
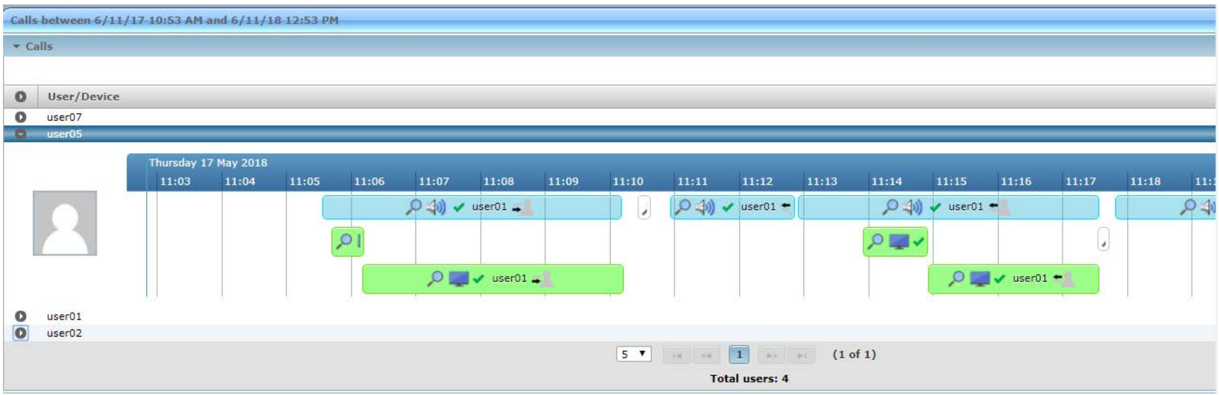


Figure 6-105: Timeline View Details



- In timeline view, the calls are grouped according to their target type. Each target type is represented by a different color. The calls for the same target type are displayed as events in a continuous timeline.
- Call events from one or more timelines can be selected to a playable table. Calls from the playable list can be loaded to player by clicking an icon in the timeline and then clicking the **Load** button.

Figure 6-106: Call Events from Multiple Timelines

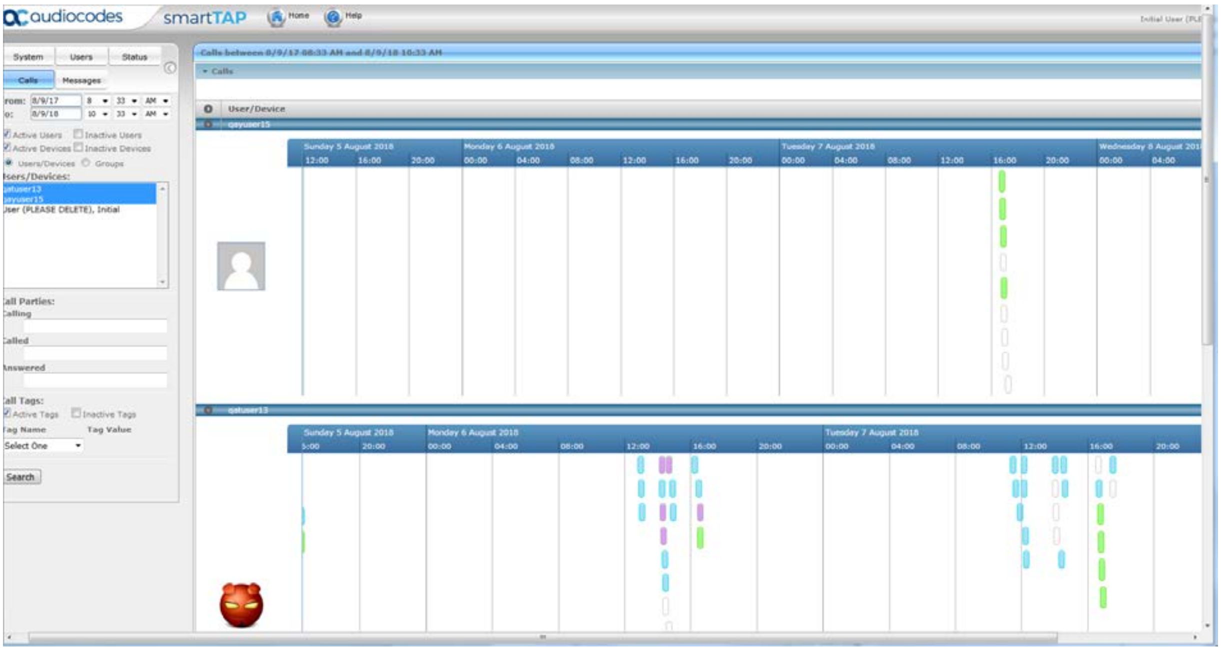
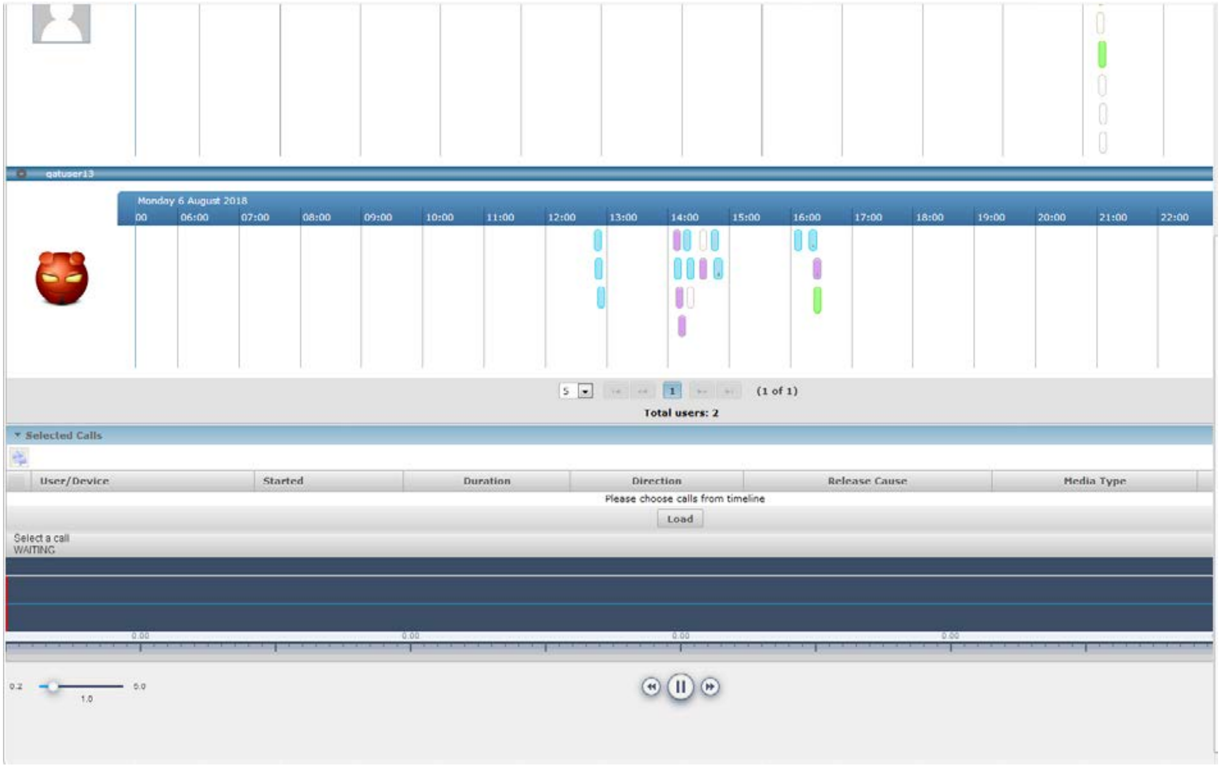


Figure 6-107: Load Calls to Timeline



The following rules are applied when more than one call is selected to play from the playable list:

- Only calls for the same user can be selected to be played together.
- The total time for playback of multiple segments should not exceed 6 hours if there is video/sharing, otherwise it can be up to 24 hours.
- Only calls of different types can overlap:
  - Audio call segment can overlap with Desktop Sharing call segment
  - Audio Video call segment can overlap with Desktop Sharing call segment

- Audio call segment can't overlap with another audio or Audio Video call segment
- Desktop Sharing call segment can't overlap with another Desktop Sharing call segment

Table 6-45: Call Events Description

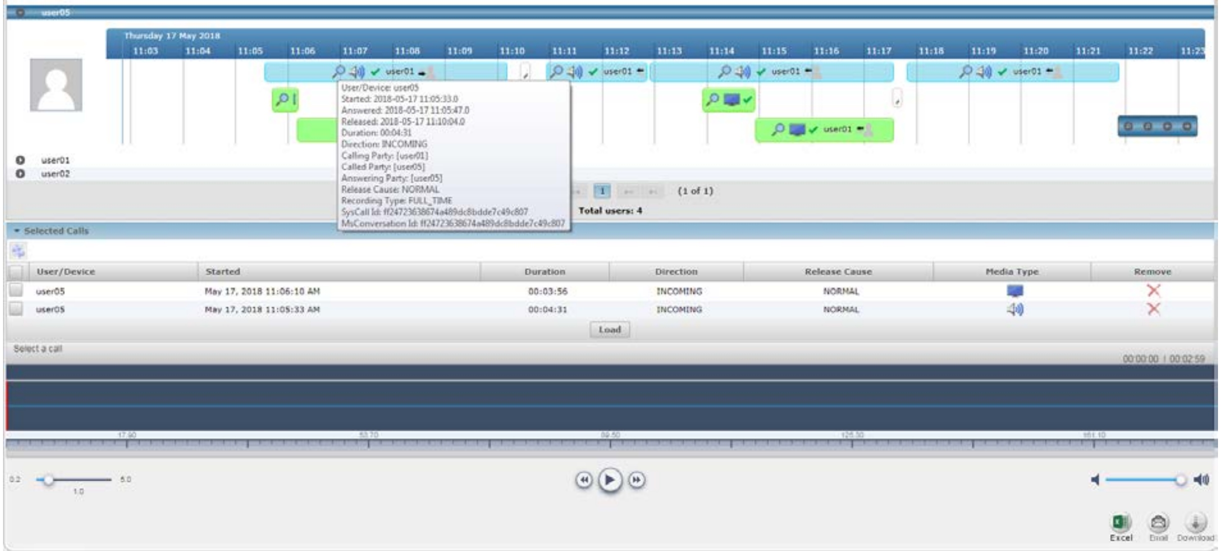
Media Type	Description
	Represents an Audio call.
	Represents a Video call
	Represents a Desktop Sharing call
	Represents a call that has no media. When a call is abandoned or missed, this target is displayed without the red warning.

Each event includes different call information statuses as shown in the table below:

Table 6-46: Call Icons

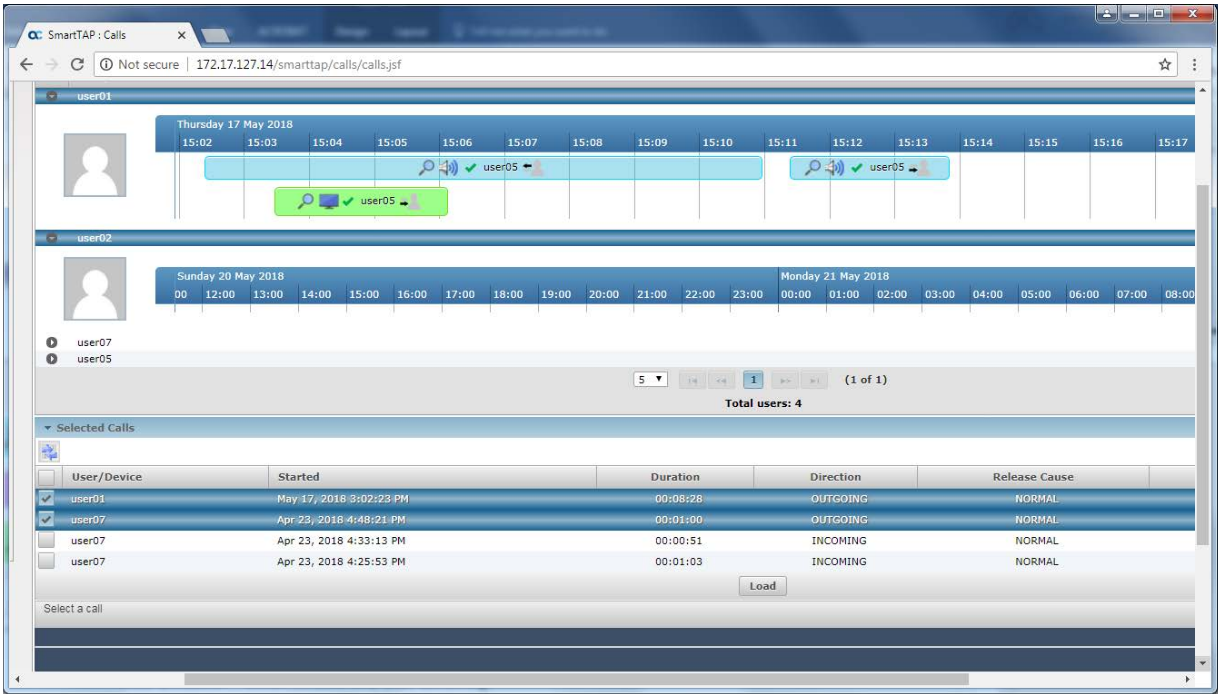
Item	Icon	Description
Call Details		Right-click the magnifying glass icon to view the call details.
Media Type		Indicates an audio call.
		Indicates a video call
		Indicates a desktop application call
Media Status		Indicates a successful call
		Indicates a call with silent media
		Indicates an unsuccessful call.
Called Party and Call Direction		Indicates an incoming call.
		Indicates an outgoing call.

Figure 6-108: Call Details



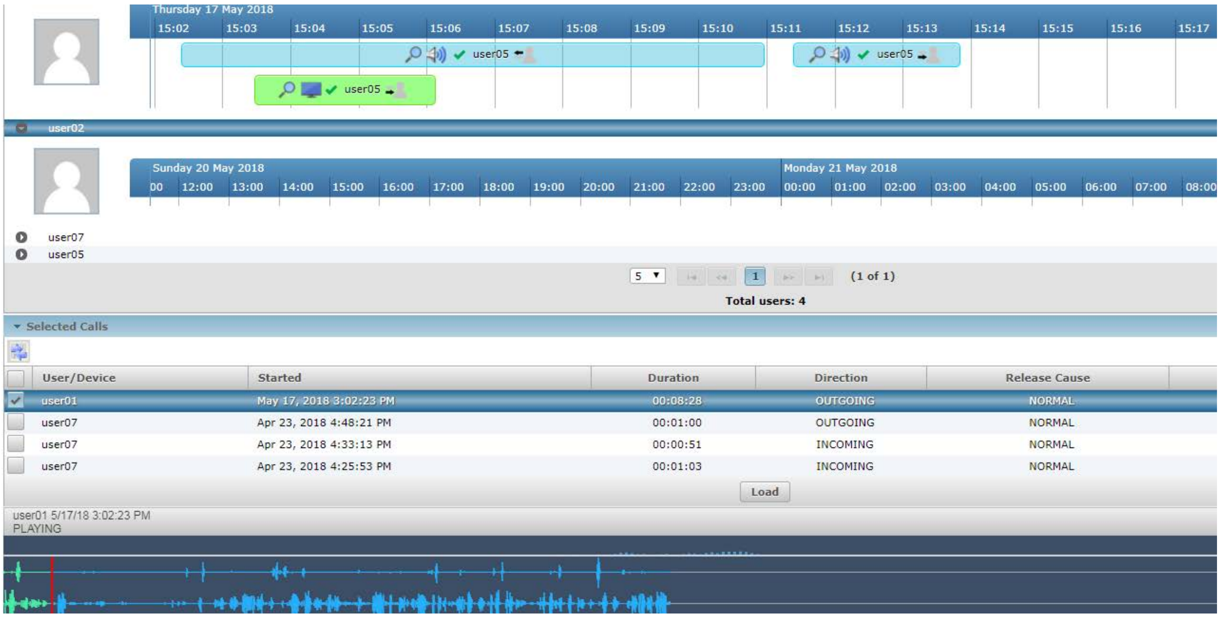
5. In the timeline, click on each call that you wish to playback; each call is added to the load dialog below.

Figure 6-109: Loading Calls



6. Select the check box adjacent to the call recording that you wish to playback and click **Load** to playback the call.

Figure 6-110: Call Playback



6.12.5 Downloading Call Recordings

You can download both audio and video call recordings components to your PC.

> **Note:** Download with 'Display Video' selected is limited to five concurrent sessions.

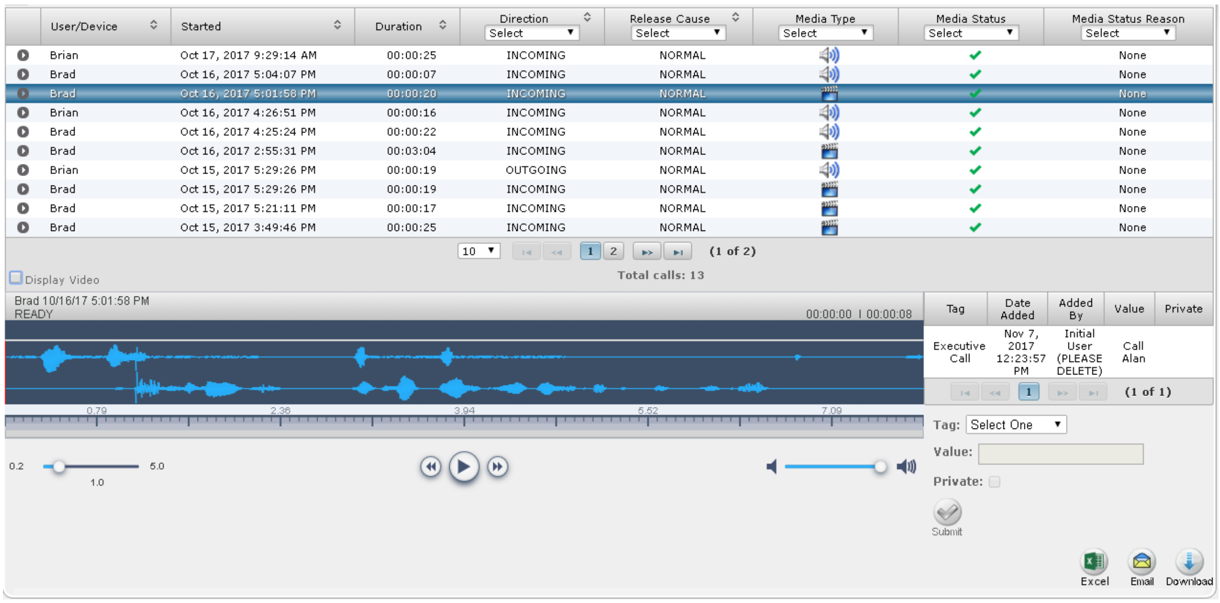
6.12.5.1 Downloading an Audio Call

This section describes how to download an audio call.

➢ **To download an audio call:**

1. Follow the instructions in Section 6.12.1 to search for the call to download.
2. From the Media Type drop-down list, select **Audio**.
3. Select the call that you wish to download.

Figure 6-111: Download Call



4. The Player screen opens; click  to open the download menu.
5. Select 'Basic' or 'Advanced' format depending on file formats, encoding, and mixing for the download files.

Figure 6-112: Basic Audio Download

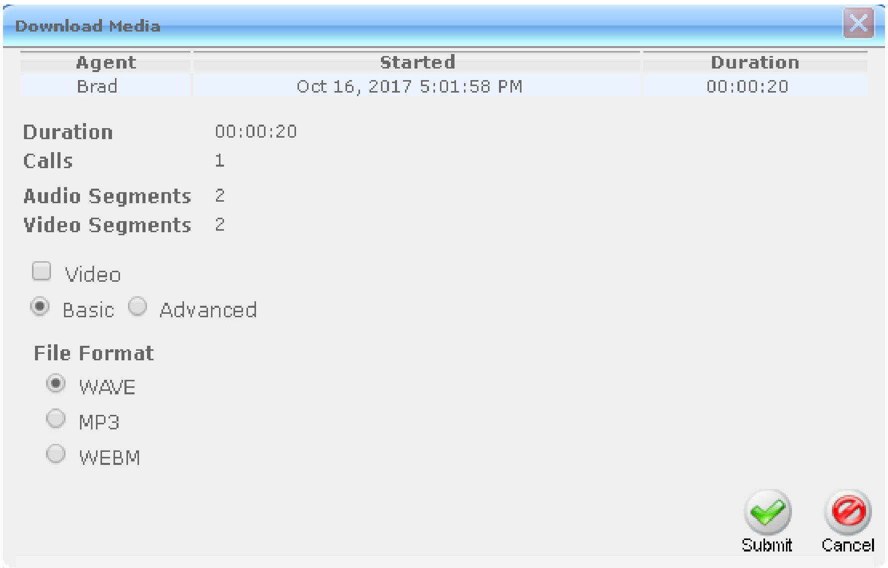


Figure 6-113: Advanced Audio Download

6.12.5.2 Downloading a Video Call

This section describes how to download a video call.

➢ **To download a video call:**

1. Follow the instructions in Section 6.12.1 to search for the call to download.
2. From the Media Type drop-down list, select **Video**.
3. Select the video you wish to download.
4. Select the **Video** check box.
5. Select 'Basic' or 'Advanced' format depending on file formats, encoding, and mixing for the download files.

Figure 6-114: Basic Video Download

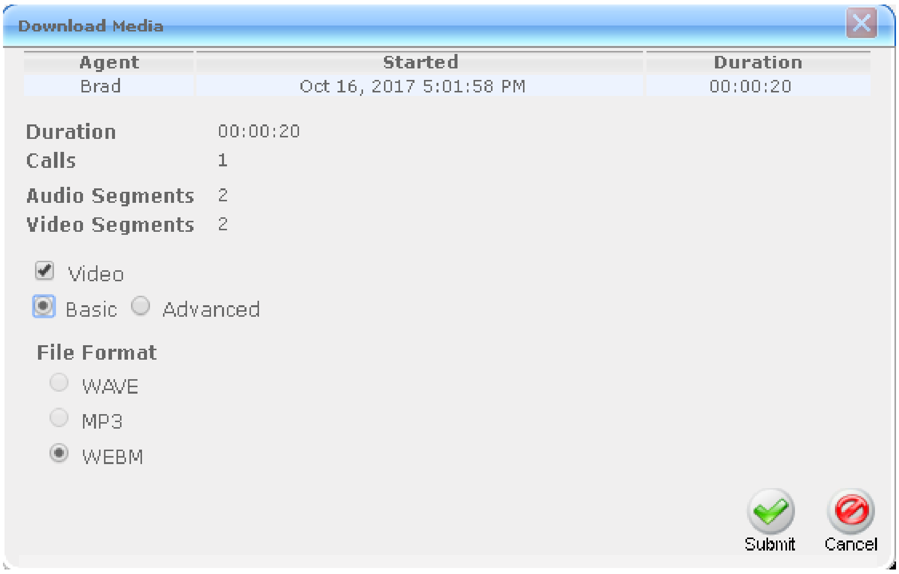
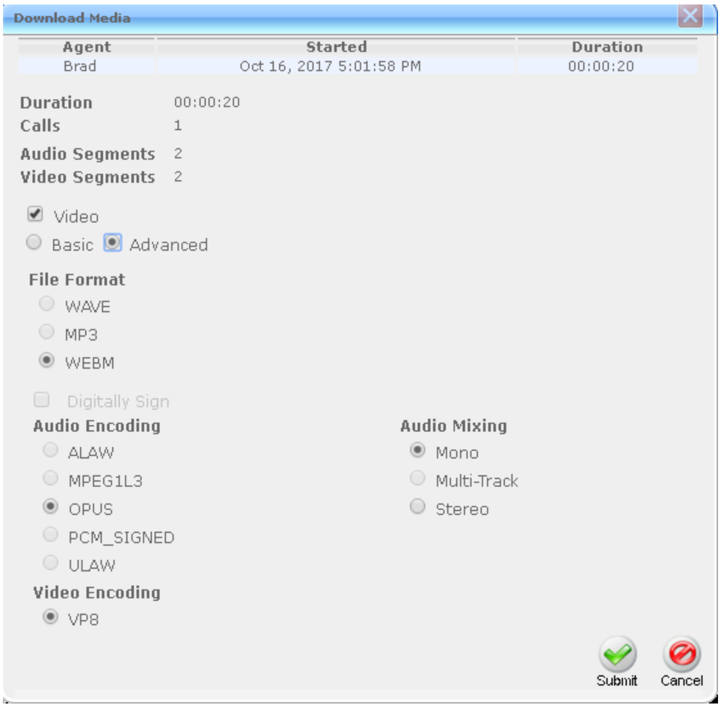


Figure 6-115: Advanced Video Download



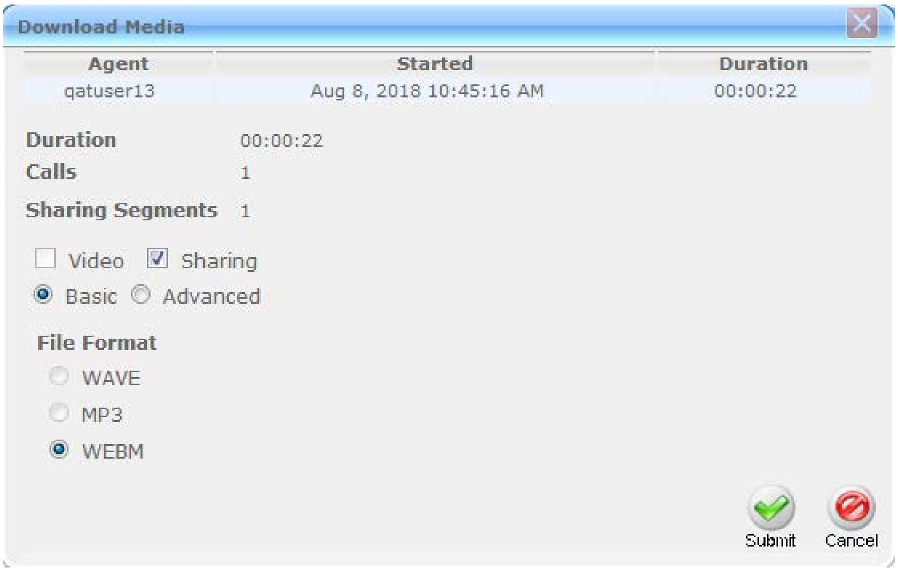
6.12.5.3 Downloading a Desktop Sharing Call

This section describes how to download a Desktop Sharing call.

➢ **To download a desktop sharing call:**

1. Follow the instructions in Section 6.12.1 to search for the call to download.
2. From the Media Type drop-down list, select **Sharing**.
3. Select the desktop sharing session you wish to download.
4. Select the **Sharing** check box.

Figure 6-116: Downloading a Desktop Sharing Call



5. Use the table below as a reference.

Table 6-47: Download Media Screen

Field	Description	Basic / Advanced
Agent	The name of the targeted user associated with this call.	Basic
Started	The call's start time.	Basic
Duration	The call's duration.	Basic
Remove ( )	Click to remove the call from download.	Basic
Duration	Duration for all selected calls.	Basic
Calls	Number of calls selected.	Basic
Video	Select this option to download recorded video. When this option, the video file format WEBM is automatically selected.	Basic
Basic	Basic format for the 'Download Media' screen.	Basic
Advanced	Advanced format for the 'Download Media' screen.	Basic
File Format	Option to select the format of the downloaded file. One of the following: ▪ Audio: ✓ Wave ✓ MP3	Basic

<table>
<tr><th>Field</th><th colspan="2">Description</th><th>Basic / Advanced</th></tr>
<tr><td></td><td colspan="2">▪ Video:
✓ WEBM
▪ Desktop Sharing:
✓ WEBM</td><td></td></tr>
<tr><td>Digitally Sign</td><td colspan="2">Add a Digital Signature to download call. See Section 6.10.1 for more details. This feature is only supported for Audio downloads.</td><td>Advanced</td></tr>
<tr><td>Audio Encoding</td><td colspan="2">Option to select the encoding of the downloaded file. One of the following:
• Audio:
✓ ALAW
✓ MPEG1L3
✓ Opus
✓ PCM_Signed
✓ ULAW</td><td>Advanced</td></tr>
<tr><td>Video Encoding</td><td colspan="2">VP8</td><td></td></tr>
<tr><td rowspan="3">Mixing</td><td colspan="2">Option to select the mixing of the downloaded file.</td><td>Advanced</td></tr>
<tr><td>Mono</td><td>All audio tracks from the selected call will be mixed into a single mono track in the downloaded file.</td><td>Advanced</td></tr>
<tr><td>Multi-Track</td><td>All tracks from the selected call will be placed on a separate track within the downloaded media file.</td><td>Advanced</td></tr>
<tr><td></td><td>Stereo</td><td>Audio of each side of a call will be placed on a separate track within the downloaded media file.</td><td>Advanced</td></tr>
<tr><td>
Submit</td><td colspan="3">Apply the changes.</td></tr>
<tr><td>
Cancel</td><td colspan="3">Cancel the changes.</td></tr>
</table>

6. Click **Submit** to download and save the file on the local computer.

6.12.6 Emailing Call Recordings

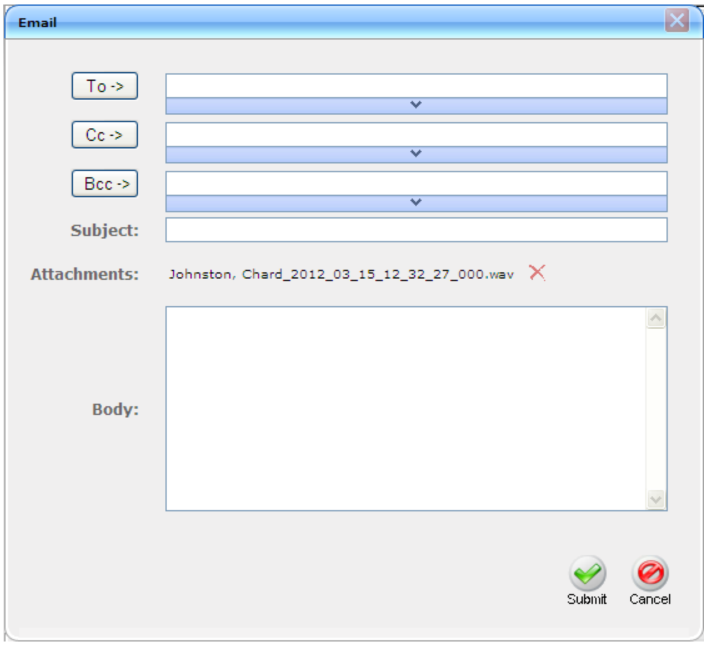
You can send call recordings to an email address. Note that when this option is selected, only the audio components of the call are sent to an email address.

Note: Video components cannot be sent by email.

➢ **To email a call:**

1. Follow the instructions in Section 'Searching for Calls' (see 6.12.1) to find the call to email.
2. Select the call entry to email and then click the email button Email ; the Email screen opens.

Figure 6-117: Email Screen



3. Use the table below as reference. Enter the recipients email addresses, or select from the dropdown.
4. Enter Cc and Bcc recipients if appropriate.
5. Enter Subject and Body.

Table 6-48: Email – Field Descriptions

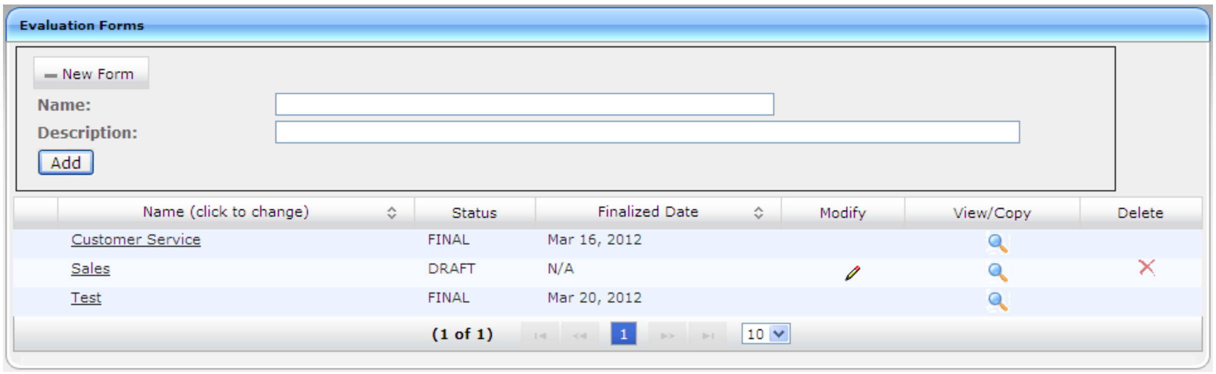
Field	Description
To > Cc > Bcc >	Clicking the **To>**, **Cc>**, **Bcc>** buttons expands and collapses the list of users within the current user's group(s). Selecting/deselecting users from this list adds / removes them. The recipient list is a comma separated list of email addresses in the format 'jsmith@example.com'. The recipient list may also include the display name of the recipient. To add a display name for a recipient, the recipient's email address should be in angled brackets, for example: **John Smith <jsmith@example.com>**
Subject	Subject of the email.
Attachments	List of attachments included with this email message. Clicking the **X** next to the attachment removes the attachment from the email.
Body	Body of the email.
Submit	Sends the email.
Cancel	Cancels the email.

6. Click **Submit** to send the email.

6.13 Using the Evaluation Feature

The **Evaluation** tab accesses all functions related to the SmartTAP evaluation feature. From under this tab, evaluation forms to be used for evaluations are created. Later, evaluation reviews and reports can be generated. The Evaluation Forms screens, shown in the figure below, provides access to all evaluation-related features.

Figure 6-118: Evaluation Forms – New Form Subscreen



Use the table below as reference.

Table 6-49: Evaluation Forms – New Form Subscreen

Field	Description
— New Form	Click to close the Add Form sub screen.
+ New Form	Click to open the Add Form sub screen.
Name (in the New Form menu)	The name of the new form.
Description (in the New Form menu)	The description of the new form.
Add (in the New Form menu)	Click to create a new form.

➢ To add a new form

1. Open the Evaluation Forms screen (**Evaluation** tab > **Evaluation Folder** > **Evaluation Forms**).
2. In the New Form subscreen, enter the Name of the new form and a Description.
3. Click Add to create the form
4. The new form is added to the display with an (asterisk) on the rightmost column.
5. Use the **Modify** ( ) button to define the form.

➢ To rename a form:

1. Open the Evaluation Forms screen (**Evaluation** tab > **Evaluation** folder > **Evaluation Forms**).
2. In the Evaluation Forms screen, click the 'Name' of the form to rename.
3. Change the Name and/or Description of the form in the 'New Form' subscreen.
4. Click Add to rename the form.

Figure 6-119: Evaluation Forms

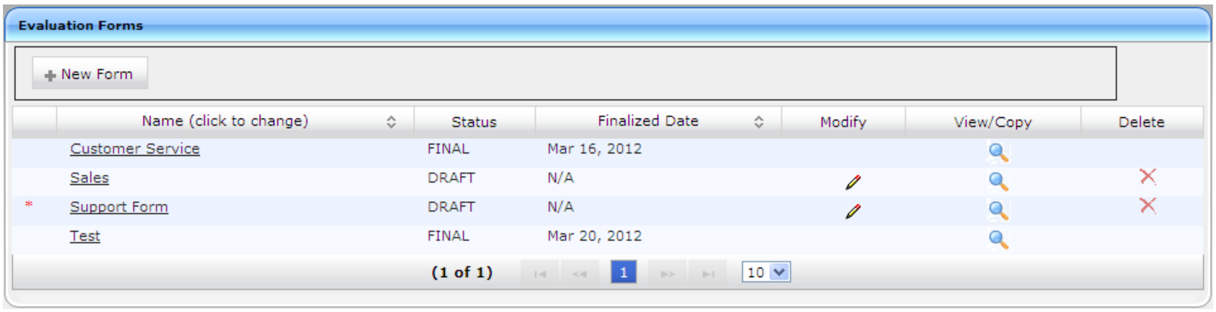
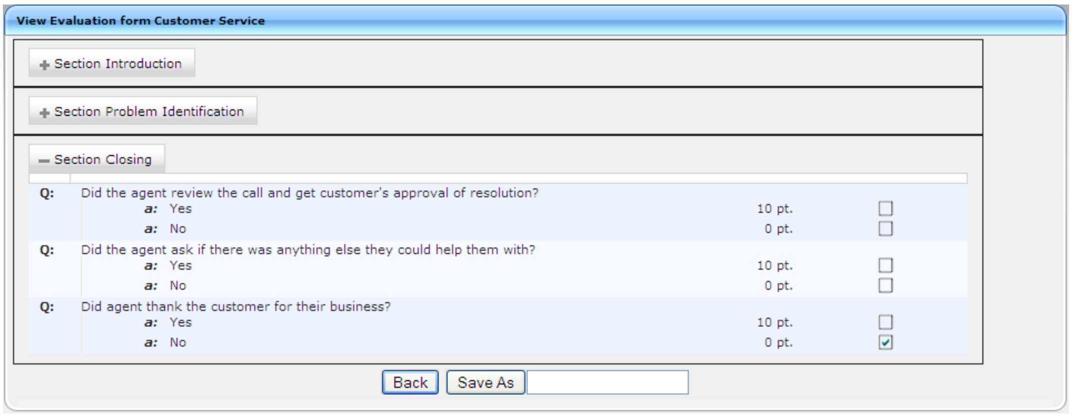


Table 6-50: Evaluation Forms – Field Descriptions

Field	Description
— New Form	Click to close the Add Form subscreen.
+ New Form	Click to open the Add Form subscreen.
Name (click to change)	Form Name sorted ascending/descending by clicking header up/down arrows.
Status	▪ FINAL (the form is final and available for use for evaluations. *FINAL status forms cannot be changed*) ▪ DRAFT (the form can be edited. *DRAFT forms are not available for use for evaluations*)
Finalized Date	▪ **(date)** (Date when the form was finalized) ▪ **N/A** (Not Applicable; the form is not finalized)
*	The form is not completed and cannot be finalized.
Modify ( )	Click to modify the form.
View/Copy ( )	Click to view or copy the form.
Delete ( )	Click to delete the form.

Figure 6-120: View/Copy Evaluation



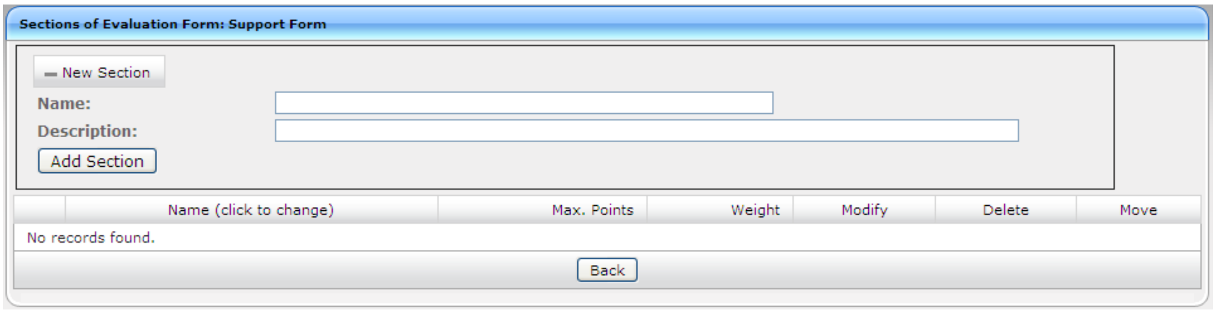
➢ To view/copy a form

1. Open the form to view or copy by clicking the **View/Copy** button in the row associated with the form in the Evaluation Forms main screen.
2. Enter the Name for the new form and click Save As.
3. The View closes and the new form is added to the list of forms in the 'Evaluation Forms' screen.

➢ To add a New Section [Evaluation Forms]:

1. Open the form (**Evaluation** tab > **Evaluation** folder > **Evaluation Forms**).

Figure 6-121: Sections of Evaluation Form – New Section Subscreen



2. Click **Modify** ( ) on the row listing the form to change to open it
3. [Use the table below as reference] Enter the new section Name and Description in the New Section subscreen
4. Click Add Section to create the new section; the new Section appears in the form with an asterisk on the leftmost column indicating that the form is missing fields and cannot be finalized.

Table 6-51: Sections of Evaluation Form – Field Descriptions

Field	Description
— New Section	Click to close the New Section subscreen.
+ New Section	Click to open the New Section subscreen.
Name (in new section subscreen)	The name of the new Section.
Description	The description of the new Section.
Add Section	Create a new section.

➢ **To add New Questions [Evaluation Forms]:**

Figure 6-122: Sections of Evaluation Form – New Questions Subscreen

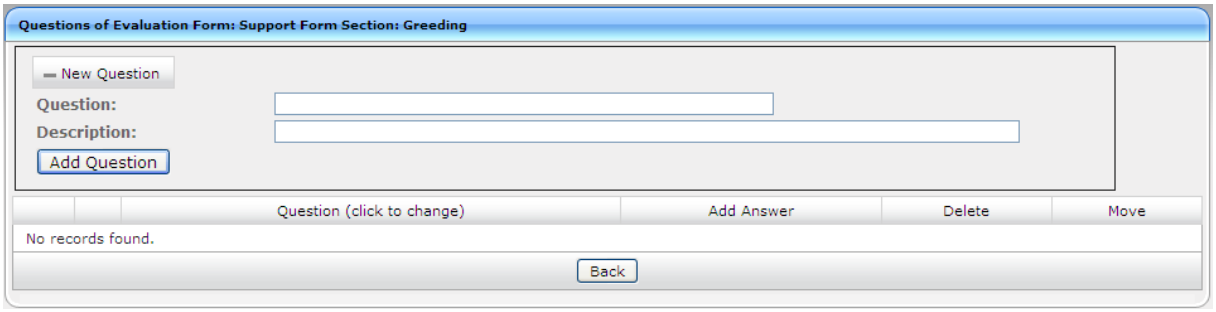


Table 6-52: Sections of Evaluation Form – New Question Subscreen

Field	Description
– New Question	Click to close the New Question subscreen.
+ New Question	Click to open the New Question subscreen.
Question	The name of the new Question.
Description	The description of the new Question.
Add Question	Create a new Question.

➢ To add a New Question:

1. Open the form (**Evaluation** tab > **Evaluation** folder > **Evaluation Forms**).
2. Click **Modify** ( ) on the row listing the **Form** to change, to open it.
3. Click **Modify** ( ) on the row listing the **Section** to change, to open it.
4. Enter the new Question Name and Description in the New Question subscreen.
5. Click Add Question to create the new Question; the new Question appears in the form with an asterisk * on the leftmost column indicating that the form is missing fields and cannot be finalized.

➢ To add a New Answer [Evaluation Forms]:

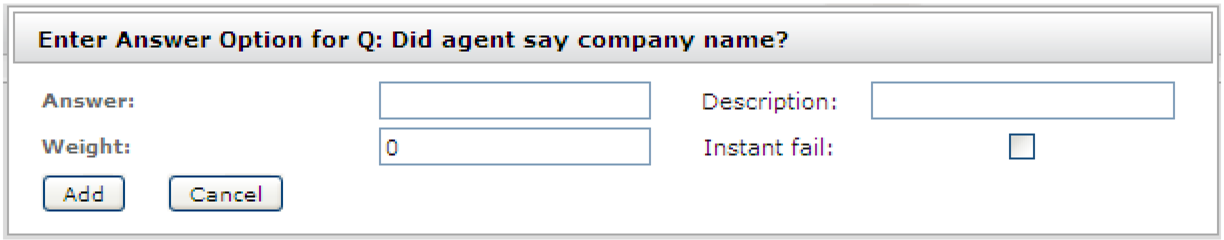
Table 6-53: Sections of Evaluation Form – New Answer Subscreen

Field	Description
Answer	Acceptable answer to the associated question.
Weight	Weight associated with this answer.
Description	Description of the answer.
Instant fail	Check if this answer causes an instant fail during evaluation.
Add	Add new answer.

➢ To add a new answer:

1. Open the form (**Evaluation** tab > **Evaluation** folder > **Evaluation Forms** > **Form**).
2. Click **Modify** ( ) on the row listing the **Form** to change, to open it.
3. Click **Modify** ( ) on the row listing the **Section** to change, to open it.
4. Click **Modify** ( ) on the row listing the **Question** to launch the **Answer** screen.

Figure 6-123: Sections of Evaluation Form - New Answer Subscreen

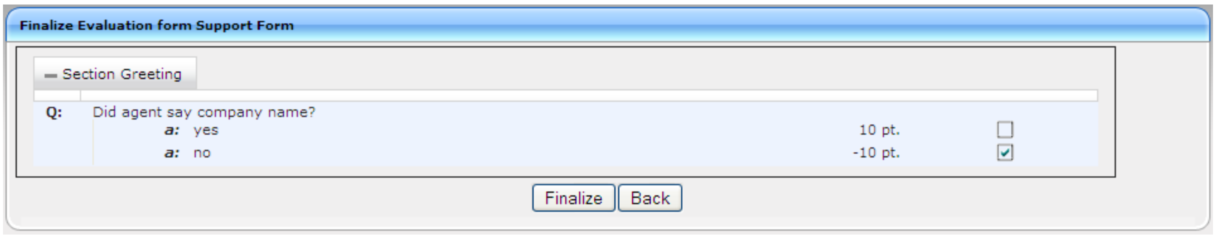


5. Enter the new Answer information.

6. Click Add to create the new Answer; the new Answer will appear in the form with an asterisk * on the leftmost column indicating that the form is missing fields and cannot be finalized. There is a minimum of two (2) answers required before a form can be finalized.

➢ **To finalize a Form [Evaluation Forms]:**

Figure 6-124: Form Subscreen



➢ **To finalize a form:**

1. Open the form (**Evaluation** tab > **Evaluation** folder > **Evaluation Forms** > **Form**).
2. Click Finalize to open the Finalize Evaluation form subscreen.
3. Click Finalize to change the form status from DRAFT to FINAL; the form Status on the Evaluation Forms screen changes to FINAL, and **Modify** ( ) is no longer available to change the form.

6.13.1 Performing an Evaluation

An administrator with privileges to perform an evaluation selects a finalized evaluation form, selects the call to evaluate, and from the Perform Evaluation screen, selects the appropriate answers to the questions in the evaluation form.

When all answers in the evaluation form are provided, the user may save the evaluation for later review.

Table 6-54: Select Evaluation Form Screen

Field	Description
Name	The name of the form.
Description	Description of the form.
Select	Select click to select the form.

Figure 6-125: Call Search/Selection Evaluation Form

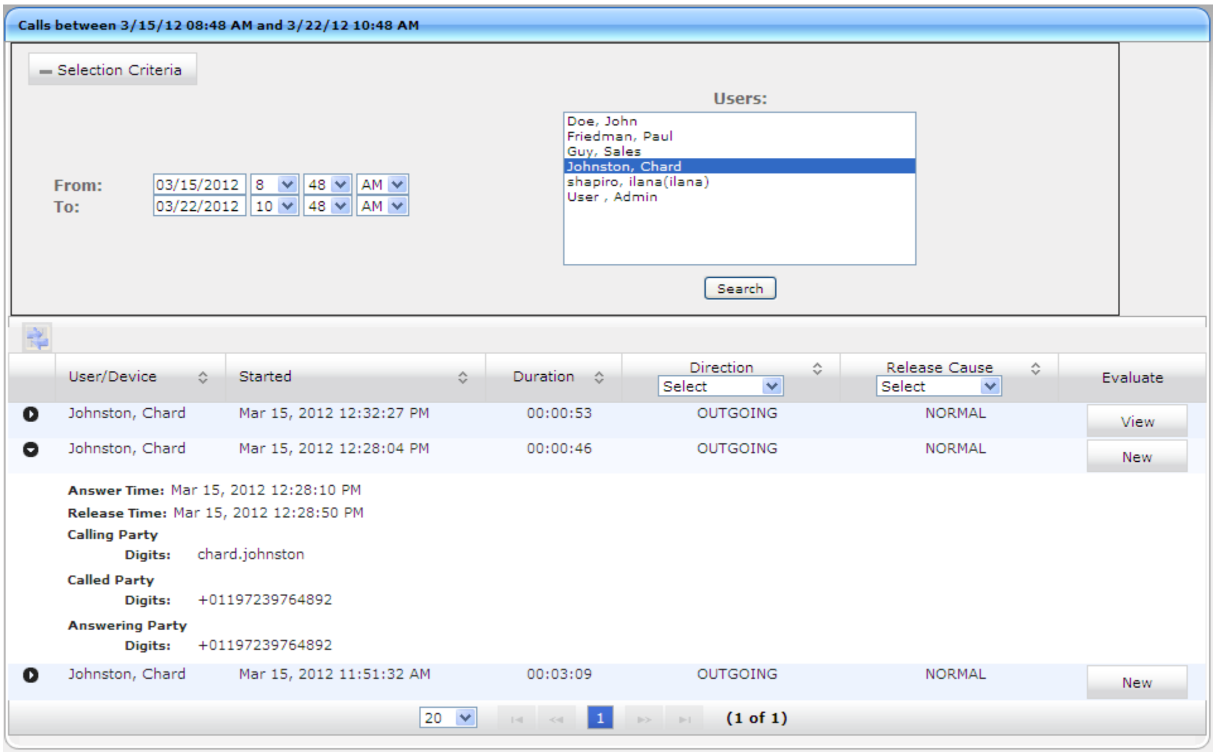
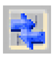


Table 6-55: Call Search/Evaluation Form – Field Descriptions

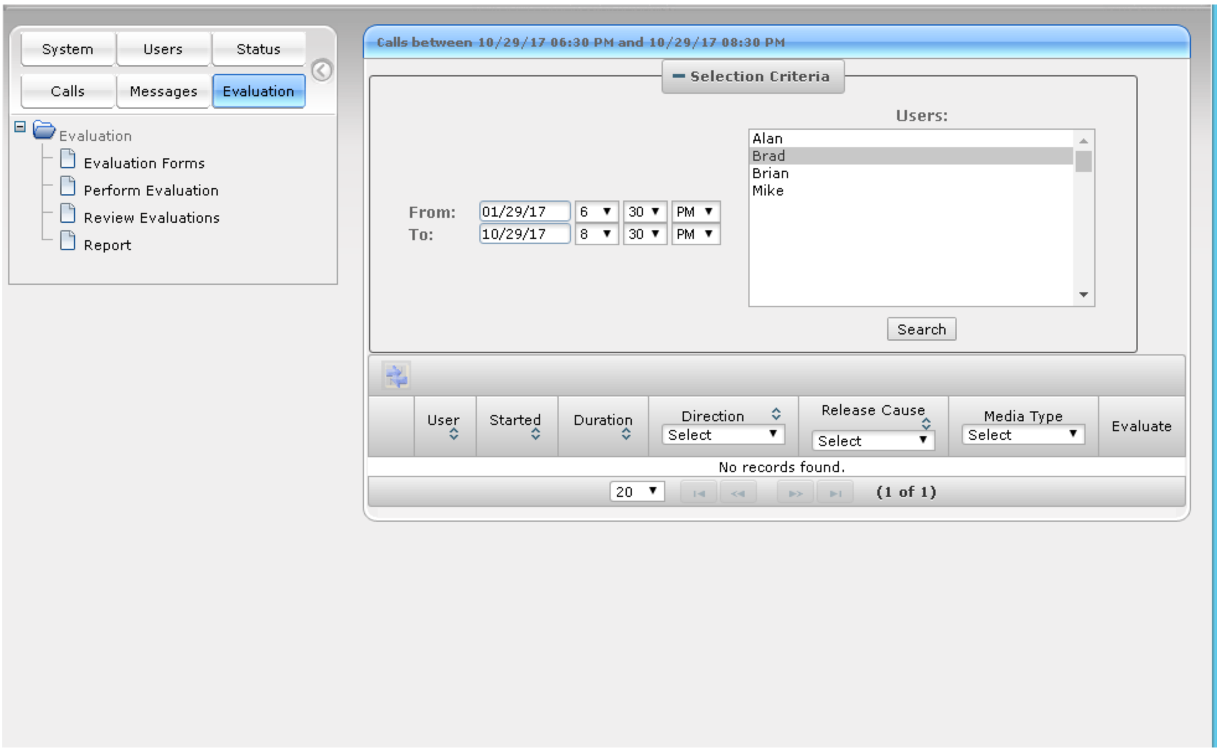
Field	Description
From:	Earliest date and time to search from. Click the date field for a calendar to pop up showing one month at a time. Use the dropdown to change the time of day.
To:	Latest date and time to search to. Click the date field for a calendar to pop up showing one month at a time. Use the dropdown to change the time of day.
Users	Users whose account is enabled in SmartTAP.
Search	Click to search and display results in the Evaluation screen.
	Launch the Add and Remove Columns dialog.
User/Device	User/Device name. Clicking this header sorts the search results in Ascending/Descending order alternating with each click.
Started	Date and time the call recording started. Clicking this header sorts the search results in Ascending/Descending order alternating with each click.
Duration	Call Duration. Clicking this header sorts the search results in Ascending/Descending order alternating with each click.
Direction	Direction of the call. Clicking this header sorts the search results in Ascending/Descending order alternating with each click. The dropdown entry shows only the matching results.
Release Cause	Release cause for the call. Clicking this header sorts the search results in Ascending/Descending order alternating with each click. The dropdown entry shows only the matching results.
Media Type	The Media Type of the call. One of the following values: • Audio

Field	Description
	• Video • Desktop Sharing • None
	Click to expand the view of a call, to show additional details.
	Click to minimize the view of a call, to just one row of information.
View	A Finalized Evaluation exists for the selected Evaluation form and call, and will be presented for viewing.
New	A new Evaluation will be created for a previously selected Evaluation Form, and the call selected.
Continue	Continue previously started Evaluation.
Page Navigation buttons	Buttons are shortcuts to the beginning/end, previous/next page of the displayed entries. The dropdown allows changing the number of entries per page.

➢ To start an evaluation:

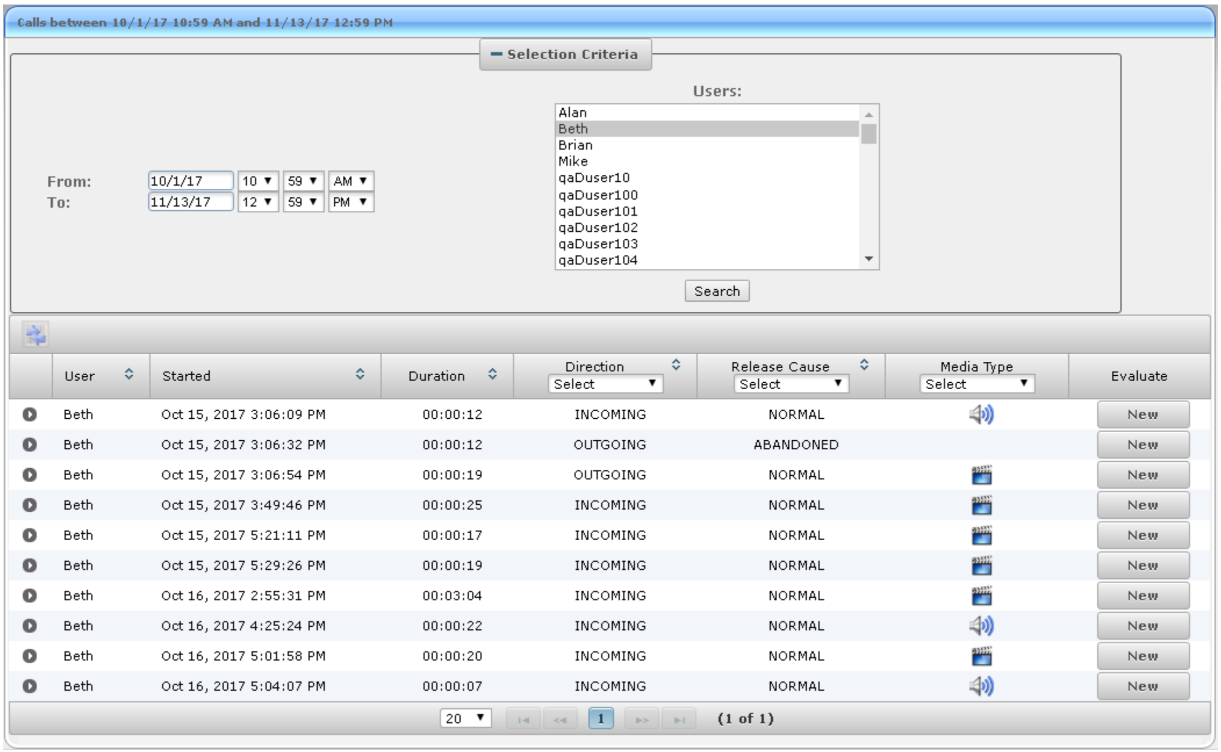
1. Open the Select Evaluation Form (**Evaluation** tab > **Evaluation** folder > **Perform Evaluation**).
2. Click Select to select the form for this evaluation; the Call Search/Selection screen launches for the user to select the calls to evaluate.

Figure 6-126: Select User for Evaluation



3. Select a date range to search from and then click Search. A list of call records for the selected user is displayed.

Figure 6-127: Select Call to Evaluate



4. Click **New** on the row of the call to evaluate.

Figure 6-128: Perform Evaluation Screen

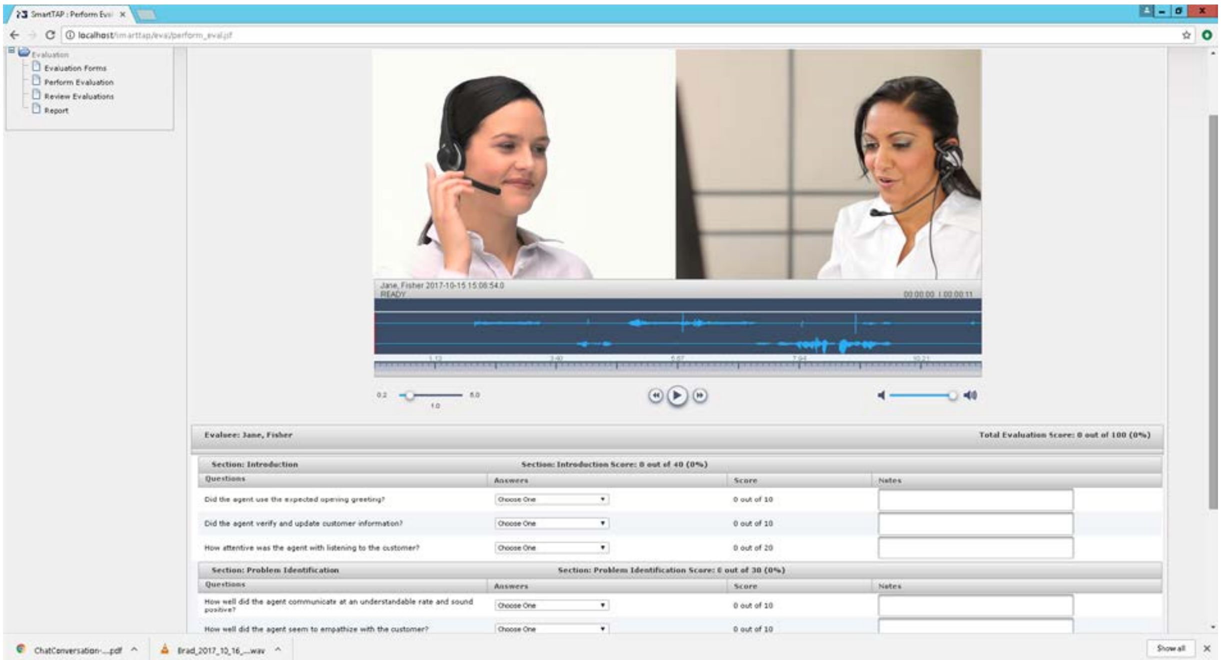


Table 6-56: Perform Evaluation Screen

Field	Description
Display Video	Displays the video screen. When you click the ▶ button the recorded video is replayed.

Field	Description
	Call details for the selected call / Form
	Volume control
	Status and other information
	Playback the entire recording or a selected segment. If the 'Display Video' option is selected, both the video and audio recordings are replayed.
	Pause the playback of the recording.
	Rewind to immediately replay the selected segment of the recording from the start point of the segment.
	Return to the start point of the selected segment of the recording, then click the  button to replay the segment.
Evaluee:	Targeted user associated with the call being evaluated.
Total Evaluation Score:	Total score for the form, displayed as a percentage.
Section:	Section header
Questions	List of questions for this section
Answers	Dropdown menu with possible answers to this question.
Score	Score associated with the answer provided.
Notes	Field for the evaluator to enter notes.
Score:	Score for this section, displayed as a percentage.
Back	Abort evaluation.
Save as Draft	Save Evaluation as a draft. Save as Draft to save evaluation before all answers scored.
Save as Final	Save Evaluation as Final. The **Save as Final** button will only be available after all answers are scored.

➤ **To perform the evaluation:**

1. Start the evaluation as described previously.
2. If an evaluation was previously started, click the Continue button to resume it.
3. Start the evaluation by clicking the player buttons (**Play/Stop**) and moving back/forward by dragging the audio position indicator in the player.
4. For every Question, select the appropriate answers and optionally add notes in the Notes area.
5. To stop the evaluation before completing the form, select Save as Draft to save the current evaluation and resume later.
6. After all questions are answered, the Save as Final button becomes available.

7. Click Save as Final to complete the evaluation.

➢ To review evaluations:

Figure 6-129: Review Evaluations

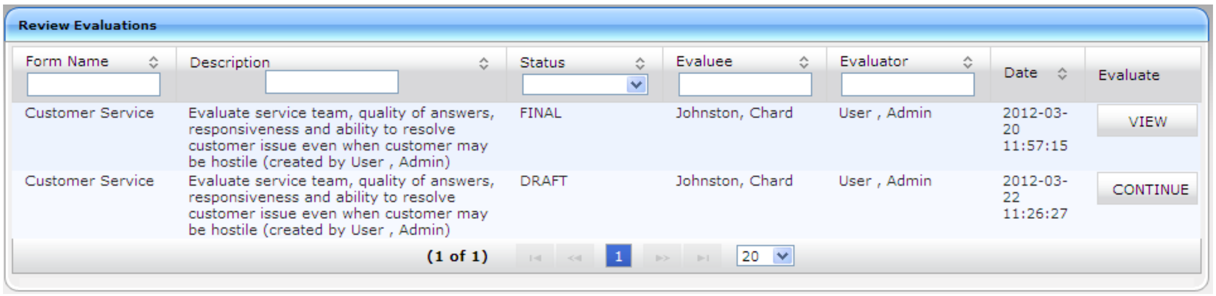


Table 6-57: Review Evaluations – Field Descriptions

Field	Description	
Form Name	Form Name used in the evaluation. Clicking this header sorts the search results in Ascending / Descending order alternating with each click. The dropdown entry shows only the matching results.	
Description	Release cause for the call. Clicking this header sorts the search results in Ascending/Descending order alternating with each click. The dropdown entry shows only the matching results.	
Status	Status of the Evaluation. Clicking this header sorts the search results in Ascending/Descending order alternating with each click. The dropdown entry shows only the matching results.	
Evaluee	User whose recording is evaluated. Clicking this header sorts the search results in Ascending / Descending order alternating with each click. The dropdown entry shows only the matching results.	
Evaluator	User performing the evaluation. Clicking this header sorts the search results in Ascending/Descending order alternating with each click. The dropdown entry shows only the matching results.	
Date	Date of the evaluation. Clicking this header sorts the search results in Ascending/Descending order alternating with each click.	
	View	Click to view evaluation; the View Evaluation screen opens.
	Continue	Click to continue evaluation; the Perform Evaluation screen opens.
Page Navigation buttons	Buttons are shortcuts to beginning/end, previous/next page of displayed entries. The dropdown allows changing the number of entries per page.	

➢ To review evaluations:

1. Open the Review Evaluations screen (**Evaluation** tab > **Evaluation** > **Review Evaluations**).
2. Click View to open the View Evaluation screen, or Continue to open the Perform Evaluation screen to complete the evaluation.

➢ To create an Average Score Report:

Figure 6-130: Average Score Report

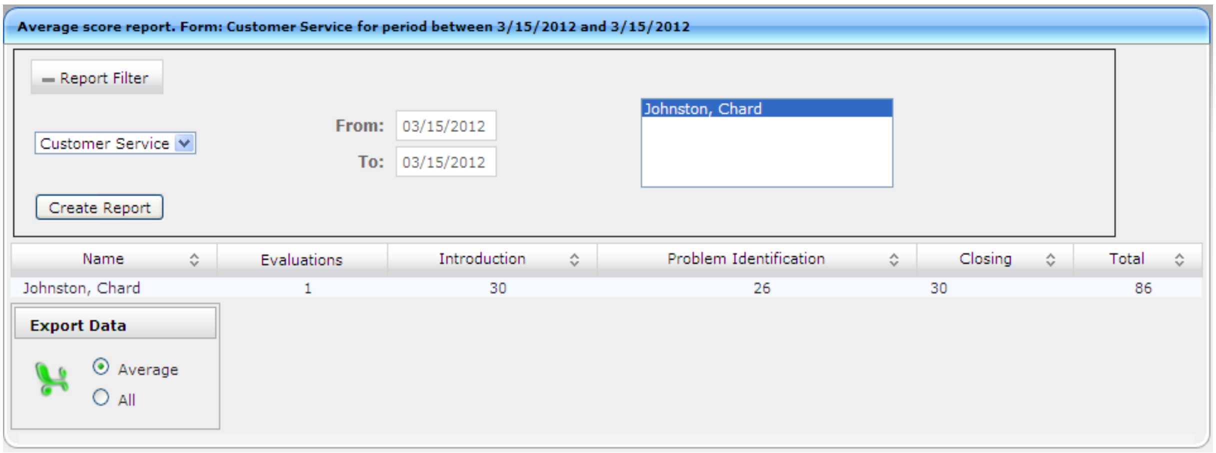
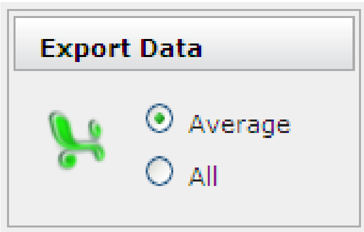


Table 6-58: Average Score Report – Field Descriptions

Field	Description
— Report Filter	Click to hide the report filter.
+ Report Filter	Click to show the report filter subscreen.
Select form	Dropdown menu with evaluation forms.
From:	Search from this call date(s). Automatically populated by SmartTAP; can be changed by the user.
To:	Search before this call date(s). Automatically populated by SmartTAP; can be changed by the user.
List of users	List of evaluees. Automatically populated by SmartTAP; select by clicking the required user.
Create Report	Only active when an Evaluee is selected.
Only visible after clicking Create Report	▪ **Name** (Name of Evaluee) ▪ **Evaluations** (Number of evaluations for this user) ▪ **Name of section (from form)** (Total points in this section. In the figure above, the section name is 'Introduction'. Clicking this header sorts the search results in Ascending/Descending order alternating with each click). ▪ **Name of section (from form)** (Total points in this section. There is a column for each section in the form. Clicking this header sorts the search results in Ascending/Descending order, alternating with each click. ▪ **Total** (Total points in this evaluation)  Click to export data to Excel.

➢ **To create a report:**

1. Open the Average score report screen (**Evaluation** tab > **Evaluation** folder > **Report**).
2. Select the evaluation by entering the search data into the report filter area.
3. Click Create Report to create the report; the report is displayed on the screen.

➢ **To export a report (to Excel):**

1. Create the report as described above.
2. Select the **Average** or **All** button and click to export the data; you're prompted to save or open the exported file.

6.14 Managing Instant Messages

Instant Messages are managed in the Search Messages Navigation screen, under the Messages tab. These messages reflect either person-to-person chat between two users or group chat between two or more users. When you select a conversation record (as shown below), you can view the action conversation made between the parties (as shown below).

Figure 6-131: Managing Messages

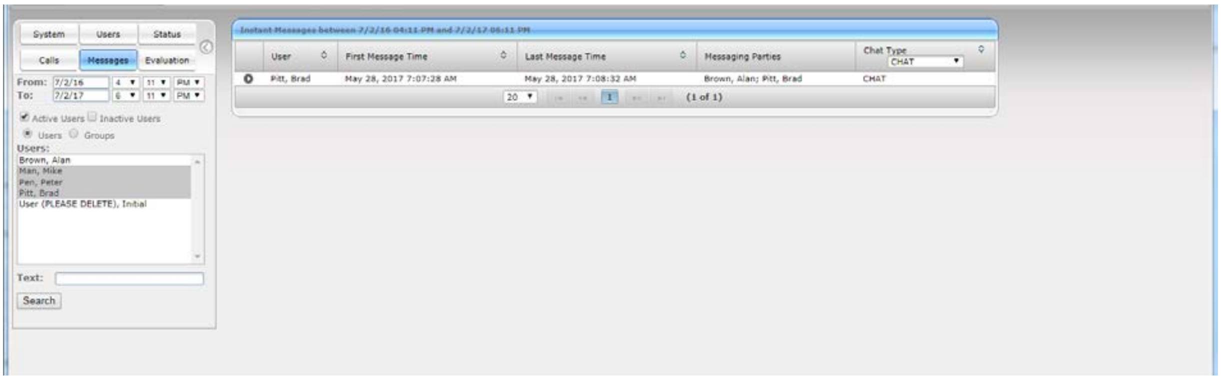


Figure 6-132: Instant Message Display

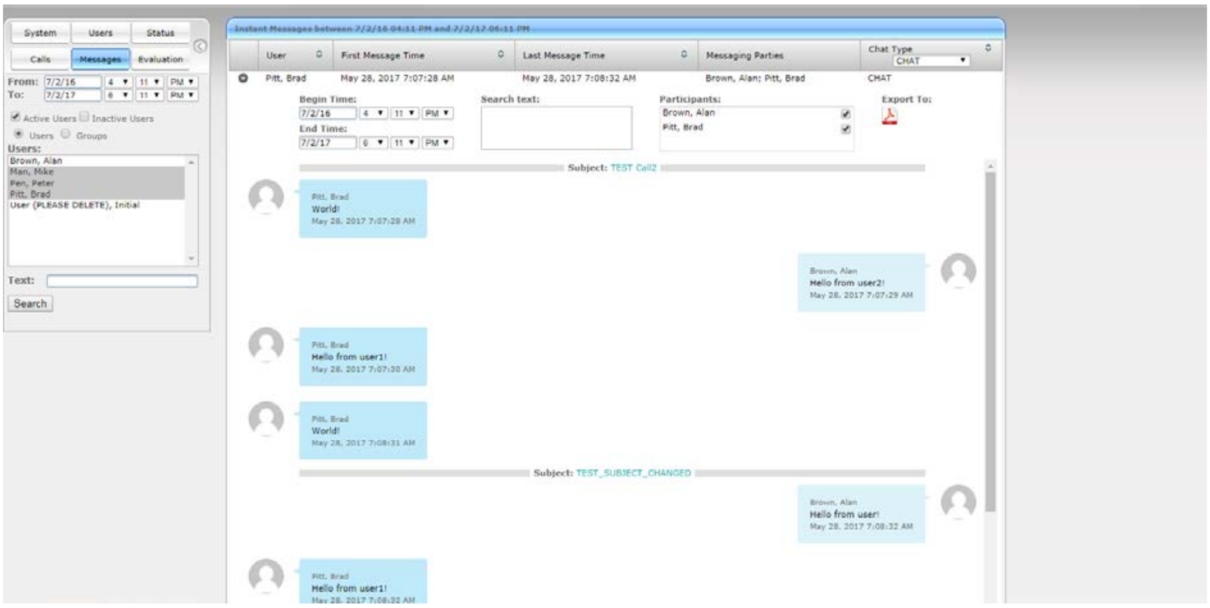
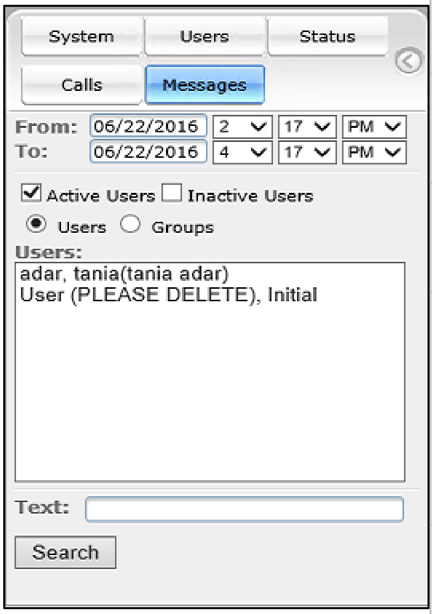


Table 6-59: Search Messages Navigation Screen - Messages Tab

Search Messages Navigation	Field	Description
	From:	Earliest date and time to search from. Click the date field for a calendar to pop up showing one month at a time. Use the dropdown to change the time of day.
	To:	Latest date and time to search to. Click the date field for a calendar to pop up showing one month at a time. Use the dropdown to change the time of day.
	Active Users	Users whose account is enabled in the SmartTAP application.

Search Messages Navigation	Field	Description
	Inactive Users	Users whose account has been deleted from the SmartTAP application.
	Users	Only Users will be listed in the Search list. Either the **Users** or the **Groups** option must be selected.
	Groups	Only Groups will be listed in the Search list. Either the **Users** option or the **Groups** option must be selected.
	Users (list)	Select the User to search for by clicking their name. To select multiple Users, hold down the <Ctrl> key and click each User to search for. To select a range of Users, hold down the <shift> key, click the User at the top of the range and the User at the bottom of the range.
	Groups (list)	Select the Group to search for by clicking its name. To select multiple Groups, hold down the <Ctrl> key and click each Group to search for. To select a range of Groups, hold down the <shift> key, click the Group at the top of the range and the Group at the bottom of the range. Calls for all users in the groups selected will be searched.
	Text	Searches for message conversations that contain the entered text. The search string may contain words to search for, and 'operators' (AND, NOT, words contribution, exact match, and more) to specify search criteria.
	Search	Click to search and display results.

6.14.1 Searching for Messages

This section shows how to search for messages.

➢ **To search for messages:**

1. Click the **Messages** tab to open the Search Messages screen.
2. In the Search Navigation screen (left side of the screen), enter the time range, and then select the type of Users.

Note: When searching for messages within a time range, only conversations that contain messages within the provided time range will be returned in the search results.

3. Select either the **Users** or the **Groups** option.
   - Selecting the **User** option changes the display below to show a list of Users.
   - Selecting the **Groups** option changes the display below to show a list of Groups and Sub Groups (if the **Search Sub Groups** option is selected).
4. Select one of more User or Groups by highlighting them in the list (see the notes above on Search Calls Navigation screen fields and on how to select more than one User or Group).
5. Optionally, enter the text for search output conversations to contain. Instant messages and conversations can be filtered using SmartTAP's Full-Text search feature built on top of 'MySQL Boolean Full-Text Search'. The search field value is logically ANDed and applied to the instant messages search criteria. All instant message conversations that have at least one message with the matching search text as part of the message body will be displayed in the instant message conversations table. MySQL Boolean full-text search supports the operators shown in the table below. More detailed examples can be found inside MySQL online documentation, available at http://dev.mysql.com/doc/refman/5.6/en/fulltext-boolean.html
6. If files are sent between two call parties, you can search for the filename in the free 'Text' field (see example in Figure 6-137).

Table 6-60: Operators Supported by MySQL Boolean Full-Text Search

Operator	Description	Example
+	A leading or trailing plus sign indicates that this word must be present in each message that is returned.	'+apple +juice' Find messages that contain both words. '+apple juice' Search messages that contain the word 'apple', but rank rows higher if they also contain 'juice'.
-	A leading or trailing minus sign indicates that this word must not be present in any of the rows that are returned.	'+apple -juice' Find messages that contain the word 'apple' but not 'juice'.
(no operator)	By default (when neither + nor - is specified), the word is optional, but the conversations or messages that contain it are rated higher.	'apple -juice' Search rows that contain at least one of the two words.
@distance	It tests whether two or more words all start within a specified distance from each other, measured in words.	'"word1 word2 word3" @8' Search for matching messages where word1, word2 and word3 are separated by a distance of 8 words from each other.

Operator	Description	Example
> <	These two operators are used to change a word's contribution to the relevance value that is assigned to a conversation or message. The > operator increases the contribution and the < operator decreases it.	'+apple +(>turnover <strudel)' Find messages that contain the words 'apple' and 'turnover' or 'apple' and 'strudel' (in any order), but rank 'apple turnover' higher than 'apple strudel'.
( )	Parentheses group words into subexpressions. Parenthesized groups can be nested.	
~	A leading tilde acts as a negation operator, causing the word's contribution to the message's relevance to be negative. A message containing such a word is rated lower than others, but is not excluded altogether, as it would be with the - operator.	'+apple ~macintosh' Find messages that contain the word 'apple', but if the message also contains the word 'macintosh', rate it lower than if message does not.
*****	The asterisk serves as the truncation (or wildcard) operator. Unlike the other operators, it is appended to the word to be affected. Words match if they begin with the word preceding the * operator.	'apple*' Find messages that contain words such as 'apple', 'apples', 'applesauce' etc.
"	A phrase that is enclosed within double quote ("""") characters matches only rows that contain the phrase literally, as it was typed.	"some words" Find messages that contain the exact phrase "some words".

Note: Some words (also known as stopwords) are ignored in full-text searches. In SmartTAP, the minimum length of the word for full-text searches is 2.

7. Click to start the search for the Messages matching the search criteria; the results are displayed in the Search Messages Results screen to the right.
8. From the Chat Type drop-down list, select either **Chat** or **Group Chat**; the results are filtered accordingly.

Figure 6-133: Search Messages Results-Person-to-Person Chat

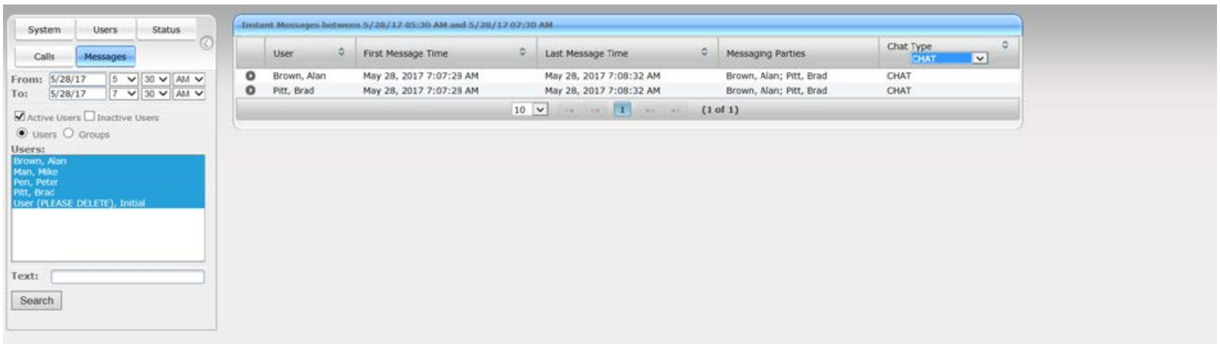
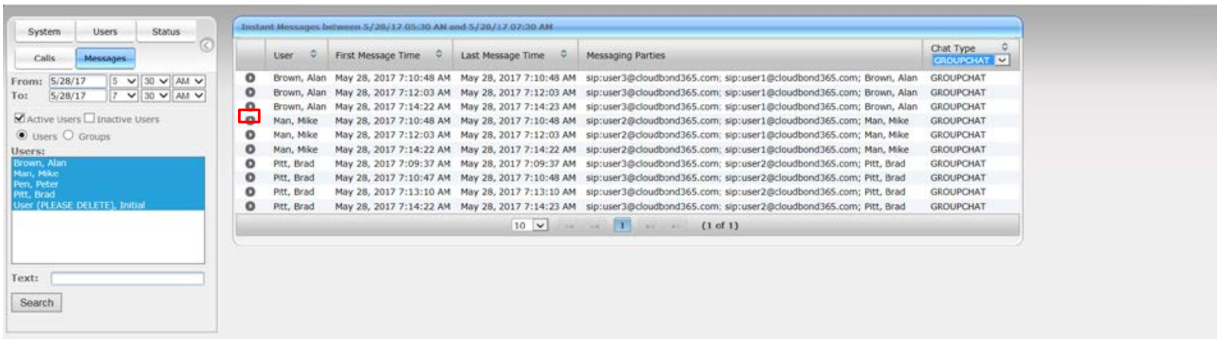


Figure 6-134: Search Messages Results-Group Chat



The search result fields are described in the table below.

Table 6-61: Search Messages Results

Field	Description
User	User name. Clicking this header sorts the search results in Ascending/Descending order, alternating with each click.
First Message Time	Date and time of the first message in the conversation. Clicking this header sorts the search results in Ascending/Descending order alternating with each click.
Last Message Time	Date and time of the last message in the conversation. Clicking this header sorts the search results in Ascending/Descending order alternating with each click.
Messaging Parties	The column represents messaging parties, parties which sent or received the conversation messages.
Chat Type	The following chat types can be chosen: ▪ Chat: person-to-person chat ▪ Group Chat: chat for two or more persons. For Group Chat, the Conference ID is also displayed.

9. Click the arrow adjacent to the message whose conversation details you wish to view.

   Example conversations are displayed below. Note that when files are sent between two parties, the file information is also displayed in the conversation dialog (see example in Figure 6-137).

Figure 6-135: Search Messages Results-Person to Person Chat

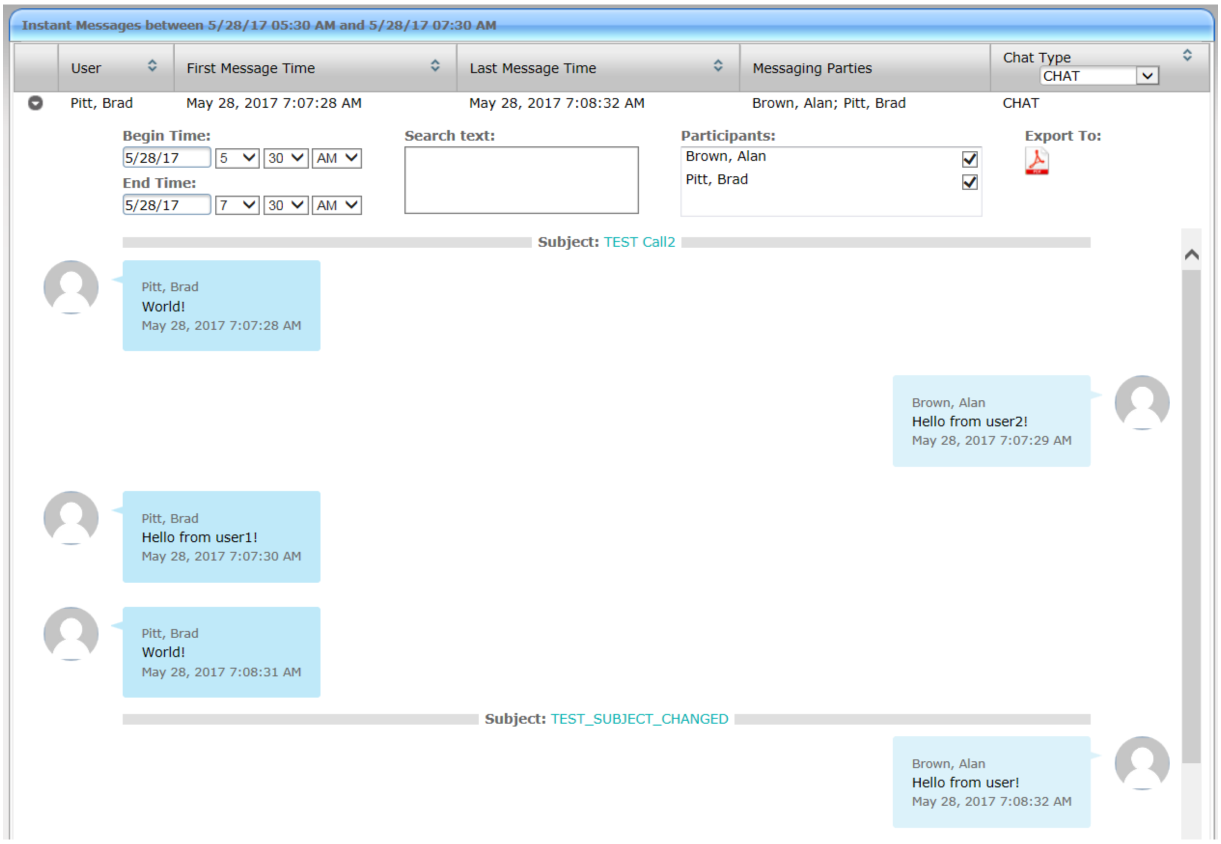


Figure 6-136: Group Chat Recording

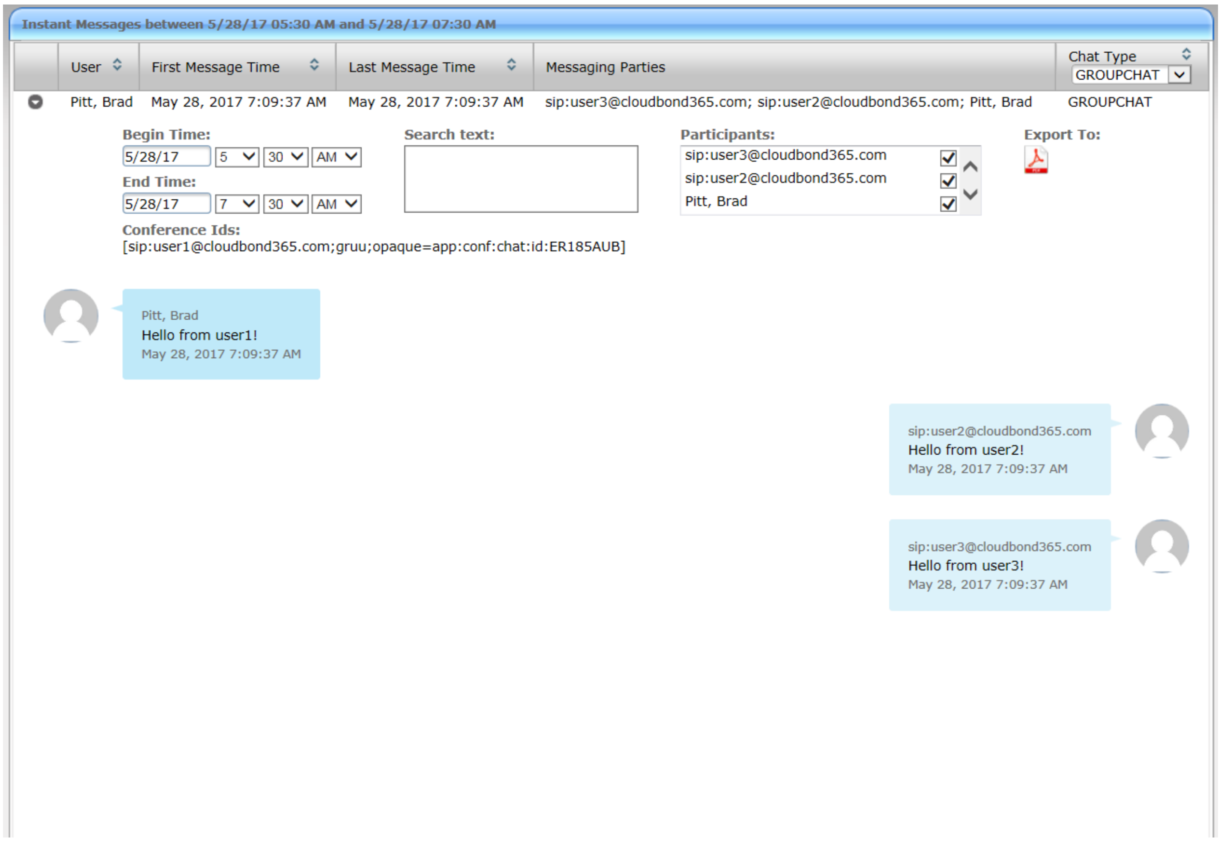


Figure 6-137: File Transfer Messages

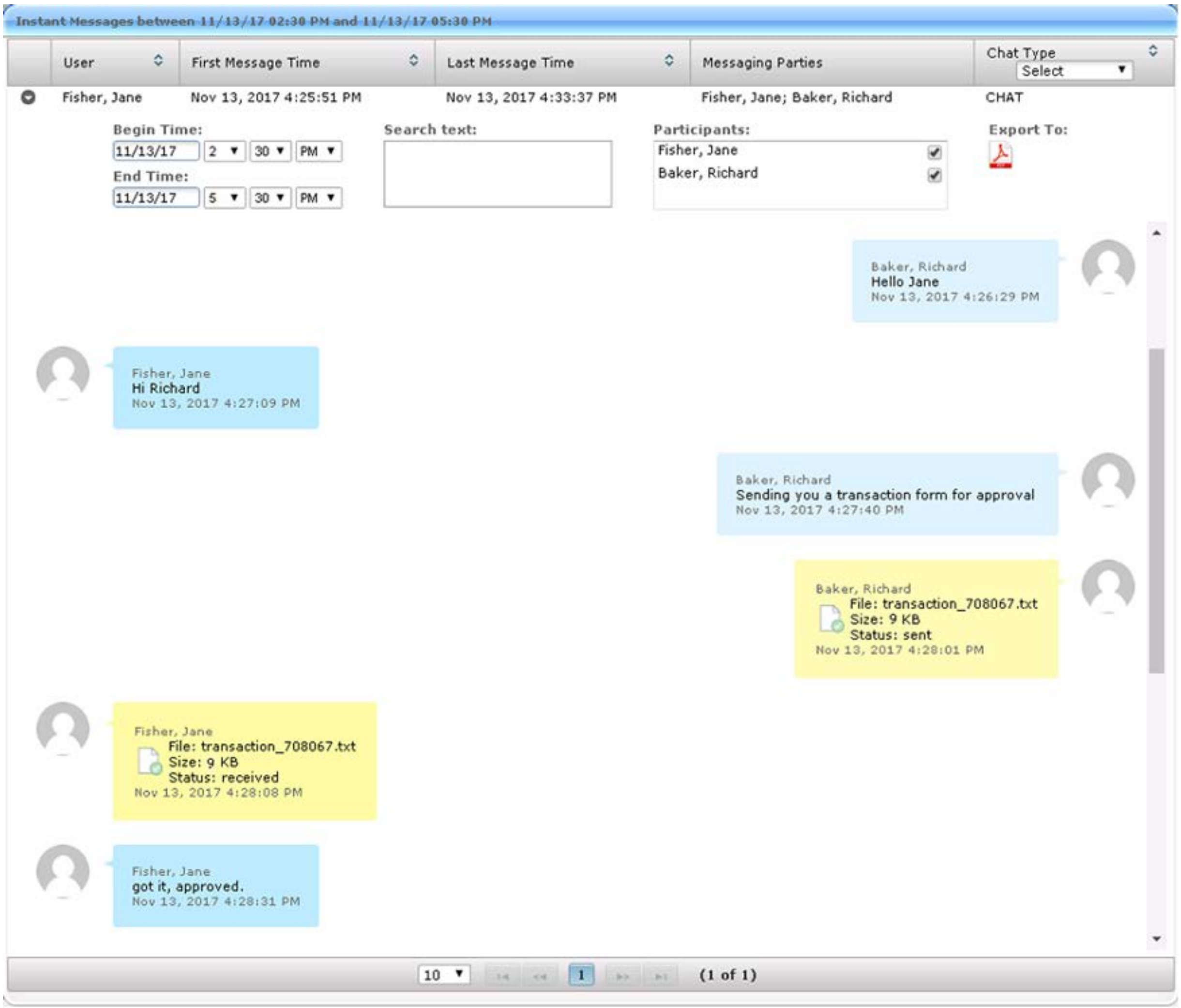


Table 6-62: Message Conversation Content – Field Descriptions

Field	Description
Begin Time	Specifies the time of the first message of the conversation.
End Time	Specifies the time of the last message of the conversation.
Search text	Filters the conversation display to show messages containing the search text. In addition, this field allows the searching for filenames (where Files have been transferred between parties).
Participants	Parties who received or sent messages of the conversation.
☑	Filter the conversation to present messages of a specific participant.
Export To:	Export the conversation messages to a PDF file (including file transfer information from messages)

Note: SmartTAP presents a collection of messages in one conversation based on the time and participants.

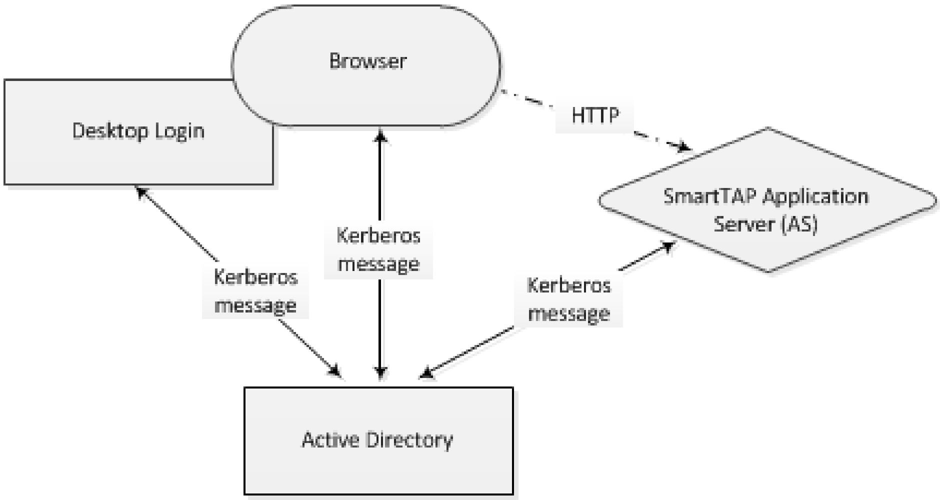
A Single Sign-On for SmartTAP

Single Sign-On (SSO) simplifies the login process for domain users. The user logs into their machine using domain credentials and then attempts to access the SmartTAP Web server via a Web browser such as IE, Chrome or Firefox.

Without SSO, the user is directed to a simple login form in which a Username and Password are entered and given to SmartTAP to authenticate.

With SSO enabled, the user is authenticated in the background through Active Directory using the same domain credentials that were used to log into the machine. This bypasses the login page and immediately brings the user to their Welcome page. This allows for a streamlined entry to the SmartTAP Web interface and for quick external links to different SmartTAP pages.

Figure A-1: Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) Web Authentication Service



Note:

- Before getting started, contact AudioCodes Support to make sure your network is SSO-ready. In some environments, if users from two different domains attempt to perform SSO to the SmartTAP server, it can create an issue.
- SSO was successfully tested with both Client Users and the SmartTAP server on the same domain with a single Active Directory server.
- SSO was successfully tested with Client Users on one domain and with the SmartTAP server on a separate domain, with one-way forest trust between the domains.

A.1 Prerequisites

LDAP configuration is optional if all Clients using SSO were manually added to the SmartTAP database. If they were not manually added, then LDAP *must* be configured so that SmartTAP can validate the user and find the user's Roles/Permissions.

LDAP configuration is outside of the scope of this appendix.

A.2 Variables for Configuring Single Sign-On

A.2.1 Getting Acquainted with Terms

Before configuration, it's best to get acquainted with the terms used (see also the Variables List in Section A.2.2 below). Use the table below as a reference.

Table A-1: Terms

Term	Meaning
{username}	New domain user required for SmartTAP to authenticate through SSO. Referred to as the 'SSO User'. Use a different user for SSO and LDAP if possible, in order to simplify later steps and facilitate troubleshooting. In this Appendix, **testUser** is used.
{domain}	The complete name of the domain to be used for SSO, for example, **myDomain.local**.
{realm}	The security realm to be used for authenticating the SSO User. Can be different to the realm of the SmartTAP server and should be the realm of the SSO User. The realm *must be specified in capital letters.* In the example of a single domain used in this Appendix, the realm is the same as **{domain}**: **MYDOMAIN.LOCAL**.
{kdc}	The fully qualified domain name (FQDN) of the Key Distribution Center (KDC) which must be the Active Directory server to be used to authenticate the SSO User (created in the next step). Example: **ad.myDomain.local**
{user password}	The password defined for the SSO User when created. In this Appendix: **testUserPassword**
{short domain}	Shortened version of **{domain}** used to reference user logins such as **myDomain\userName**. Using the same example as above, it would be just **myDomain**.
{hostname}	The fully qualified domain name (FQDN) of the SmartTAP server. Must be in the form **{machine name}.{domain}**. Example: smarttap.myDomain.local. If a CNAME alias is used to map an unfriendly machine name to a friendlier one such as **smarttap**, the original machine name must be used.
{principal}	Special string defining a service running on a host within a security realm, in this case, HTTP/**{hostname}**@**{realm}** Example: HTTP/smarttap.myDomain.local@MYDOMAIN.LOCAL

A.2.2 Variable List

For reference, note your variables here. It may be useful to print out this page and write them all down, or to fill in these details in this or another document.

{username}____

{user password} ____

{domain} ____

{short domain} ____

{realm} ____

{hostname} ____

{kdc} ____

{principal} ____

A.2.3 Validate the Hostname to be Used for the Principal Name

A CNAME alias for the SmartTAP server can cause problems when used as part of the Principal Name. A Client machine will request a Kerberos ticket for the FQDN using the actual hostname, not the version using the CNAME. So the Principal to be used must contain the name that the Client will be requesting.

Validate that the hostname is OK to use in the Principal by pinging the name from the command shell:

```
ping {hostname}
```

The command shell then prints out

```
Pinging {ping destination name} [IP Address]
```

If **{ping destination name}** is the same as **{hostname}**, then this is the correct hostname to use for the Principal. If different, then the correct hostname must be investigated further. Most likely, **{ping destination name}** is the correct one to use. However, SSO may have to be configured in SmartTAP and Wireshark run in order to see what hostname the Client machine will use when requesting a ticket from Kerberos.

A.2.4 Windows KTPASS Command and Choice of User

Active Directory must then be commanded to map the HTTP service on the SmartTAP server to the newly created user. The `ktpass` command included on Windows servers will be used. It must also be run on the Active Directory server.

`ktpass` changes the SSO user's attributes. It strips the realm from the data specified in the command when setting the user attribute. The realm *must* be specified in the command as it will be part of the next attribute that is modified. Using the `setspn` command does the same thing. The user's **userPrincipalName** is then changed to be the complete Principal Name. This makes it appear as if the user's login ID is now the Principal Name but **sAMAccountName** is unchanged.

`ktpass` most importantly creates the keytab for the Principal. SmartTAP does not need this file to be exported. The Client obtains an encrypted version of the keytab and sends it to SmartTAP as part of the authentication process.

Note on Choice of User & Security Concerns: The domain administrator for security reasons may not want to run the `ktpass` command with the user's password within the command arguments, as others can discover the username and password by watching the process and its input arguments.

Instead of entering the password, the domain administrator can use the **-pass *** option. The user is then prompted for the password. Although more secure, in some cases this changes the user's password within Active Directory. If this user is used by SmartTAP for SSO only, this is acceptable. If the user is also used for LDAP, LDAP authentication will fail after the password is changed. Manually resetting the user's password in Active Directory corrects the LDAP authentication error but breaks the mapping performed by `ktpass` and therefore SSO fails.

The only way to use SSO and LDAP while also using the **-pass *** option is to use two separate users for SmartTAP – one for SSO and one for LDAP. For simplicity, try to use two different users for LDAP and SSO to facilitate troubleshooting and configuration.

A.2.5 User Properties – Before and After Running `ktpass`

Before and after running the `ktpass` command, observe the changes to the SSO User to determine what user properties are modified. Use the screenshots below as reference. If the command is successful, the user's properties will not need be validated in Active Directory.

Figure A-2: Before Running the `ktpass` Command

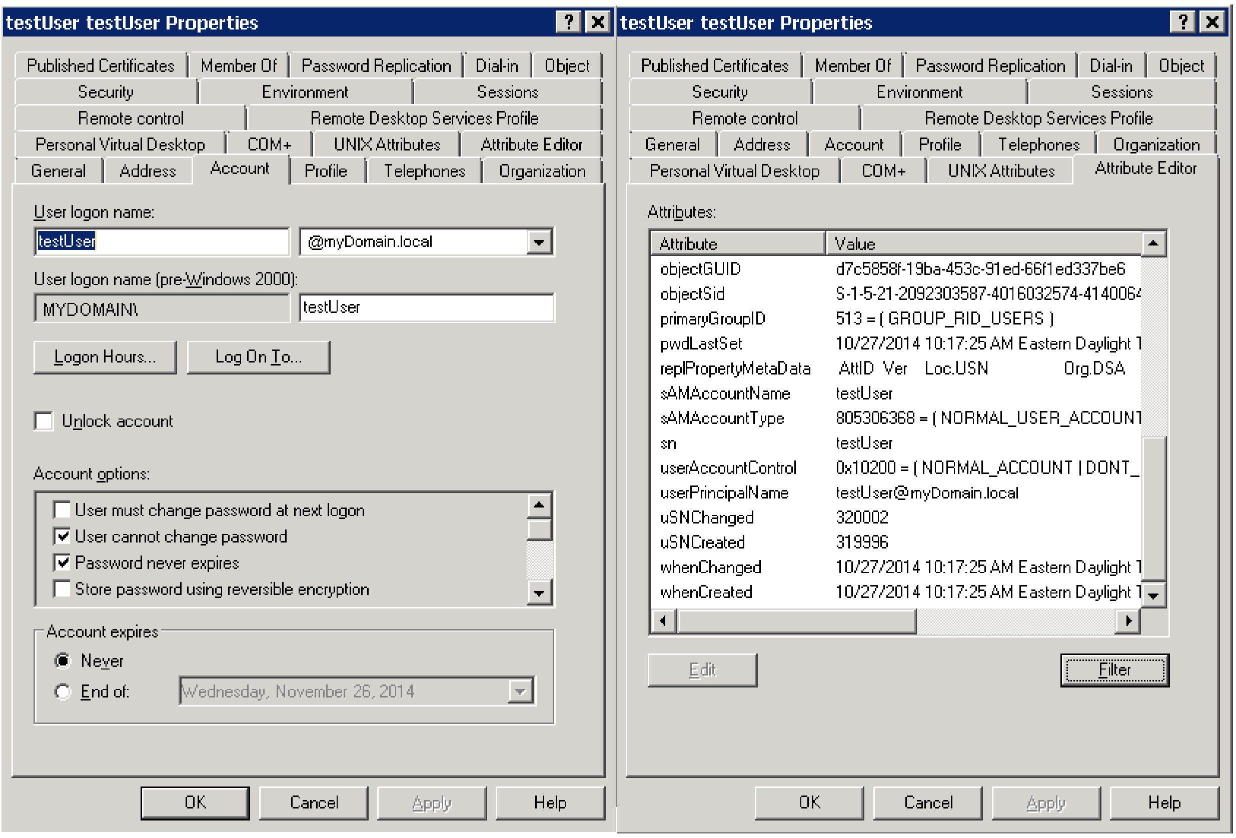
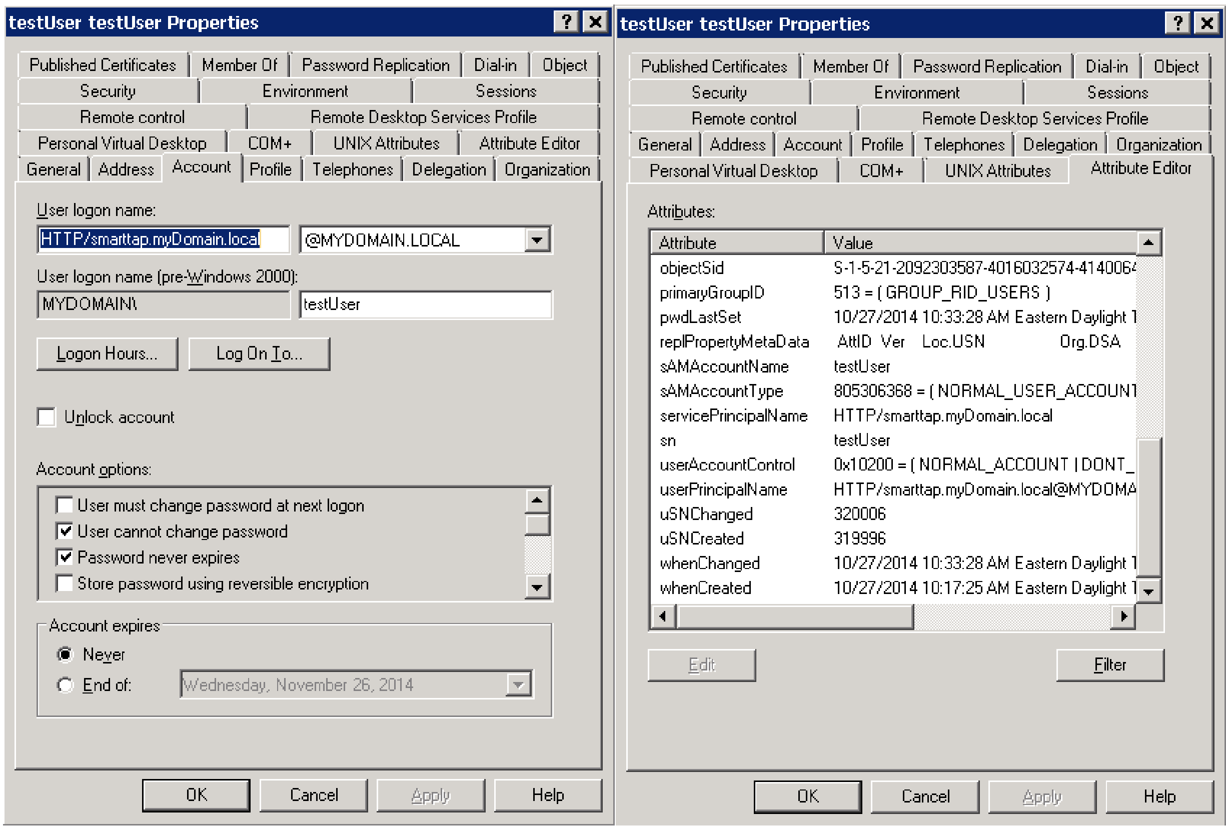


Figure A-3: After Running the `ktpass` Command

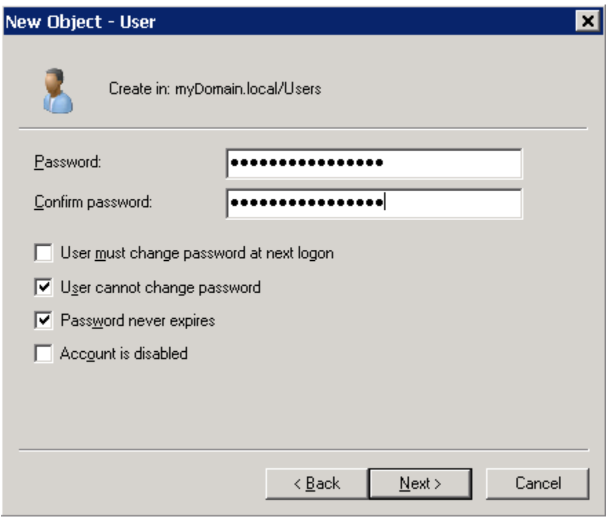


A.3 Configuration for Active Directory

A.3.1 Create a New Domain User

A dedicated user called 'Single Sign On User' or 'SSO User' is required on the domain for the SmartTAP Application Server to use for authenticating clients login attempts. The SSO User is only to be used within SmartTAP and should not be used to log into any machine on the domain, including the SmartTAP server. It is recommended to create this user and to select the options ‘Password never expires' and 'The user cannot change password' as shown in the figure below. Assign the username a login ID of **{username}** and a password of **{user password}**.

Figure A-4: Create a New Domain User



A.3.2 Active Directory Commands - `ktpass`

Run the `ktpass` command *on the Active Directory server that corresponds to the domain for the SSO User*. You *must* use the exact syntax shown below. This is critical for flawless SSO operation. Mistakes are difficult to troubleshoot. Note that the `–out` option is not used to output the keytab file.

```
ktpass –princ {principal} –mapuser {short domain}\{username} –pass
{user password} –ptype KRB5_NT_PRINCIPAL –kvno 0 –crypto AES128-
SHA1
```

Note on the Level of the Encryption Used:. SmartTAP supports encryption types as high as AES-128 though not all Windows Server OS versions support this level of encryption. It only depends on the OS version, not on the domain’s Functional Level.

- If the Active Directory server is Windows Server 2008 or higher, the **`–crypto`** parameter must specify **AES128-SHA1**.
- If the Active Directory server is Windows Server 2003, the **`–crypto`** parameter must specify **RC4-HMAC-NT**.

Example:

```
ktpass –princ HTTP/smarttap.myDomain.local@MYDOMAIN.LOCAL –mapuser
myDomain\testUser –pass testUserPassword –ptype KRB5_NT_PRINCIPAL
–kvno 0 –crypto AES128-SHA1
```

When running flawlessly, the command outputs:

```
Targeting domain controller: <DC hostname>
Successfully mapped {principal} to {username}.
Key created.
```

The command may take a few minutes to propagate through the network. It's recommended to log out and then back in on any client machines that will attempt SSO, in order to speed up the process for laboratory testing. This ensures that the Client machine is not caching any Kerberos tickets that will be out of date after making changes to the User in Active Directory. If the Client machine used for testing has not previously accessed the SmartTAP server, logging out is unnecessary.

The command parser sometimes gets invalid characters when copy/pasting the command. If you see the error `unknown option 'ûprinc'.` try manually typing the command in or try retyping all the '-' characters again. Note the error indicates **ûprinc** instead of **-princ**.

A.3.3 Verify the User's Credentials

AudioCodes has observed cases in which the `ktpass` command changed the user's password even when explicitly defined in the `ktpass` command. To avoid confusion later, make sure the user's credentials are still correct. From the command prompt on either the SmartTAP server or the Active Directory server, run the command:

```
runas /user:{short domain}\{username} cmd
```

A new command window is opened using the SSO user's credentials. You're prompted for the SSO user's password. Enter it.

- If a new command window launches, the password is correct and you can continue to the next step.
- If the password is incorrect, an error will be displayed in the command window. Some errors indicate that the user credentials are incorrect, thus the password is no longer valid. Other errors indicate that the user credentials are OK, but the command failed for other reasons.

Error 1326: Logon failure: unknown user name or bad password indicates that the credentials are incorrect. Make sure the username and password are correct. If this error persists it means the user's password must have been changed. If this fails to run and SmartTAP is configured with the same password, then Single Sign-On will fail. Try resetting the password in Active Directory and re-running the `ktpass` command to make sure the password is correct. Repeat this test to validate that the user's credentials are still known before continuing.

Error 1385: Logon failure: the user has not been granted the requested logon type at this computer indicates that the password is correct but the SSO user is disallowed from running the command. This is acceptable for testing purposes.

A.4 Configuration on SmartTAP Server

The SmartTAP server must be added to the domain. The rest of the SmartTAP configuration is performed through the Web portal. You can use any Web browser to access the SmartTAP Web page. Initially, SSO is disabled, so the usual login form must be used. Log in with any account with permissions such as the default administrative user **admin** to make system changes to SmartTAP.

➢ **To configure SSO:**

1. Open the SSO Web Configuration page (**System** tab > **System** > **System Settings** > **Web**).

Figure A-5: SSO Configuration

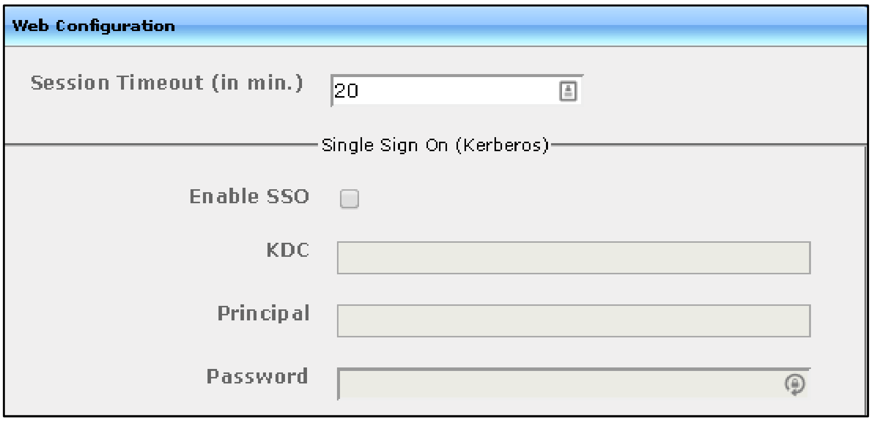


Table A-2: SSO Configuration Parameters

Parameter	Description
Enable SSO	Select this option to enable Single Sign-On.
KDC	Key Distribution Center, which is probably located on the Active Directory server. Enter **{kdc}**. In the example shown in this Appendix, **ad.myDomain.local** is used.
Principal	The Service Principal Name mapped in the previous steps. Enter **{principal}**. Note: The principal name must include the security realm. **HTTP/smarttap.myDomain.local@MYDOMAIN.LOCAL** is used in the example in this Appendix.
Password	The password set previously in Service Principal Name Mapping. Enter **{user password}**. **testUserPassword** is used in the example in this Appendix.

2. Submit the changes when complete; a status message is displayed at the top of the screen indicating that the entries were validated and applied; a popup is displayed warning that the SmartTAP Application Server must be restarted for the changes to take effect.
3. Restart the SmartTAP Application Server.

A.4.1 Validation

The page validates some of the parameters entered but cannot fully validate that SSO is functioning flawlessly.

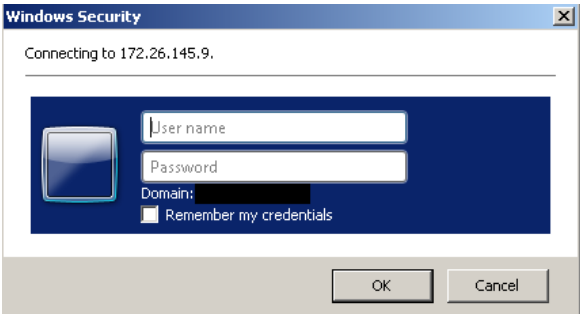
- The KDC hostname is resolved into an IP address. If the name cannot be resolved, an error is issued indicating that the KDC is invalid.
- The Principal name is parsed to ensure it contains the service, hostname and realm. Text for the service (HTTP) is followed by a forward slash **/** which is followed by more text for the principal name and a @ which is followed by the text for the realm. Each part of the name is not checked and is used as given.
- The password is not validated in any way and is taken as entered.

A.5 Configuration on the Client's Browser

After enabling SSO on SmartTAP as shown above, the Web server requests that each client's Web browser negotiate authentication. Most browsers are configured to dislike this negotiation without making any changes and present this condition to users differently.

A.5.1 Internet Explorer Browser Settings

When browsing to the SmartTAP Web server, IE prompts the user for credentials. This is *not* the SmartTAP login form but rather a prompt *from IE*. The user *could* enter the domain credentials to log in but this would not be SSO.

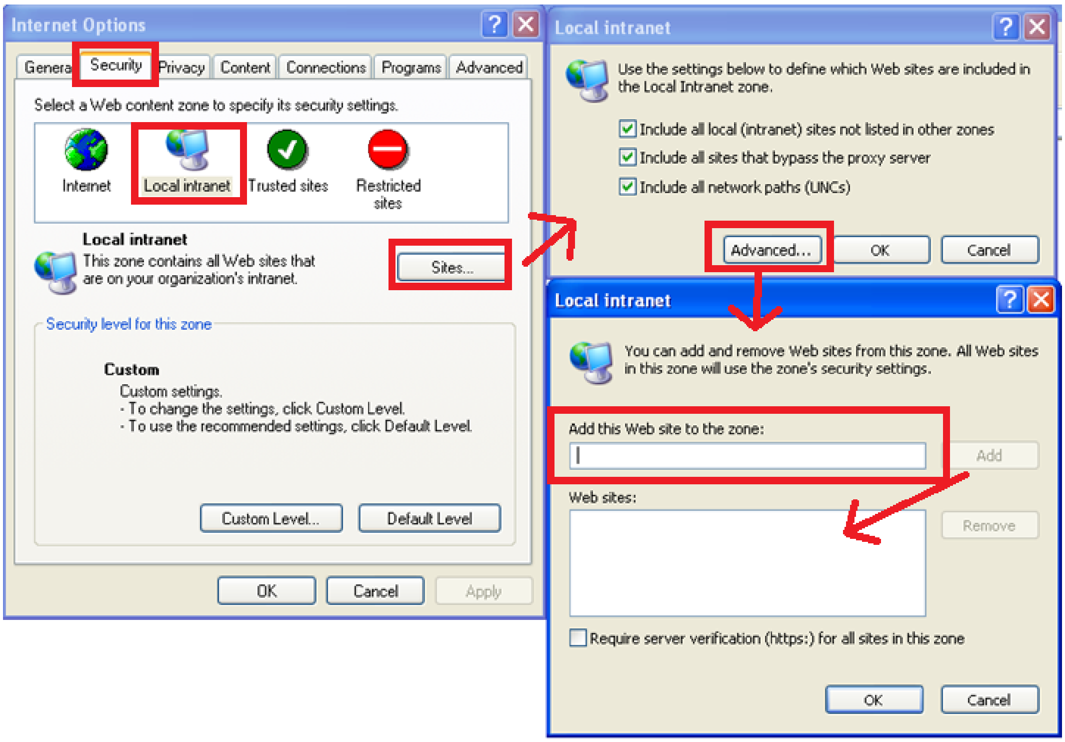


You must allow IE to negotiate with the SmartTAP Web server. Each browser features a different way of enabling this security feature. IE must be configured to 'trust' the SmartTAP server. IE must be instructed that the SmartTAP server is part of the local intranet so that IE can send proper authentication to the SmartTAP Web server.

➢ **To do this:**

1. In IE, open **Internet Options** > **Security** tab > **Local Intranet zone** > **Sites…** > **Advanced…** > add the SmartTAP FQDN to the local Intranet zone.
2. Click **OK** to close all windows. All IE instances must be closed.

Figure A-6: Internet Explorer Browser Settings



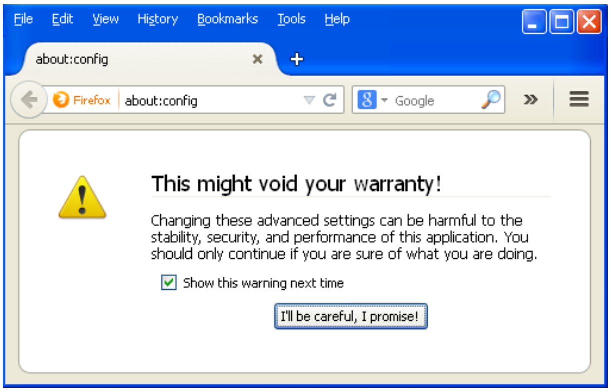
A.5.2 Firefox Browser Settings

Firefox issues a 401 error code instead of negotiating security.

➢ **To configure Firefox:**

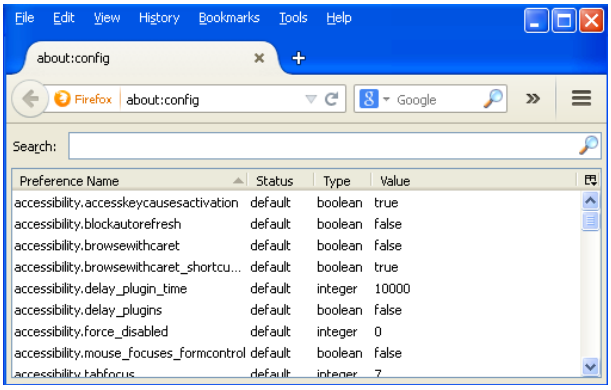
1. Open Firefox, enter the URL **about:config** and then press Enter; Firefox warns you're updating its internal settings.

Figure A-7: Firefox Advanced Settings



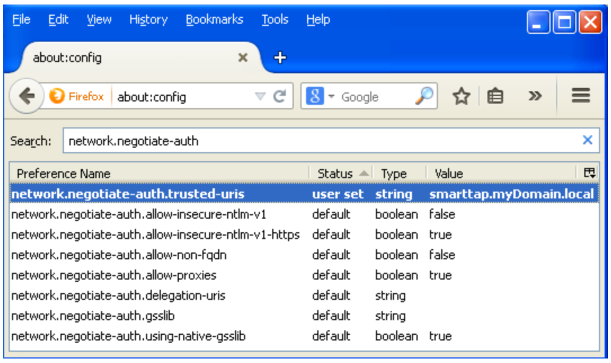
2. Click the button to continue; Firefox lists all the internal configuration options in the Web page, allowing changes to be made.

Figure A-8: Firefox about:config



3. In the 'Search' field, enter **network.negotiate-auth** to show all negotiation options. **SmartTAP FQDN** must be added to the list of trusted URIs by updating the option **network.negotiate-auth.trusted-uris**. Restart Firefox; SSO now functions on Firefox.

Figure A-9: Firefox about:config



Note that additional changes may be required for Firefox. If SSO does not function immediately after these changes, see Section A.9.

[Tested: Firefox 32.0.3 on Windows XP and Windows 7. Also Firefox 35.0.1 on Windows 7].

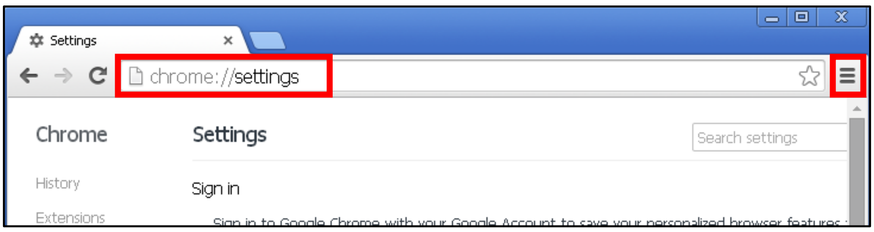
A.6 Google Chrome Browser Settings

Without changes to the configuration, Google Chrome prompts the user for Domain Credentials, similarly to IE. The Google Chrome browser uses the same underlying network configuration that IE uses. Configure IE and Chrome will accept the same settings.

➢ To configure directly through Chrome:

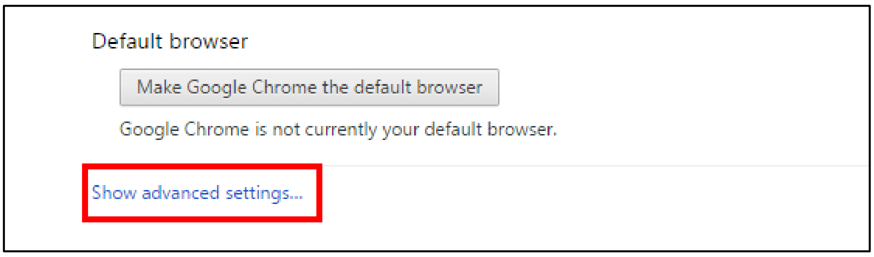
1. Open the Chrome browser and click the menu icon ≡ located to the right of the address field, and then select **Settings**. Alternatively, browse to **chrome://settings**.

Figure A-10: Google Chrome Browser Settings



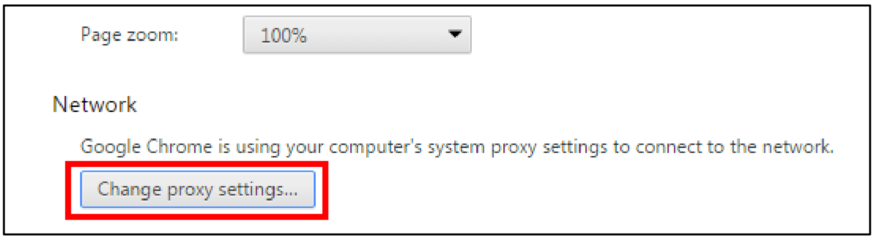
2. Scroll down to the bottom of the page and click the link **Show advanced settings…** If the advanced settings are already displayed, you can skip this step.

Figure A-11: Google Chrome Browser Settings – Show advanced settings



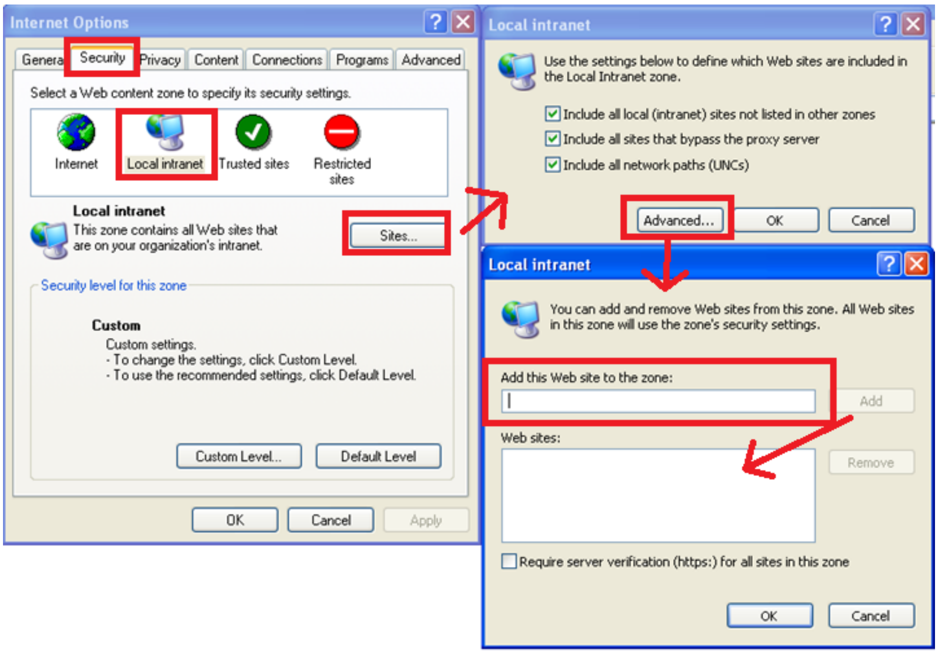
3. Locate the 'Network' setting and click the button **Change proxy settings…**; the same Internet Options window used for Internet Explorer opens, but it opens in Chrome under the **Connections** tab instead of the **General** tab as in IE.

Figure A-12: Google Chrome Browser Settings – Change proxy settings



4. Follow the same instructions as IE (**Security** tab > **Local Intranet zone** > **Sites…** > **Advanced…** > add the SmartTAP FQDN to the local Intranet zone).
5. Close all Google Chrome windows and restart; SSO now functions.

Figure A-13: Google Chrome Browser Settings – Adding a Web Site to the Zone

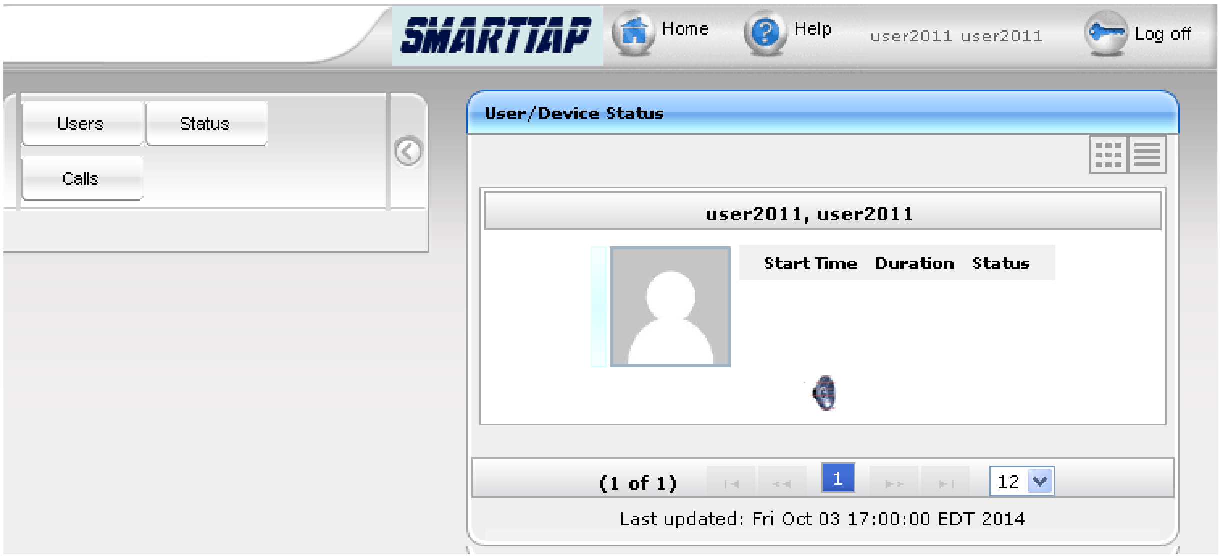


A.7 Testing Single Sign-On

After logging into the domain computer and configuring the browser to trust the SmartTAP server as described in previous sections, you can browse to the SmartTAP Web server, preferably via the SmartTAP server's FQDN. You may briefly see the Redirecting notification:

You're then brought directly to the Home page that corresponds to your user. The figure below shows the Home page of an Agent by the name **user2011**.

Figure A-14: Browsing to the SmartTAP Web Server



If an error page is displayed, or if the normal login form for SmartTAP is displayed, SSO has malfunctioned – see Section A.9.

A.8 Frequently Asked Questions

When SSO is enabled, how can I log in as the default SmartTAP administrative user?

SSO is enabled, so all login attempts will automatically attempt SSO as the domain user logged into the client machine. The SmartTAP administrative user (default username = admin) will likely not be a user in Active Directory, so it cannot be used to log into the client machine and log in to SmartTAP via SSO. The form login page of SmartTAP must be accessed in order to log in as this user.

It is recommended that a domain user be given valid SmartTAP permissions to make system changes so that the default SmartTAP administrative user can be removed.

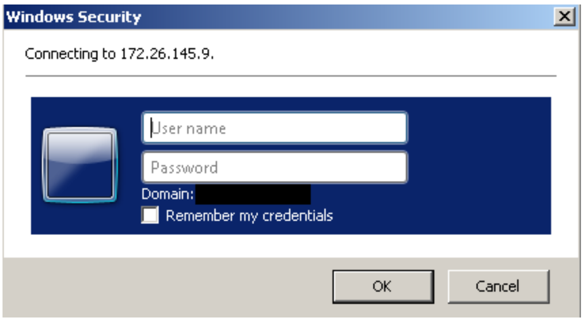
How can the form login page be accessed for non-SSO logins?

There are a few ways to do this:

- Browse to the SmartTAP server using its IP address instead of the FQDN. SSO will not function this way, so the form page will be displayed. The IP address can be obtained by pinging the hostname from a command prompt.
- Access the SmartTAP Web server from a machine that is not on a domain. As a result, no domain credentials will be available, SSO will fail, and the form login page will be displayed.
- For some internet browsers such as IE, if the trust relationship is not present (SmartTAP server hostname is not configured as an Intranet site), you may be able to access the form login page. See the next question.

Why do I see a popup window in my Web browser asking me for credentials?

When a client accesses the SmartTAP Web server, the server requests the client browser to negotiate authentication. If the browser can determine the credentials from the user's login, it will be used. However, if the browser does not trust the Website, or the user is not in the domain, the internet browser will often prompt the user for credentials, displaying a popup window. Example (IE):



This prompt is prompting for the client's domain credentials, *not* the SmartTAP login credentials.

What can I do with this login prompt?

There are a few directions this prompt can go.

- Enter a valid username and password for a domain user; SSO will be attempted using those credentials. If successful, you will be logged into SmartTAP as that user.
- Pressing the **Cancel** button aborts the login attempt and presents you with a 401 error page.
- Entering an invalid username and password combination will attempt SSO but it will fail and the form login page will be displayed.

A.9 Troubleshooting

A.9.1 HTTP Error Codes

HTTP error codes can provide you with more information about why SSO might fail.

Table A-3: HTTP Error Codes

Error Code	Description
400 – Bad Request	Indicates that part of the HTTP Request is malformed. When using SmartTAP for SSO, the likely cause is that the authentication header being sent by the client is too large. This can occur when the client has many authentication details to send. Simpler networks (such as a laboratory test domain) don't require much data for authentication. As of SmartTAP Version 2.6, the default maximum header length is 8 KB, but instances in which 32 KB was required for authentication information have been observed. A system property must be added to the Smarttap.xml file for the SmartTAP Application Server: **org.apache.coyote.http11.Http11Protocol.MAX_HEADER_SIZE** must be set to an appropriate value. The following tool, available from Microsoft (tokensz), can be used to determine the maximum Kerberos Token size, the main factor in large authentication size: http://www.microsoft.com/en-us/download/details.aspx?id=1448.
401 – Unauthorized	Indicates that the HTTP request requires authentication that was not provided by the browser. Occurs when the user cancels out of the browser prompt for domain credentials, or, if the browser does not have a trust relationship with the SmartTAP server. Can also indicate that the browser is blocking access to the page because it requires some authentication and the security settings are preventing the page from loading. When using Firefox, see Appendix A.5.2.
403 – Forbidden	The user is forbidden from viewing this page. The user was authenticated correctly (SSO is functioning) but is trying to view a restricted page. Can occur if the user manually browses to a page they're not allowed to access. Another cause is if SmartTAP cannot determine the User Roles/Permissions for this user. Make sure the user performing SSO is part of the domain and that SmartTAP can find this loginId through LDAP or in its own database. Make sure LDAP is configured correctly and can communicate with Active Directory.

A.9.2 SmartTAP Application Server Errors

If SSO authentication fails, the Application Server redirects the user to the form page. To determine the reason why SSO fails, you need to review the Application Server logs. This section shows common error messages from the Application Server logs. These are logged at ERROR level so no changes will be necessary in order to view them.

- **No Errors – Using Firefox browser**
    - The Firefox browser will by default just display the 401 Unauthorized error page until the configuration is changed to trust the SmartTAP server (see Appendix A.5.2) though instances occur in which the Firefox browser does not attempt to authenticate even when the SmartTAP server is trusted. In these instances, the user is immediately presented the form login page. When this occurs, no errors are shown in the Application Server since the browser is not attempting authentication.
    - One instance involved using an older version of Firefox and then upgrading to the latest version (35.0.1). After upgrading, SSO didn't function. However, this same version was tested to function on a fresh install and other browsers were found to function with SSO without errors. The error was likely that some previous configuration from the older version of Firefox conflicted with the configuration of the newer version of Firefox. It has not been determined exactly what configuration was causing this error. See Appendix A.10 for instructions on resetting the configuration of the Firefox browser.
- org.ietf.jgss.GSSException is thrown when authenticating with Kerberos server. The failure is unspecified at the GSS-API level (Mechanism level: **Encryption type AES256 CTS mode with HMAC SHA1-96 is not supported/enabled**)
    - The Application Server is trying to decrypt a Kerberos ticket/token that is encrypted using encryption type aes256-cts-hmac-sha1-96 to be referred to in this Appendix as AES256. The 256-bit encryption is not supported on the Application Server so it must not be used.
    - The error was observed when the SSO user was configured in Active Directory with the option **This account supports Kerberos AES 256 bit encryption**. *The highest encryption that can be supported on the SSO user is AES 128.*
    - The error was also observed when the Principal Name contained a CNAME instead of the correct hostname. This caused the Principal Name to query encryption types for the host machine (Server 2008), giving its maximum supported encryption level of AES256. This can be confirmed using WireShark to view the Kerberos request from the client PC when attempting to log in; it will be a different Principal Name to that configured for SmartTAP.
- Javax.security.auth.login.LoginException: **Pre-authentication information was invalid (24)**
    - The likely cause of this error is that the SSO user's password does not match that configured in the SmartTAP GUI.
    - Validate whether the user's password was changed or not - see Section A.3.3.
    - To resolve the error, reset the SSO user's password, re-enter this same password into the SmartTAP GUI for the SSO credentials. You may also need to re-generate the keytab using the `ktpass` command.
- Javax.security.auth.login.LoginException: **Checksum failed**
    - Occurs when the Kerberos ticket obtained by the client is out of date. Most frequently, during SSO testing, when a client cached a Kerberos ticket for the first SSO login attempt and an attribute for the SSO user was then changed.
    - To resolve this, log out on the client PC and then log back in; this immediately flushes the cache of Kerberos tickets and requires the cache to obtain a new ticket when trying to access the SmartTAP server.

- Org.ietf.jgss.GSSException is thrown when authenticating with Kerberos server. **Defective token detected (Mechanism level: GSSHeader did not find the right tag)**
  - Indicates that the client machine did not send the correct authentication token to SmartTAP. The most likely cause is that the client machine did not send *any* token at all.
  - Observed with a non-domain client machine accessing SmartTAP from a Firefox browser, with trusted site configured.

A.9.3 Troubleshooting with More Detailed SmartTAP Application Server Logging

If more detailed logging is required to troubleshoot these issues within the Application Server, configure the following loggers. Consult with AudioCodes technical support before making any changes to the SmartTAP logging.

The loggers can be configured through the SmartTAP Application Server Web interface - browse to http://localhost:9990. Note that this requires running the *add_user.bat* script to configure a user for accessing the Admin Console, or it can be configured in the *smarttap.xml* configuration file - which requires a restart of the Application Server service.

```
com.audiocodes.auth   --> TRACE
com.audiocodes.ngp.web.security   --> TRACE
com.audiocodes.ngp.web.system     --> DEBUG
org.apache.catalina.authenticator --> TRACE
```

A.10 Resetting the Configuration for Firefox Browser

In certain situations, it may be necessary to reset the configuration for the Firefox browser in order to use SSO with SmartTAP. To do this, see the Mozilla guide at https://support.mozilla.org/en-US/kb/reset-preferences-fix-problems.

Note that this wipes out all saved settings for the browser such as bookmarks, history, tabs, passwords, cookies, etc. https://support.mozilla.org/en-US/kb/reset-preferences-fix-problems

The following sections summarize the guide.

A.10.1 Refresh Firefox

This section instructs you how to refresh Firefox.

➢ **To refresh Firefox:**

1. Click the menu button ☰, click help ? and select **Troubleshooting Information**; the **Troubleshooting Information** tab opens.
2. Click the **Refresh Firefox** button in the uppermost right corner of the **Troubleshooting Information** tab.
3. When prompted to confirm, click the **Refresh Firefox** button again; Firefox closes to refresh itself. When finished, a window is displayed listing your imported information. Click **Finish**; Firefox reopens.
4. If previously set, the 'Trusted URIs' configuration will be lost. Follow the steps in the Firefox Browser configuration to assign the SmartTAP server as a trusted server.
5. Attempt SSO again; if SSO still doesn't work, delete Firefox preference files as shown in the next section.

A.10.2 Delete Firefox Preference Files

This section instructs you how to delete Firefox preference files.

➢ **To delete Firefox preference files:**

1. Click the menu button, click help and select **Troubleshooting Information**; the **Troubleshooting Information** tab opens.
2. Under the Application Basics section, click **Show Folder**; a window opens displaying your profile files.
3. Click the menu button and then click **Exit**.
4. Locate and delete the file *prefs.js* (or rename it, for example, to *prefs.jsOLD*, to keep the old file as a backup. If you find more than one, a *prefs.js.moztmp* file or a *user.js* file, delete (or rename) these as well.
5. Close the profile folder and open Firefox.
6. If previously set, the 'Trusted URIs' configuration will be lost. Follow the steps in the Firefox Browser configuration to assign the SmartTAP server as a trusted server.
7. Attempt SSO again; if SSO still does not work, uninstall and reinstall Firefox as shown in the next section.

A.10.3 Uninstall & Reinstall Firefox

This section describes how to uninstall and reinstall Firefox.

➢ **To uninstall and reinstall Firefox:**

1. Uninstall Firefox through the **Windows Control Panel**.
2. Make sure all Firefox data stored in the following locations is removed:
   - C:\Users\<user>\AppData\Local\Mozilla\
   - C:\Users\<user>\AppData\Roaming\Mozilla\
3. [Optional] Reboot the machine.
4. Reinstall the latest version of Firefox. It may be a good idea to download the latest version from Mozilla again, to be safe.
5. After the installation, follow the steps in the Firefox Browser configuration to assign the SmartTAP server as a trusted server.
6. Attempt SSO again.

This page is intentionally left blank.

B SmartTAP Lync Toolbar

The SmartTAP Lync Toolbar functions in conjunction with the Lync Conversation Window Extension (CWE) which allows the user to have access to in-call features like 'Save on Demand', 'Call Tagging', etc., without needing to open a browser window to access the SmartTAP GUI separately.

The toolbar is by default not enabled and must be installed / configured by AudioCodes, a certified AudioCodes Partner or by your local experienced IT.

To learn more about Microsoft Lync CWE, refer to:

http://msdn.microsoft.com/en-us/library/office/jj933101(v=office.15).aspx

B.1 Toolbar Features

- Single Sign-On
- Save on Demand, Record on Demand or Full Time Recording
- Pause / Resume Recording
- Call Tagging

See more information in this document to understand how to use the features above with the CWE window.

Figure B-1: SmartTAP: Save On Demand (SOD)

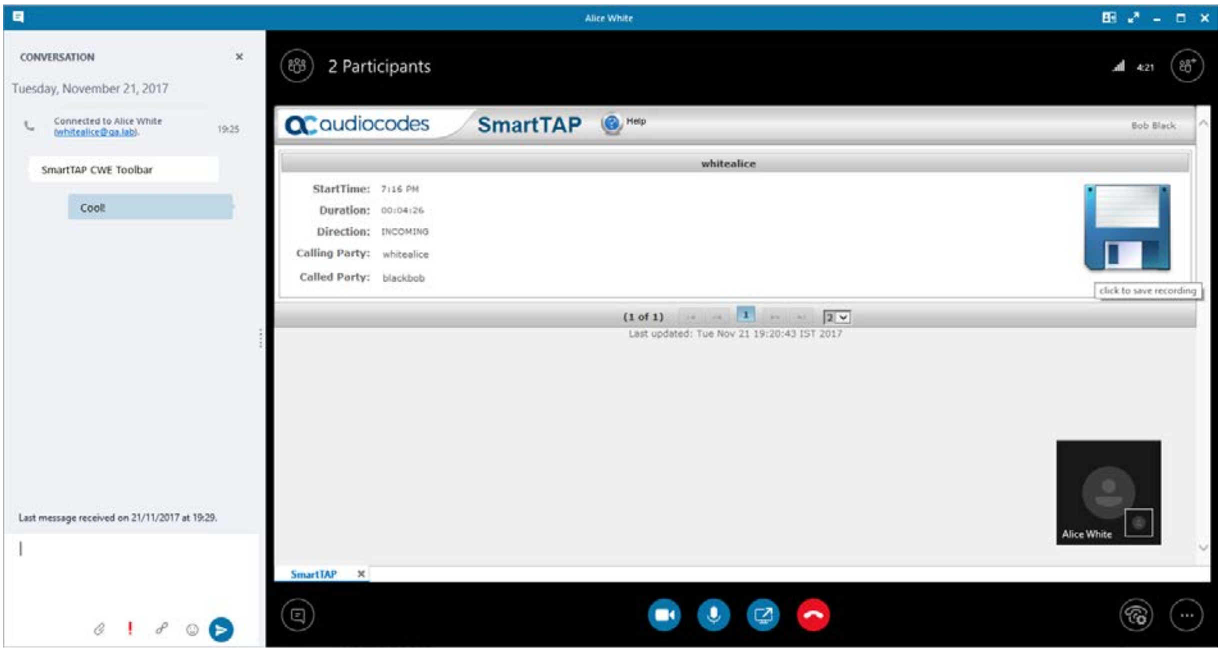


Figure B-2: Record on Demand (ROD)

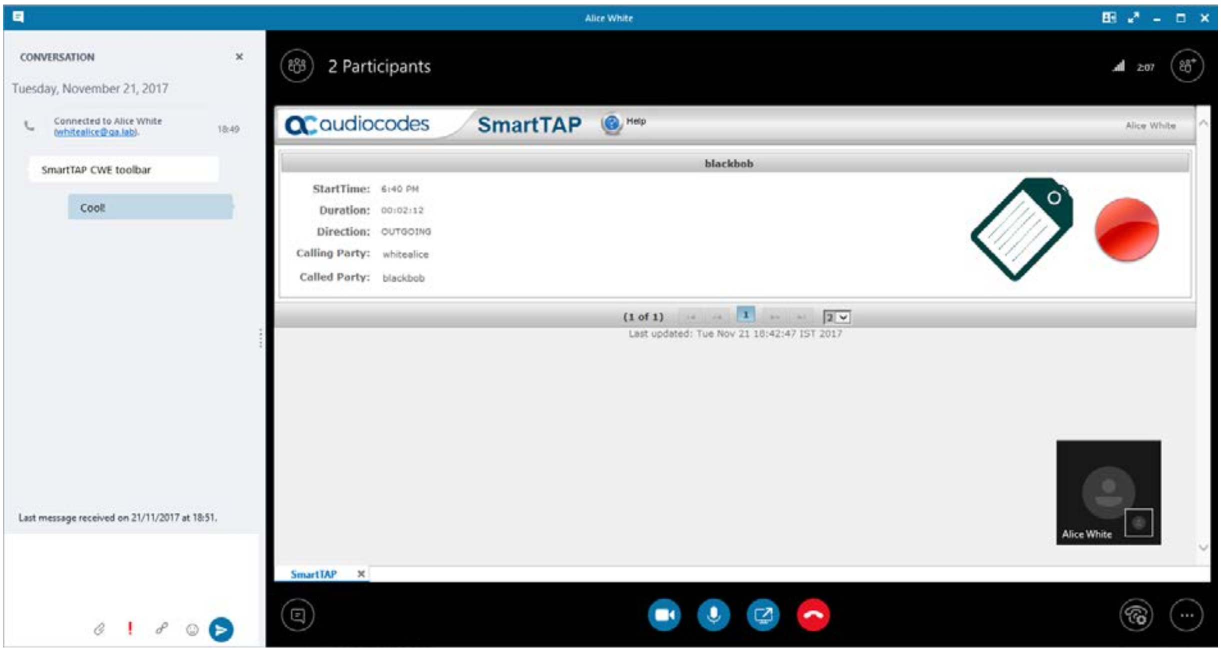
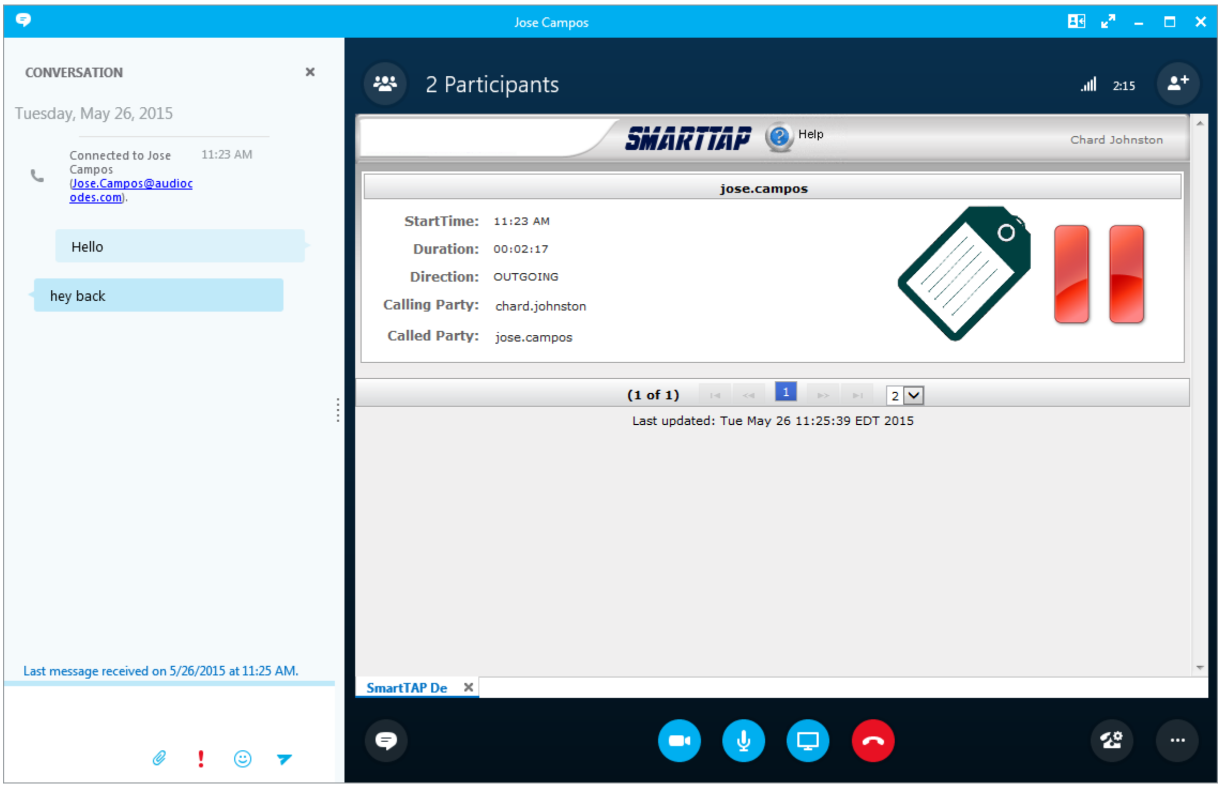


Figure B-3: SmartTAP Lync CWE Toolbar (Pause / Resume)



This page is intentionally left blank.

C Media Exporter

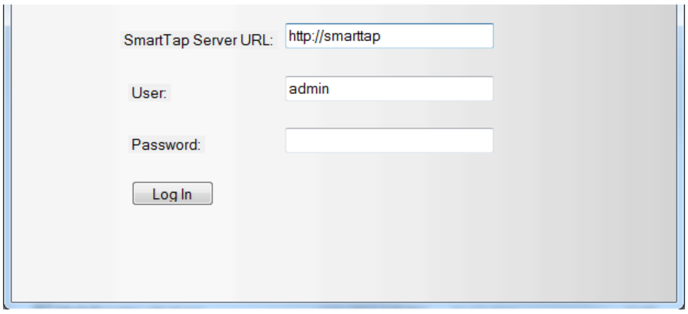
Media Exporter is a separate desktop application useful for compliance officers or for those who need to download bulk calls from SmartTAP for a specific user or for all users within a date/time range.

The search parameters are similar to the SmartTAP UI. Administrators must enter their credentials to access the application. Security credentials assigned by SmartTAP determine which users will be visible and whose associated calls will be available for downloading.

> **Note:**. Currently both audio and video call types can be exported together. The video component of video calls is not exported in the current version. Alternatively, only the audio of video calls is exported in this version.

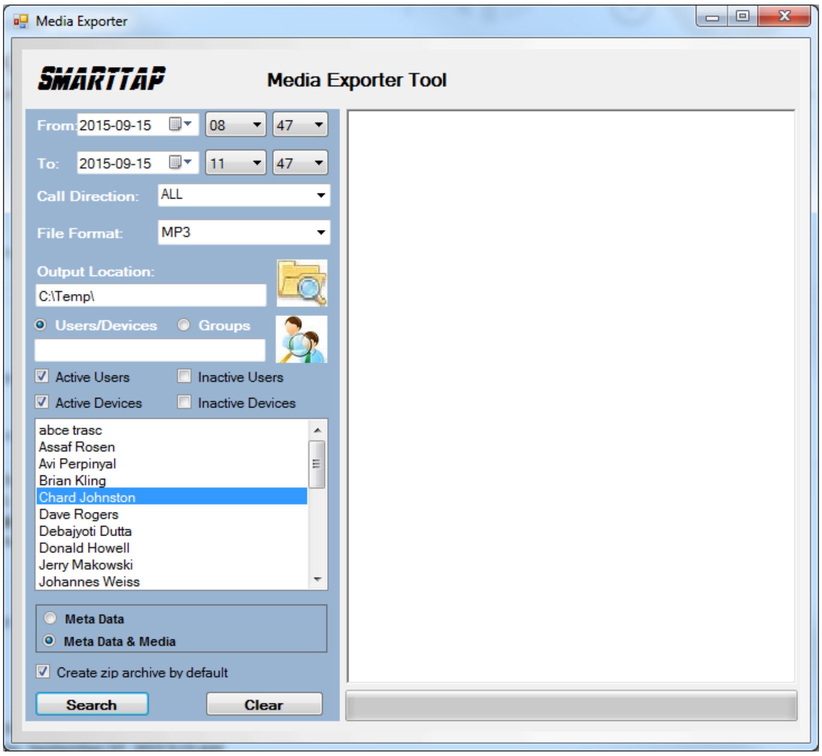
1. Run the **MediaExporter.exe** tool from your Windows PC.
2. Enter the access details and credentials:
   - SmartTAP URL to be used to access the SmartTAP UI
   - Enter the username (same as that used to access the SmartTAP UI)
   - Enter the password

Figure C-1: Credentials



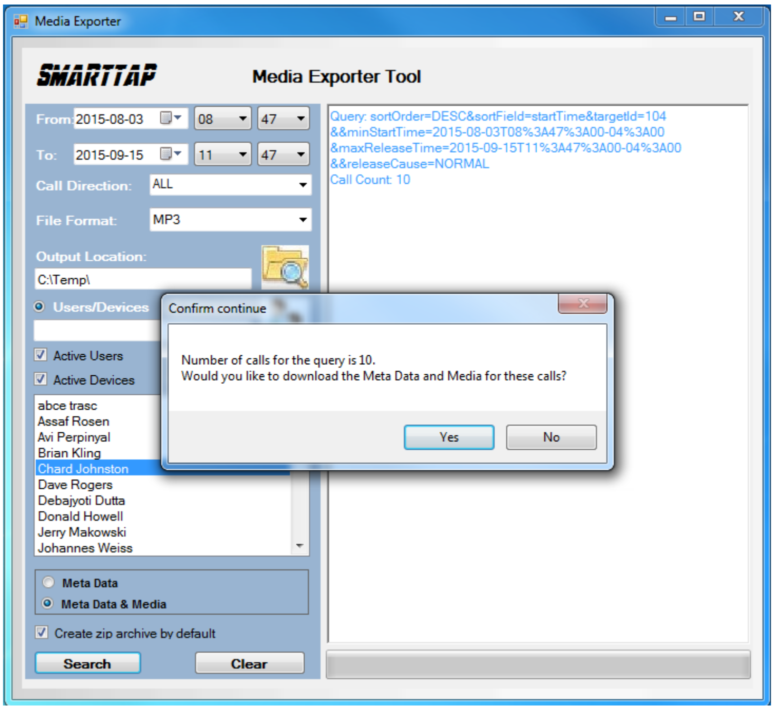
3. Enter the Search Criteria.

Figure C-2: Enter the Search Criteria



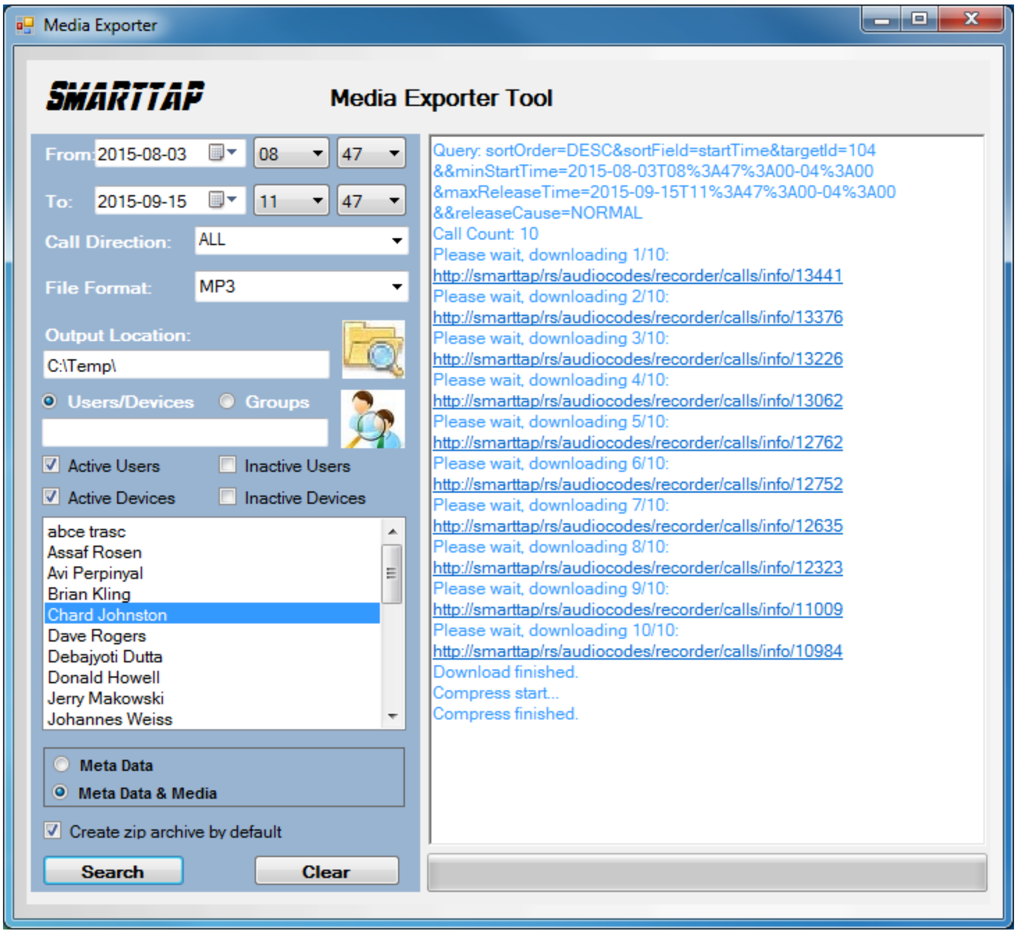
- The following search criteria definitions are the same as those of the SmartTAP UI:
  - File Format (MP3, WAV) Either format can be played using standard Media Player
  - Output location: Where do you want the zip file and contents to be saved?
  - Meta Data or Meta Data & Media: Download only the Call Records or the Call Records and the Audio Files
  - Create zip archive by default: The Meta Data and audio files will be zipped for convenient storage and distribution.

Figure C-3: Search Results



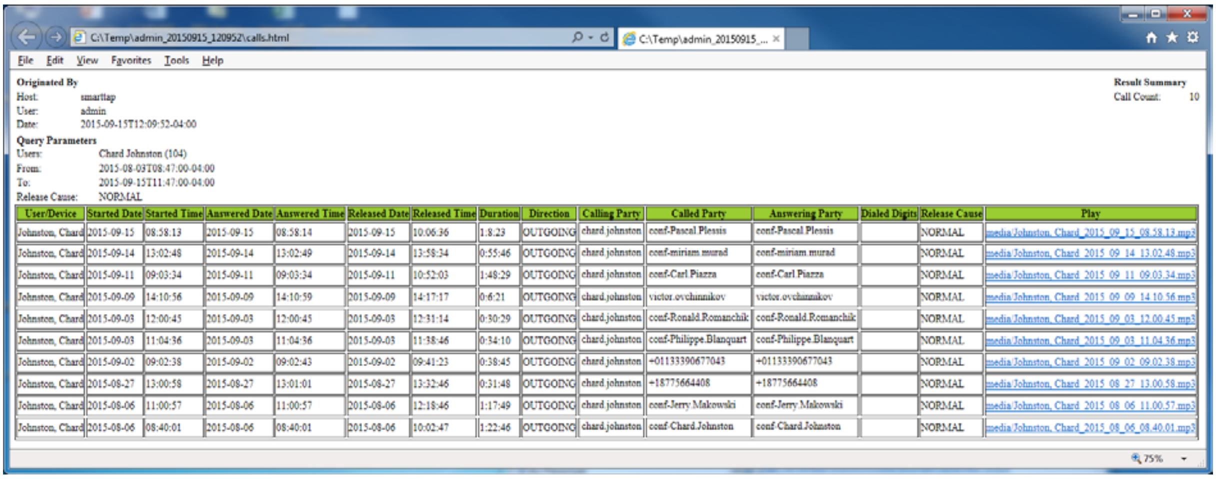
4. Select **Yes** to start downloading the calls.

Figure C-4: Downloading



After the download completes, the default browser automatically opens presenting the Call Manifest for the calls from the search results.

Figure C-5: Call Manifest



C:\Temp\admin_20150915_120952\calls.html

Originated By
Host: smarttap
User: admin
Date: 2015-09-15T12:09:52-04:00

Query Parameters
Users: Chard Johnston (104)
From: 2015-08-03T08:47:00-04:00
To: 2015-09-15T11:47:00-04:00
Release Cause: NORMAL

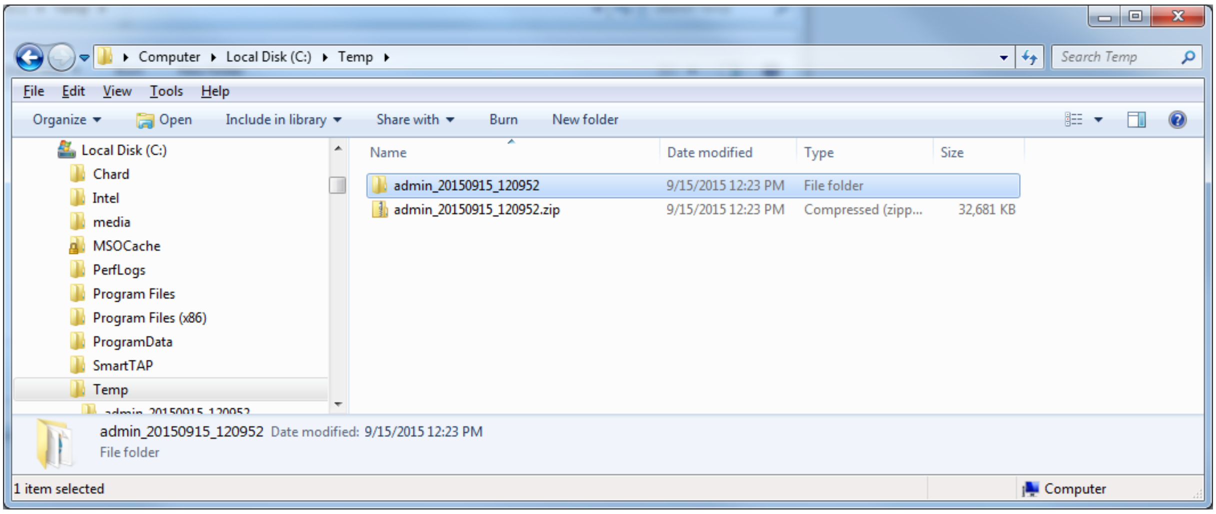
Result Summary
Call Count: 10

User/Device	Started Date	Started Time	Answered Date	Answered Time	Released Date	Released Time	Duration	Direction	Calling Party	Called Party	Answering Party	Dialed Digits	Release Cause	Play
Johnston, Chard	2015-09-15	08:58:13	2015-09-15	08:58:14	2015-09-15	10:06:36	1:8:23	OUTGOING	chard.johnston	conf-Pascal.Plessis	conf-Pascal.Plessis		NORMAL	media/Johnston, Chard_2015_09_15_08.58.13.mp3
Johnston, Chard	2015-09-14	13:02:48	2015-09-14	13:02:49	2015-09-14	13:58:34	0:55:46	OUTGOING	chard.johnston	conf-miriam.murad	conf-miriam.murad		NORMAL	media/Johnston, Chard_2015_09_14_13.02.48.mp3
Johnston, Chard	2015-09-11	09:03:34	2015-09-11	09:03:34	2015-09-11	10:52:03	1:48:29	OUTGOING	chard.johnston	conf-Carl.Piazza	conf-Carl.Piazza		NORMAL	media/Johnston, Chard_2015_09_11_09.03.34.mp3
Johnston, Chard	2015-09-09	14:10:56	2015-09-09	14:10:59	2015-09-09	14:17:17	0:6:21	OUTGOING	chard.johnston	victor.ovchinnikov	victor.ovchinnikov		NORMAL	media/Johnston, Chard_2015_09_09_14.10.56.mp3
Johnston, Chard	2015-09-03	12:00:45	2015-09-03	12:00:45	2015-09-03	12:31:14	0:30:29	OUTGOING	chard.johnston	conf-Ronald.Romanchik	conf-Ronald.Romanchik		NORMAL	media/Johnston, Chard_2015_09_03_12.00.45.mp3
Johnston, Chard	2015-09-03	11:04:36	2015-09-03	11:04:36	2015-09-03	11:38:46	0:34:10	OUTGOING	chard.johnston	conf-Philippe.Blanquart	conf-Philippe.Blanquart		NORMAL	media/Johnston, Chard_2015_09_03_11.04.36.mp3
Johnston, Chard	2015-09-02	09:02:38	2015-09-02	09:02:43	2015-09-02	09:41:23	0:38:45	OUTGOING	chard.johnston	+01133390677043	+01133390677043		NORMAL	media/Johnston, Chard_2015_09_02_09.02.38.mp3
Johnston, Chard	2015-08-27	13:00:58	2015-08-27	13:01:01	2015-08-27	13:32:46	0:31:48	OUTGOING	chard.johnston	+18775664408	+18775664408		NORMAL	media/Johnston, Chard_2015_08_27_13.00.58.mp3
Johnston, Chard	2015-08-06	11:00:57	2015-08-06	11:00:57	2015-08-06	12:18:46	1:17:49	OUTGOING	chard.johnston	conf-Jerry.Makowski	conf-Jerry.Makowski		NORMAL	media/Johnston, Chard_2015_08_06_11.00.57.mp3
Johnston, Chard	2015-08-06	08:40:01	2015-08-06	08:40:01	2015-08-06	10:02:47	1:22:46	OUTGOING	chard.johnston	conf-Chard.Johnston	conf-Chard.Johnston		NORMAL	media/Johnston, Chard_2015_08_06_08.40.01.mp3

Output Location:

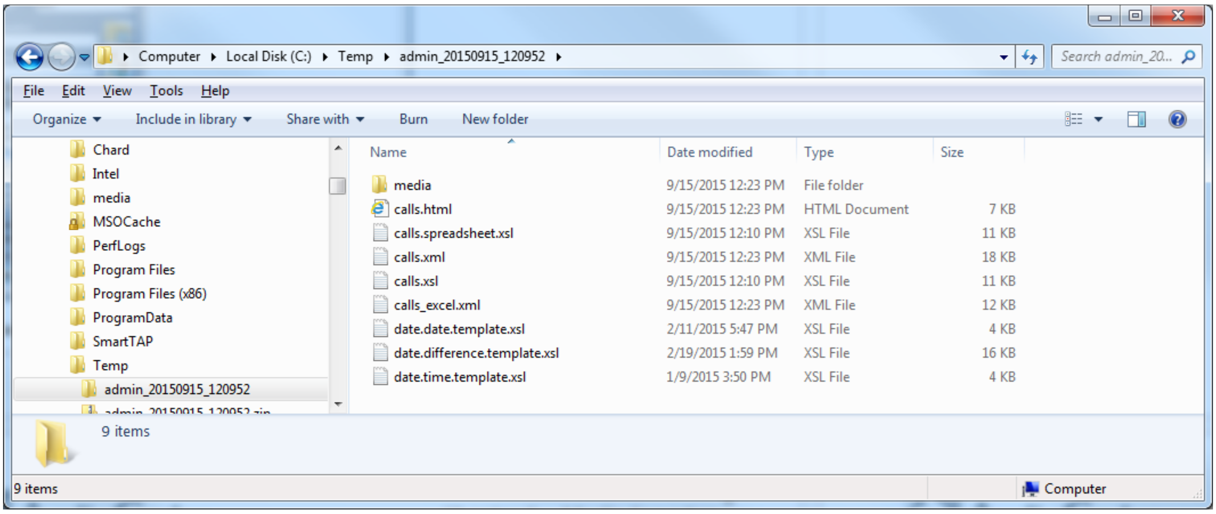
In the output location, you'll find the unzipped data and a zip file which contains the Call Manifest and all the associated audio files.

Figure C-6: Output Location



Folder Name: User Name of User that downloaded calls + Date + Time.

Figure C-7: Contents of Folder



Calls.html: Call Manifest

Calls.xml: Call Meta Data exported from SmartTAP loaded with Calls.html

Calls_excel.xml: Open file in Excel. Once in, Excel can be used to generate statistics and reports.

This page is intentionally left blank.

D API Integration

The SmartTAP API is a RESTful Web Services API that provides complete access to and control over the SmartTAP platform. The API provides:

- All administrative functions, including adding users and creating profiles
- Advanced call recording and search capabilities
- Retrieval of recordings & associated Meta Data
- Real-time call monitoring
- Others

Try the following example from your browser. Enter in the address bar:
http://url/rs/audiocodes/recorder/calls/info

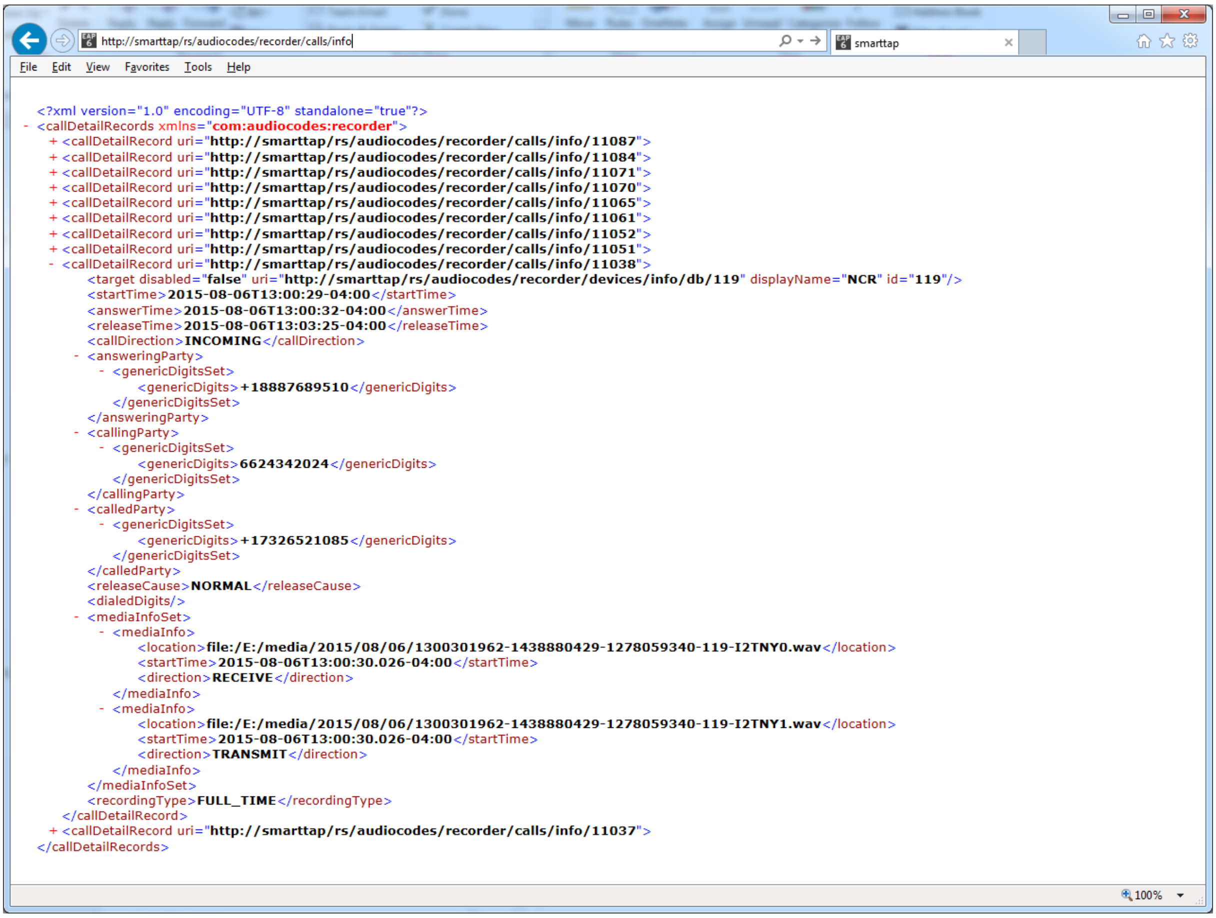
Note: Change 'URL' to the IP address or the name of your SmartTAP product.

http://smarttap/rs/audiocodes/recorder - path to SmartTAP

/calls - SmartTAP Rest API resource

/info – Returns a collection of call detail records based on search criteria parameters

Figure D-1: API Integration



To learn more about the SmartTAP REST API see the *HTML documentation* included with the SmartTAP software distribution.

This page is intentionally left blank.

E Recording Health Monitor

The Recording Health Monitor (HM) service is used to monitor the health of the system by automatically monitoring users records and their associated media. It identifies and reports the following behavior:

- Number of recorded calls per enabled for recording user
- Silent or no media in answered call recordings
- Accessibility to associated media files in answered call recordings

The service utilizes the REST API to retrieve the data from an Application Service and to generate daily reports. The following daily report of calls for targeted, recording enabled, users are generated:

1. recording_report_YEAR-Month-Day.txt – general report of all targeted users and calls in text format.
2. recording_summary_report_YEAR-Month-Day.csv - general report of all targeted users and calls in CSV format (Excel).
3. recording_err_warn_report _YEAR-Month-Day.csv – warnings report in CSV format (Excel) that includes a list of possible recording issues such as no recordings for a targeted user, silent or zero media in answered call recordings, in CSV format (Excel).

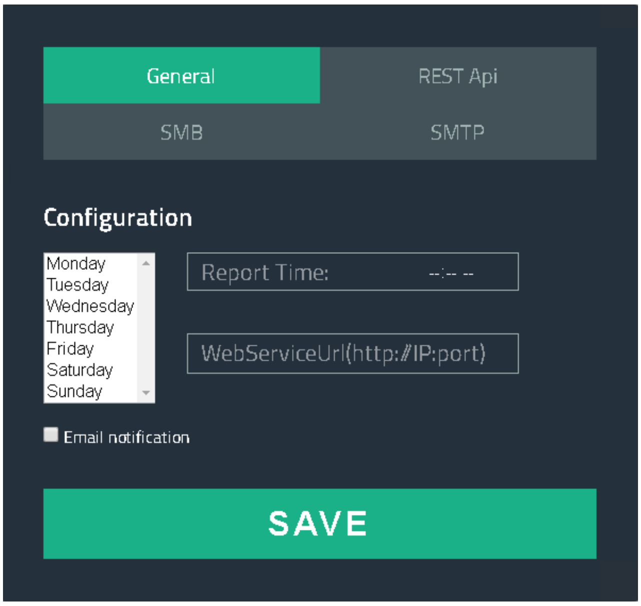
See example reports below in Section E.1.

The reports generation schedule (default 11:00 pm) can be configured using HP configuration file, located in AudioCodes tools folder in Program Files under Config (ex. C:\Program Files\AUDIOCODES\Tools\HealthMonitor\Config). Email notification with generated reports can be sent via email (requires HealthMonitor SMTP configuration).

The Health Monitor is installed automatically on SmartTAP server as a part of the SmartTAP installation, under the AudioCodes tools folder in Program Files (ex. C:\Program Files\AUDIOCODES\Tools\HealthMonitor). The Health Monitor is installed as a Windows Service under the name “AudioCodes HM”.

- **General configuration:**

Figure E-1: General Configuration



- Scheduled report monitoring days: HM monitors call activity for the selected days. If no days are selected, HM monitors all days. Default: All days.
- Report Time – Health Monitor start time. Monitoring will start on scheduled time. Default: 11:00 pm.

- Report Retention Days – Sets the number of days to store reports. Old reports are purged from the database accordingly. By default, this parameter is configured to 0. This default can be changed in the configuration file as follows:

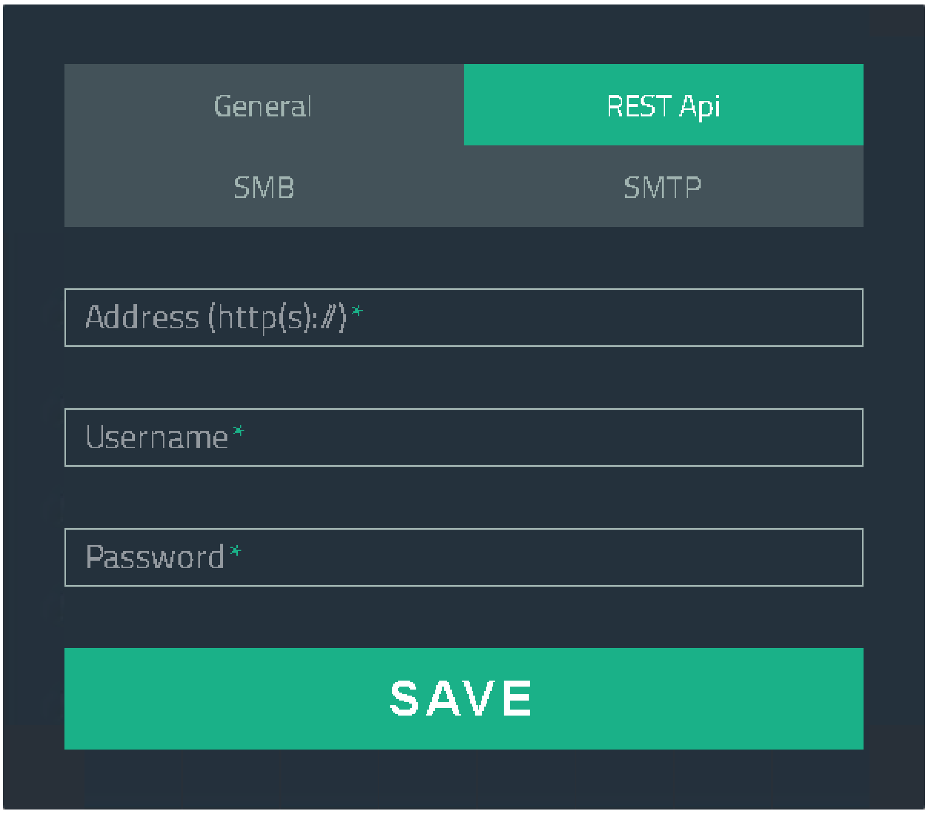
```
AudioCodes\Tools\HealthMonitor\Config
<ReportRetentionDays>10</ReportRetentionDays>
```

- WebServiceUrl – Health Monitor Web Service configuration page. Default: http://localhost:10101.

4. Email notification – enables email notification option. HM sends an email with attached daily reports on a scheduled time. SMTP configuration is required if this option is enabled. For more details see Section 6.10.2. Default: Disabled.

- REST API configuration:

Figure E-2: REST API Configuration

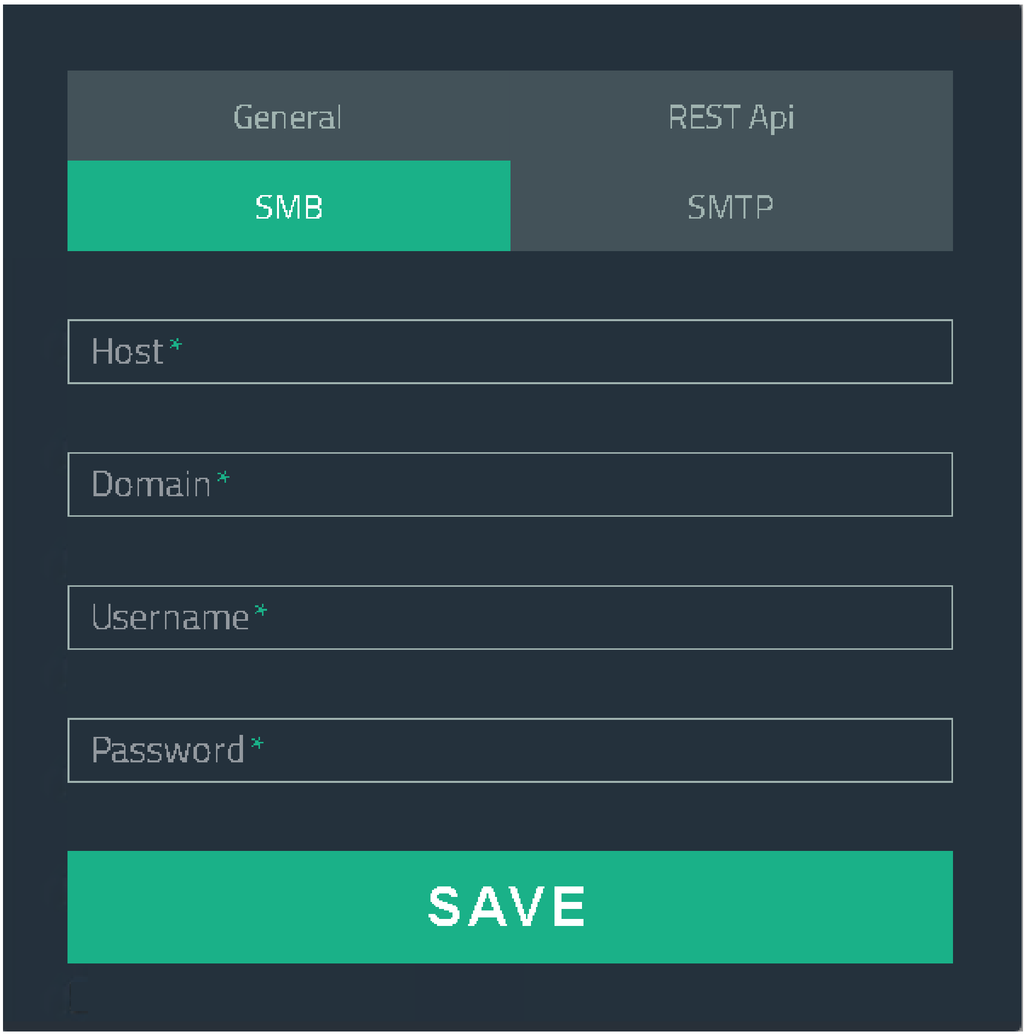


The Health Monitor uses a dedicated user for REST communication with Application Server. It is not necessary to modify this configuration (with the exception of the note below).

> **Note:** In case the Application server is configured for HTTPS only, the Address field should be changed to https://FQDN of Application Server, where FQDN should be the same as in the certificate that was issued for the Application Server. This is necessary for authentication purposes.

- SMB – network media files location:

Figure E-3: SMB Configuration

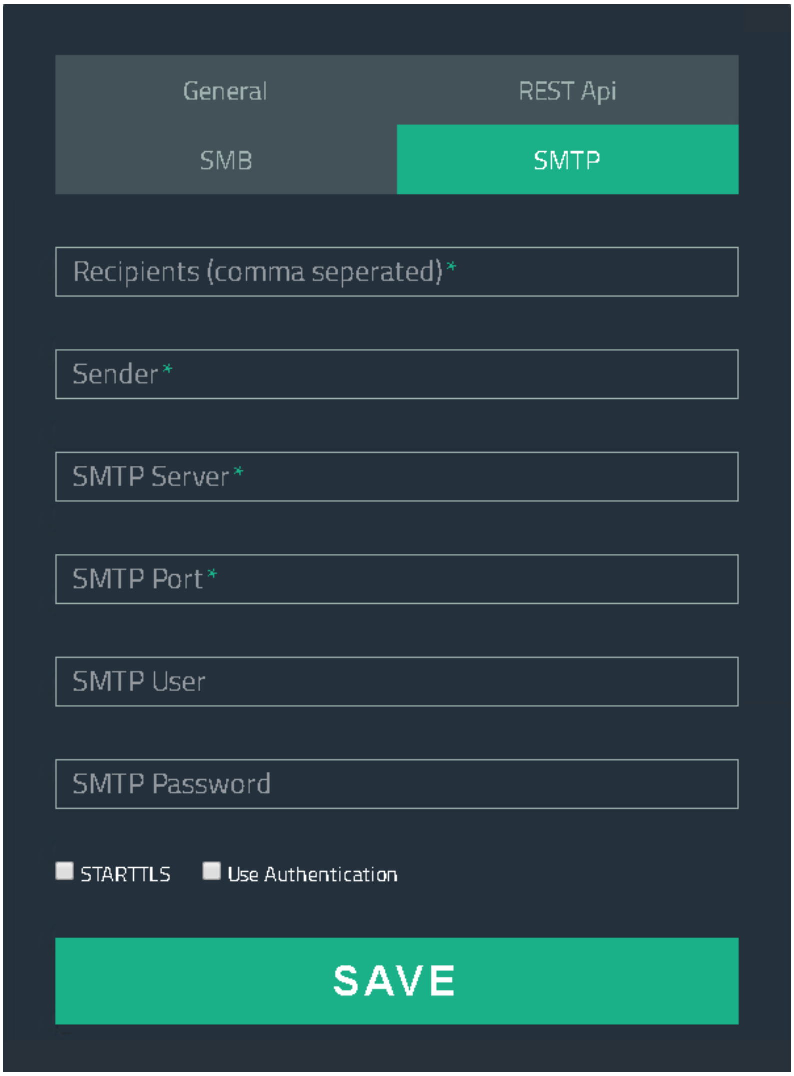


In case SmartTAP uses a network location for media storage, this configuration must be updated with the following parameters:

- Host – hostname of network media server
- Domain – domain name of the remote network storage
- Username/password – remote network media storage credentials

- SMTP – mail notification:

Figure E-4: SMTP Configuration



The following parameters can be configured in this screen:

- Recipients – mail notification recipient list. Comma separated format for multiple recipients.
- Sender – mail notification initiator address. All reports will be sent from this mail address.
- SMTP Server – mail server address (IP, FQDN).
- SMTP Port – mail server port.
- SMTP User – mail server user.
- SMTP Password – mail server password.
- STARTTLS - secure connection using SSL/TLS.
- Use Authentication – use authentication to connect to mail server.

E.1 Reports Format

The Health Monitoring utility generates a report including the following fields:

- Display name – display name of targeted user
- Recording profile – assigned call recording type
- Number of answered calls – total number of answered calls
- Warnings – number of warnings
- Errors – number of errors

Figure E-5: Example 1: recording_report_YEAR-Month-Day.txt

```
******************************************************************************
Display Name=qaTuser12; Recording profile=FULL_TIME; Number of answered calls=2; Warnings=0; Errors=2
|
|_Call details 1:
        Called party - qatuser11
        Calling party - qatuser12
        Answering party - 7010
        Call answer time - 11/6/2017 2:17:44 PM
        Integration call-id - 7e026b38ae624edd8e1f952075eda17a
        SmartTAP call-id - 81
        Message - ERROR [NO_MEDIA]
                file:/E:/media/2017/11/06/1417445-1509970655-1275549367-103-ICyc11.wav missing or not accessible
                file:/E:/media/2017/11/06/1417445-1509970655-1275549367-103-ICyc10.wav missing or not accessible
|
|_Call details 2:
        Called party - qatuser11
        Calling party - qatuser12
        Answering party - 7010
        Call answer time - 11/6/2017 3:57:32 PM
        Integration call-id - 20b38ef59d314e13b377f1e09c2afa7c
        SmartTAP call-id - 90
        Message - ERROR [NO_MEDIA]
                file:/E:/media/2017/11/06/15573214-1509976648-1275549367-103-W9Wjp0.wav missing or not accessible
                file:/E:/media/2017/11/06/15573214-1509976648-1275549367-103-W9Wjp1.wav missing or not accessible

******************************************************************************
Display Name=qaTuser15; Recording profile=FULL_TIME; Number of answered calls=0; Warnings=0; Errors=0
```

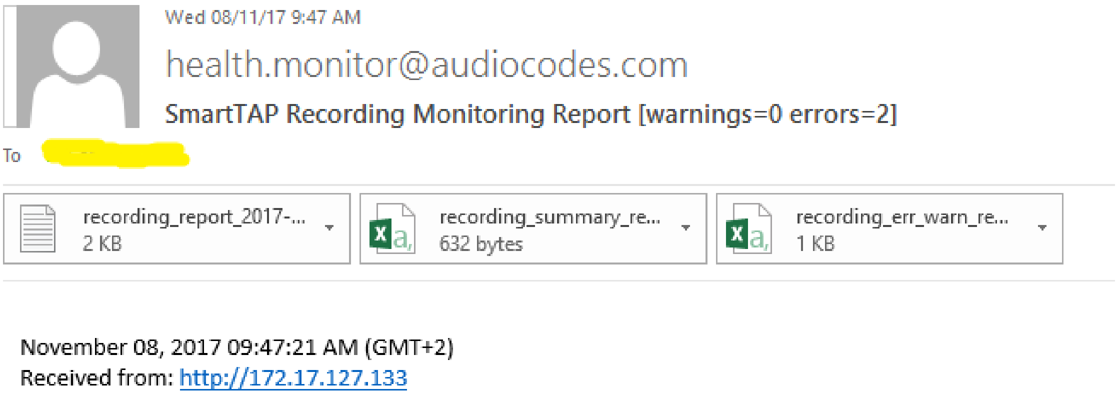
Figure E-6: Example 2: recording_summary_report_YEAR-Month-Day.csv:

Display name	Recording profile	Number of answered calls	Warnings	Errors
qaTuser12	FULL_TIME	2	0	2
qaTuser15	FULL_TIME	0	0	0
qaTuser14	FULL_TIME	0	0	0
qaTuser11	FULL_TIME	0	0	0
qaTuser10	FULL_TIME	0	0	0

Figure E-7: recording_err_warn_report _YEAR-Month-Day.csv

Display name	Called party	Calling party	Answering party	Call answer time	Integration call-id	SmartTAP call-id	Status	Status reason	Details
qaTuser12	qatuser11	qatuser12	7010	11/06/17 14:17	7e026b38ae624edd8e1f952075eda17a	81	ERROR	NO_MEDIA	file:/E:/
qaTuser12	qatuser11	qatuser12	7010	11/06/17 15:57	20b38ef59d314e13b377f1e09c2afa7c	90	ERROR	NO_MEDIA	file:/E:/

Figure E-8: Email Format:


Wed 08/11/17 9:47 AM

health.monitor@audiocodes.com

SmartTAP Recording Monitoring Report [warnings=0 errors=2]

To

recording_report_2017-... 2 KB

recording_summary_re... 632 bytes

recording_err_warn_re... 1 KB

November 08, 2017 09:47:21 AM (GMT+2)

Received from: http://172.17.127.133

F Announcement Server (Skype for Business)

SmartTAP offers Announcement Server (AN) in the Microsoft Skype for Business environment to inform the call parties that their call will be recorded. When the Announcement Server (AN) is deployed, SmartTAP Skype for Business plugin on the FE servers redirects inbound, outbound, and internal calls with enabled for recording users (targeted users) to the Announcement Server. The Announcement Server plays the announcement according to the configuration and redirects the call to the original destination.

The Announcement Server can be configured to play announcements to parties on the calls, to play Music-on-Hold to the calling party while the announcement is played to the answered party, and play announcements according to an IVR script to one or both call parties. The announcements and IVR menus are configurable as well.

F.1 Enabling Routing Calls to the Announcement Server in Skype For Business Plugin

Skype for Business plugin components have to be configured to route the calls to the AN. The procedure below should be applied to each Skype for Business plugin component.

> **Note:** Announcement-related configuration is global for all targeted users when this document was published.

F.1.1 Configuration

This section describes how to add configuration support for plugins.

➢ **To add support for plugins:**

1. Edit the file “LyncPlugIn.exe.config”.
2. Change <add key="EnableAnnouncements" value="false"></add> to “true”.
3. If you would like to record the incoming Announcement leg of the call, enable the following:
```
<add key="RecordAnnouncements" value="false"></add> change to
“true”
```
4. If you like to record the outgoing Announcement leg (AN is configured to play announcements to both parties of the calls), enable the following:
```
<add key="RecordAnnouncementOutCall" value="false"></add>
change to “true”
```
5. If you like to set the call type on which the announcements should be played to other then InboundExternal, change the following element value to one of the following options:
   - InboundExternal – announcement will be played on inbound calls between an external party and a targeted user only
   - OutboundExternal - announcement will be played on outbound calls between an external party and a targeted user only
   - AllExternal - announcement will be played on inbound and outbound calls between an external party and a targeted user only
   - All - announcement will be played on all types of the calls, external and internal
```
<add key="AnnouncementCallType" value="InboundExternal"></add>
```

6. Save and close the configuration file.
7. Restart the plugin service.

Note: SmartTAP requires two concurrent audio recording licenses to record both legs of the announcement part of the call. Make sure that the number of the system's concurrent recording licenses is equal to or higher than the number of concurrent announcements multiplied by 2.

F.2 Simple Announcement

SmartTAP can be configured to play announcements to the calling party and if required called parties on a call with a targeted user.

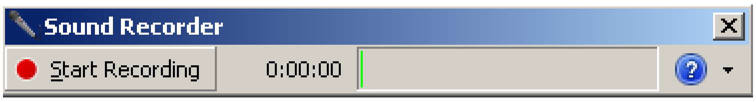
F.2.1 Configuration

The configuration enables setting of announcements to the calling party and if required called parties on a call with a targeted user.

➢ **To configure a simple announcement:**

1. Create a WMA audio file. You can use the Windows Sound Recorder.

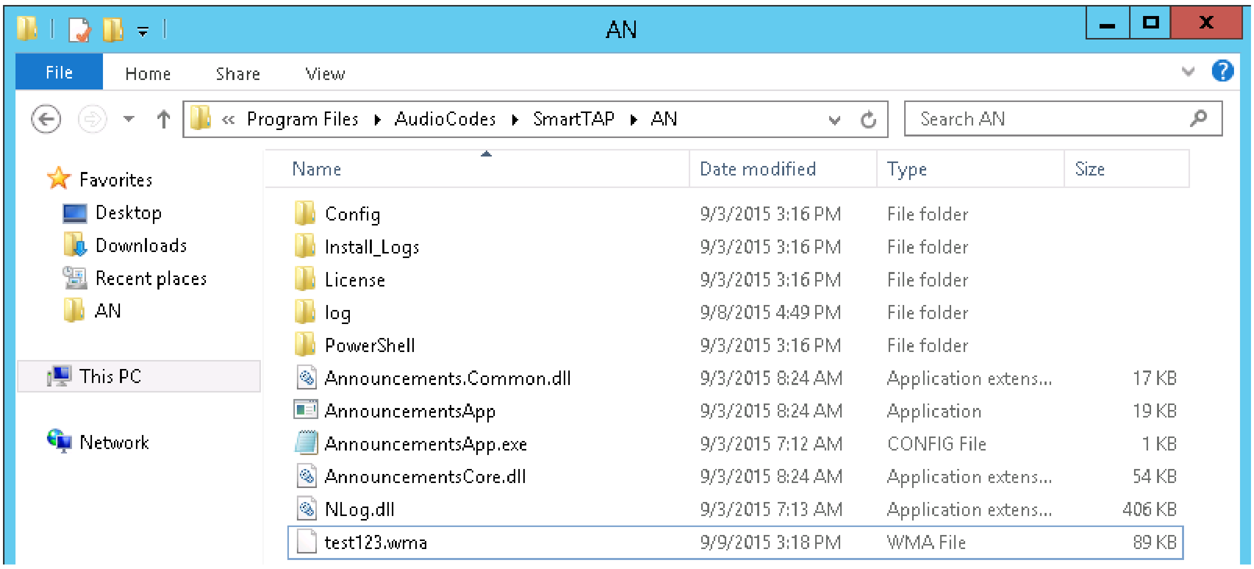
Figure F-1: Sound Recorder



Example: "Thank you for calling Company A, your call may be recorded for quality assurance".

2. When done, click **Stop Recording** and it will prompt for the new file destination.
3. Save it and copy this file to the AN server. Location: Program Files\AudioCodes\SmartTAP\AN\.

Figure F-2: AN Server



4. Edit the System.config file at Program Files\AudioCodes\SmartTAP\AN\Config\ as described below:
    - To play an announcement to the calling external party in the inbound calls add the options inCallPlayPrompt=”true” and inCallPlayPromptFilePath=”filename.wma” as below:
      ```
      <System
         InCallPlayPrompt=”true”
         inCallPlayPromptFilePath=”filename.wma”
      />
      ```
    - To play an announcement to the called external party in the outbound calls, add the following options:
      ```
      <System
         OutCallPlayPrompt=”true”
         OutCallPlayPromptFilePath=”filename.wma”
      AnnouncementRecipients=”BothParties”
      />
      ```
5. Edit the file “LyncPlugIn.exe.config”:
    a. Change <add key="AnnouncementCallType" value="InboundExternal"></add> to “OutboundExternal”.
    b. Save and close the configuration file.
    c. Restart the plugin service.
6. To play an announcement to the calling and called external parties in inbound and outbound calls:
    a. Add the following options:
      ```
      <System
         InCallPlayPrompt=”true”
         inCallPlayPromptFilePath=”calling.wma”
         OutCallPlayPrompt=”true”
         OutCallPlayPromptFilePath=”called.wma”
      AnnouncementRecipients=”BothParties”
      />
      ```
    b. Edit the file “LyncPlugIn.exe.config”.
    c. Change <add key="AnnouncementCallType" value="InboundExternal"></add> to “AllExternal”.
    d. Save and close the configuration file.
    e. Restart the plugin service.

Note:

- When SmartTAP is configured to play an announcement to both inbound and outbound calls, the SFB plugin routes both inbound and outbound calls with a targeted user to the AN service. The AN service establishes a call to the original destination and plays the configured announcements to the parties when the call is answered and then reroutes the call to the original destination.
- The configured calling and called prompts are played to calling and called parties accordingly regardless of the call direction, inbound or outbound. To configure different prompts for inbound and outbound calls, enable the IVR and configure the IVR state machine according to requirements.

7.

8. To play an announcement to external calls and internal calls:

   a. Add the following options:

```
<System
   InCallPlayPrompt=”true”
   inCallPlayPromptFilePath=”calling.wma”
   OutCallPlayPrompt=”true”
   OutCallPlayPromptFilePath=”called.wma”
AnnouncementRecipients=”BothParties”
/>
```

   b. Edit the file “LyncPlugIn.exe.config”.

   c. Change <add key="AnnouncementCallType" value="InboundExternal"></add> to “All”.

   d. Save and close the configuration file.

   e. Restart the plugin service.

Note:

- Playing announcements on the calls between targeted users and Skype For Business Conference Server are not supported.
- In this configuration, the AN service establishes a call to the original destination and plays the configured announcements to the parties when the call is answered and then reroutes the call to the original destination.
- The configured calling and called prompts are played to calling and called parties accordingly regardless of the call direction. To configure different prompts for inbound and outbound calls, enable the IVR and configure the IVR state machine as required.

F.3 IVR

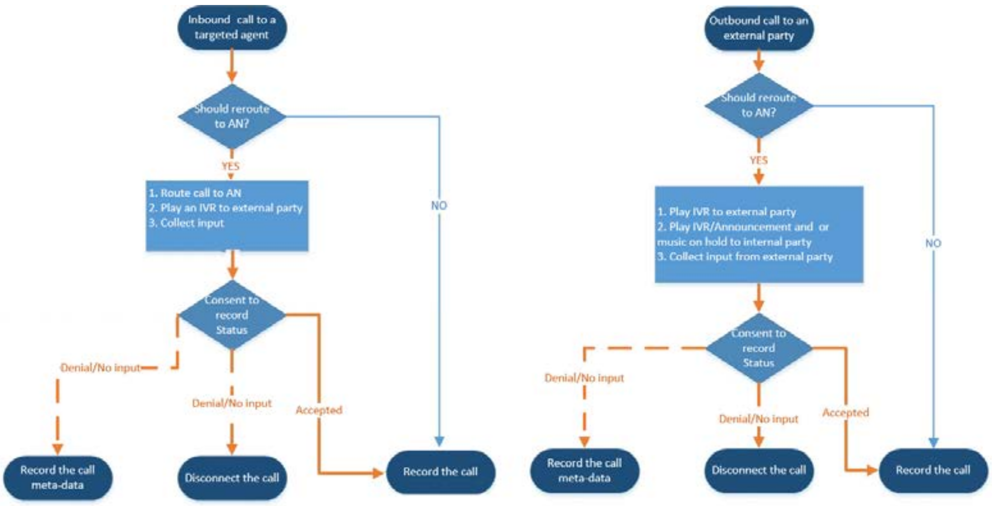
SmartTAP supports interactive voice response (IVR) announcements. The IVR menus are configured by default to request recording consent from a call party(s). These menus can be can be customized. Text-to-speech support is available in 26 languages.

Below is an example of a call consent prompt:

"This call may be recorded for quality assurance purposes. Press one to accept or press zero to continue without recording."

If the call party does not consent, the conversation is not recorded. The following illustrates the Inbound and outbound call decision process:

Figure F-3: IVR Announcements



Consent result and action are displayed as part of call record meta-data as shown below:

Figure F-4: Consent Accepted

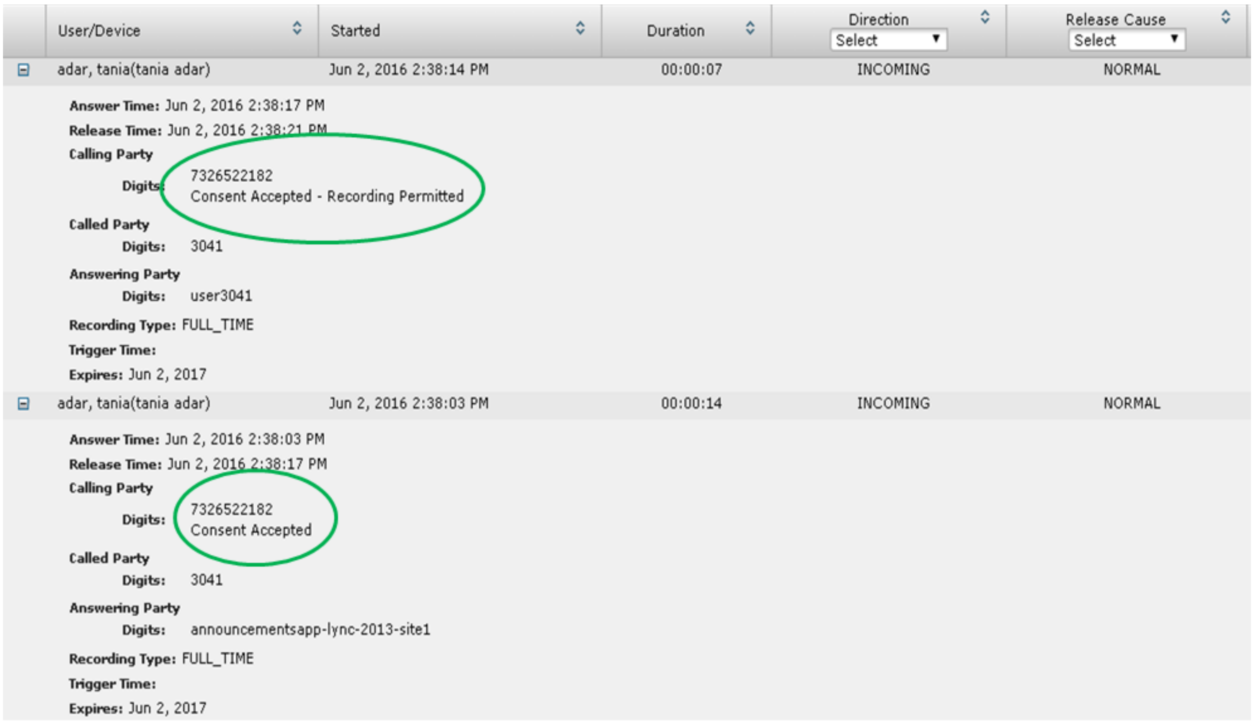
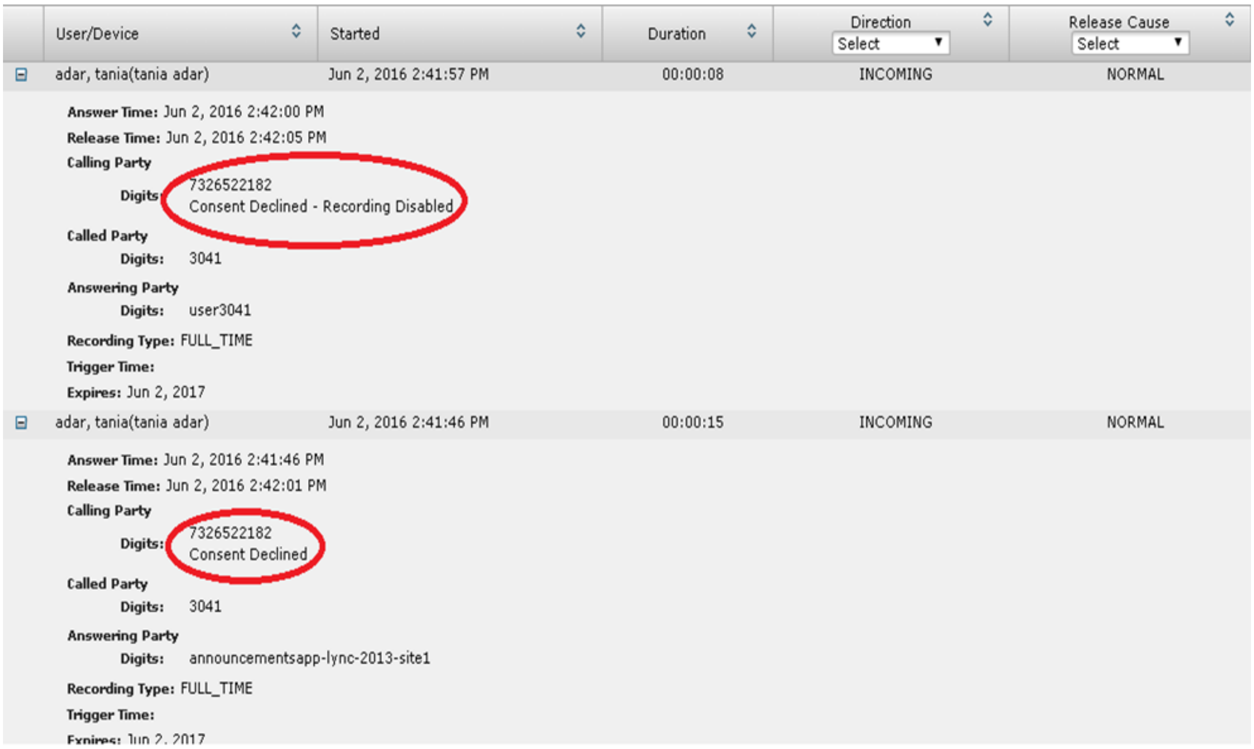
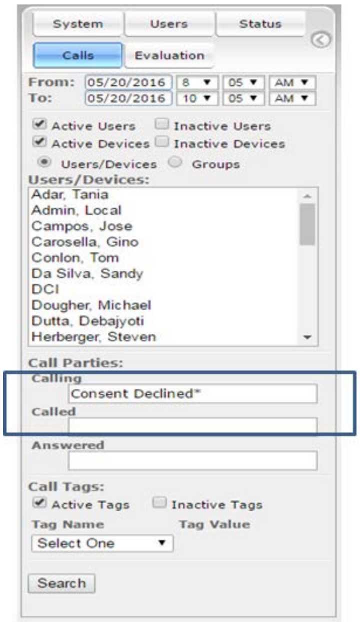


Figure F-5: Consent Declined



Search calls based on the consent as shown below:

Figure F-6: Call Parties



F.3.1 Configuration

By default, call consent is disabled.

F.3.1.1 Enabling IVR

1. Open the System.config file located under …\Program Files\AudioCodes\SmartTAP\AN\Config\.
2. Add option

```
enableIvr =”true” and playIVRToExternalCallingParty =”true”
<System   enableIvr="true"
playIVRToExternalCallingParty="true"
/>
```

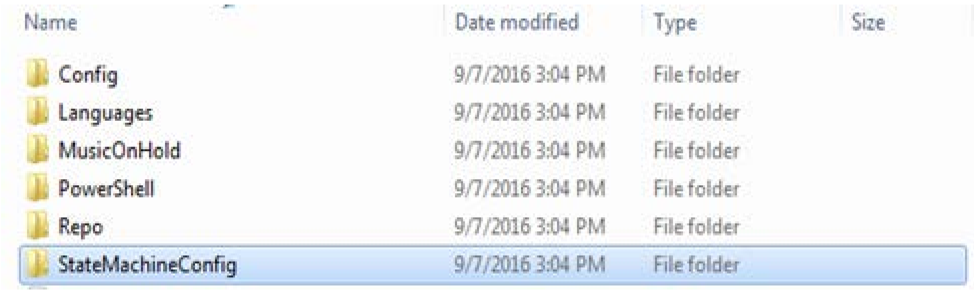
3. Restart the AN Service.

F.3.1.2 Files Location

The following describes the location for the program files:

- The prompt media files are located under …\Program Files\AudioCodes\SmartTAP\AN\Languages. USA English media files are under en-us folder.
- The IVR state machines are located under Program Files\AudioCodes\SmartTAP\AN\Config\StateMachineConfig
- The IVR sample state machines are located under Program Files\AudioCodes\SmartTAP\AN\Config\Repo

Figure F-7: File Location



Name	Date modified	Type	Size
Config	9/7/2016 3:04 PM	File folder	
Languages	9/7/2016 3:04 PM	File folder	
MusicOnHold	9/7/2016 3:04 PM	File folder	
PowerShell	9/7/2016 3:04 PM	File folder	
Repo	9/7/2016 3:04 PM	File folder	
StateMachineConfig	9/7/2016 3:04 PM	File folder	

The AN state machine can be fine-tuned according to requirements in the state machine file. File content sample:

Figure F-8: File Content Sample


```
{
  "$type": "AnnouncementsCore.AnnTree.AnnStateMachine, AnnouncementsCore",
  "DefaultLanguage": "en-us",
  "AnnNodes": [
    {
      "$type": "AnnouncementsCore.AnnTree.AnnLanguageNode, AnnouncementsCore",
      "PromptName": "chooseLanguage.wma",
      "Languages": [
        {
          "$type": "AnnouncementsCore.AnnTreeModel.LanguageDtmf, AnnouncementsCore",
          "Dtmf": "1",
          "Language": "en-us",
          "NextId": "2"
        },
        {
          "$type": "AnnouncementsCore.AnnTreeModel.LanguageDtmf, AnnouncementsCore",
          "Dtmf": "2",
          "Language": "ru-ru",
          "NextId": "2"
        }
      ],
      "ToneHandlerConfig": {
        "$type": "AnnouncementsCore.AnnTreeModel.ToneHandlerConfig, AnnouncementsCore",
        "MaxAttempts": 5,
        "WaitTimeDtmfSec": 5,
        "StartRecognizeAfterPromptDtmf": false
      },
      "Id": "1",
      "NextId": "2",
      "ErrorNextId": "5",
      "IsFirst": true
    },
    {
      "$type": "AnnouncementsCore.AnnTree.AnnMenuNode, AnnouncementsCore",
      "PromptName": "ivr.wma",
      "AcceptDtmf": {
        "$type": "AnnouncementsCore.AnnTreeModel.DtmfAndOutput, AnnouncementsCore",
        "Dtmf": "1",
        "NextId": "3"
      },
      "DeclineDtmf": {
        "$type": "AnnouncementsCore.AnnTreeModel.DtmfAndOutput, AnnouncementsCore",
        "Dtmf": "0",
        "NextId": "4"
      },
      "ToneHandlerConfig": {
        "$type": "AnnouncementsCore.AnnTreeModel.ToneHandlerConfig, AnnouncementsCore",
        "MaxAttempts": 3,
        "WaitTimeDtmfSec": 5,
        "StartRecognizeAfterPromptDtmf": false
      },
      "Id": "2",
      "NextId": "3",
      "ErrorNextId": "5",
      "IsFirst": false
    },
    {
      "$type": "AnnouncementsCore.AnnTree.AnnPlayPromptNode, AnnouncementsCore",
      "PromptName": "AcceptResultPrompt.wma",
      "Id": "3",
      "NextId": null,
      "ErrorNextId": null,
      "IsFirst": false
    },
    {
      "$type": "AnnouncementsCore.AnnTree.AnnPlayPromptNode, AnnouncementsCore",
      "PromptName": "DeclineResultPrompt.wma",
      "Id": "4",
      "NextId": null,
      "ErrorNextId": null,
      "IsFirst": false
    },
    {
      "$type": "AnnouncementsCore.AnnTree.AnnPlayPromptNode, AnnouncementsCore",
      "PromptName": "errorPrompt.wma",
      "Id": "5",
      "NextId": null,
      "ErrorNextId": null,
      "IsFirst": false
    }
  ]
}
```


F.3.1.3 Enabling Text -to-Speech Platform

The actual consent to record announcements can be played from a text-to-speech (TTS) file or from a recorded audio file. If you want to use the TTS method, follow the procedure described below.

➢ **To enable text-to-speech platform:**

1. Download and install Microsoft Speech Platform - Runtime (Version 11) from here:

   https://www.microsoft.com/en-us/download/details.aspx?id=27225

2. After you have the platform installed, now you need to download and install TTS languages which you want to support in yours AN application.
   Microsoft Speech Platform - Runtime Languages (Version 11)

   https://www.microsoft.com/en-us/download/details.aspx?id=27224

   The link above is for download the whole TTS (text to speech) and SR (speech recognition) files.

3. After you download it, you need to install each relevant file you want according to language. For example, if you want to support text to speech for Russian then install the file **MSSpeech_TTS_ru-RU_Elena.msi**.

   For English, install **MSSpeech_TTS_en-US_Helen.msi** or **MSSpeech_TTS_en-US_ZiraPro.msi**.

> **Note:**
> - It is not recommended to install Speech Recognition files because currently AN doesn't support speech recognition. It may support it in the future. If you install SR, it won't damage AN behavior. It just won't be used.
> - It is important to install platform and language from the same Version 11. A combination of Versions 10 and 11 won't work.

4. To enable TTS copy over and if needed modify state machine(s) from the folder ending with tts in …\Program Files\AudioCodes\SmartTAP\AN\Repo to the Program Files\AudioCodes\SmartTAP\AN\StateMachineConfig folder.

F.3.1.4 Consent to Record Calls Demo

➢ To enable playing the demo IVR to External Calling Party:

1. To enable playing the demo IVR to External Calling Party, add the following:
   On each Announcement Server, uncomment and edit the System.config file at Program Files\AudioCodes\SmartTAP\AN\Config\ to have:

```
<System
enableIvr="true"
playIVRToExternalCallingParty="true"
/>
```

2. Restart AN Service.

➢ To enable playing the demo IVR to External Answering Party

1. To enable playing the demo IVR to External Answering Party, add the following:
   On each Announcement Server, uncomment and edit the System.config file at Program Files\AudioCodes\SmartTAP\AN\Config\ to have:

```
<System
enableIvr="true"
playIVRToExternalAnsweringParty="true"
AnnouncementRecipients="BothParties"
/>
```

2. Restart AN Service.
3. On each FE running SmartTAP Plug-in, open the LyncPlugIn.exe.config and modify the AnnouncementCallType parameter to OutboundExternal as shown below:

```
<add key="AnnouncementCallType"
value="OutboundExternal"></add>
```

4. Restart Plug-in Service

➢ To enable playing the demo IVR to External Calling and Answering Parties

1. To enable playing the demo IVR to External Calling and Answering Parties add the following:
   On each Announcement Server uncomment and edit the System.config file at Program Files\AudioCodes\SmartTAP\AN\Config\ to have:

```
<System
enableIvr="true"
playIVRToExternalCallingParty="true"
playIVRToExternalAnsweringParty="true"
```

```
AnnouncementRecipients="BothParties"
/>
```

2. Restart AN Service.
3. On each FE running SmartTAP Plug-in, open the LyncPlugIn.exe.config and modify the AnnouncementCallType parameter to AllExternal as shown below:

```
<add key="AnnouncementCallType" value="AllExternal"></add>
```

4. Restart Plug-in Service

The table below describes all the parameters that can be configured in the System.config file.

F.4 Configuration Parameters

The table below describes the configuration parameters.

Table F-1: System.config File

Parameter	Description
appEndpointDiscoveryName	Defines the value of Skype for Business trusted application endpoint that will be used by this application. The default value is "AnnouncementsApp".
userAgent	Defines the Application User agent. The default value is " AnnouncementsApp".
inviteDest	If the value is not empty, the application will call to this destination and ignore the To header of incoming INVITE. The default value is "".
bufferSize	Defines buffer size of transferring data between calls. The default value is "60".
supervisedTransferHeaderName	Defines the header name of supervised transfer INVITE that should be returned by the FE to the application. The default value is "X-Announcements-Supervised-Transfer".
supervisedTransferHeaderValue	Defines the header value of supervised transfer invite that should be returned by FE to the application. The default value is "$1MsplApp".
outCallPassThroughHeaderNames	Defines the headers to pass from in call to out call. The default value is "Ms-Exchange-Command;HISTORY-INFO" e.g.,"headerNameA;headerNameB;headerNameC".
inCallPlayPrompt	Defines playing announcements to in call before the call is accepted. Possible values: ▪ True ▪ False (default)
inCallPlayPromptFilePath	Defines the file path of in call announcements. The default value is "".
outCallPlayPrompt	Defines playing announcements to out call after the call is accepted. Possible values: • True • False (default)

Parameter	Description
outCallPlayPromptFilePath	Defines the file path of out call announcements. The default value is "".
diagnosticsHeaderName	Defines the diagnostics header name. The default value is X-Announcements-DIAGNOSTICS.
maxEndpointDiscoveryMiliSeconds	Defines the maximum time in milliseconds to wait for first application endpoint discovery. The application exits if no endpoints are discovered within this time. The default value is 30000.
maxPlayPromptsMiliSeconds	Defines the maximum time in milliseconds to play prompts. The default value is 1800000.
nlogNetworkLayout	Defines the Nlog network layout. The default value is: ▪ ${longdate} ${level} ${message} ▪ ${exception:format=Message}${newline}
referredByAddedParamName	This parameter name is added to the SIP 'Referred-By' header. The default value is " X-Announcements".
referredByAddedParamValue	This parameter value is added to the SIP 'Referred-By' header. The default value is " AnnouncementsApp".
transferType	Defines the Transfer Type. Valid Values: ▪ Attended - Perform attended transfers. ▪ Unattended - Performs unattended transfers.
AnnouncementRecipients	This parameter determines how the Announcement server plays the prompt. Valid Values: • CallingParty - announcement played only to calling party. • BothParties - announcement played to calling party and called party as well.
webServiceBaseUrl	Describes the listening URL of the Announcement server's Web service Rest API.
enableMoh	Sets true to enable Music on Hold. Possible values: • True (default) • False
mohFileName	Defines the Music on Hold file name. The file must be located in the project directory tree inside the MusicOnHold directory. The default value is " music-default.wma".
enableIvr	If this parameter is set to "true", the IVR will be played instead of an Announcement for an incoming call. Possible values: • True • False (default)
playIVRToExternalCallingParty	If this parameter is set to "true", the IVR will be played to a calling external user. Possible values: • True (default) • False

Parameter	Description
playIVRToExternalAnsweringParty	If this parameter is set to "true", the IVR will be played to an answering external user. Possible values: ▪ True ▪ False (default) Note: In order to play the announcement to an answering party, the AnnouncementRecipients parameter has to be set to"BothParties".
ivrResultParamName	Defines the parameter name that will be added in the referred-By header. The default value is "X-AnnIvrResult".
ivrCleanerSec	Clean stale calls IVR container every period of time in seconds. The default value is 1800.
impersonateInCall	If true, in call will be impersonated, i.e. for the P-Asserted header of 200 OK, the value in the header will not be Announcement user/ID?? and instead the original destination user. Possible values: • True • False (default)
uaReceiveReferRegex	if UserAgent matches the regular expression then the REFER will be sent to this device. Solves a problem with the Polycom 500VVX phone where AN should send the SIP Refer to the phone when rerouting the call to the original destination. Default value: "PolycomVVX-VVX_500"
asList	Application server comma-separated list. AN sends alarms to the AS in the list. For example http://10.21.8.120:80,https://10.21.80.170:443
restClientTimeoutMiliseconds	Alarms timeout in milliseconds. Default Value: 5000
normalizeNumbers	The parameter should be set to true when normalization of called numbers in the Announcement server is required. AN will normalize the called number before rerouting the call to the original destination. Possible values: • True • False (default)
managedDeviceHeartbeatIntervalMs	Interval in milliseconds between each heartbeat request to AS. valid range [1000 - max int] Default Value: 30000
disableAlarms	Set true to disable the alarms mechanism. Possible values: True False (default)

Parameter	Description
uaDontReceiveReferRegex	A regular expression (case insensitive). If the value of the UserAgent header matches the expression then the SIP refer will not be sent to that device when rerouting the call to the original destination. This solves the problem of S4B clients answering 488 not acceptable on reception of SIP INVITE with replaces from the mobile clients. Default Value: "ucwa"
noAttentedTransferSupportRegex	A regular expression (case insensitive). When one of the devices in the call to AN doesn't support the Attended transfer, AN will execute the UnAttended transfer. Mobile clients (S4B) and voicemail don't support Attended transfers. Default Value: "ucwa"
redirectIfReferNotSupported	When the caller doesn't support refer, AN may redirect the caller without playing AN (true) or disconnect the call (false. In BothParties mode redirect the caller if both sides don't support refer (true), or disconnect the calls (false) Possible values: True (default) – AN redirects the caller False – AN disconnects the call
voicemailRegex	A regular expression (case insensitive). The parameters is used to identify voicemail as a participant of the call routed through the AN according to 'user-agent' and 'server' headers. Default Value: "Exchange"
dontPlayAnnRegex	A regular expression (case insensitive). The parameters are used to identify conference as a participant of the call routed through the AN according to 'user-agent' and 'server' headers. Default Value: "AV-MCU"
isPlayAnnIfAnsweredByVoicemail	The announcement is not played to the caller when the call routed through AN is answered by the voicemail. Possible values: True False (default)
AnnouncementBlackList	Announcements will not be played for calls that are defined in a Comma-separated designated “Black list” including destination numbers and usernames, for example: "911,Bob.Johnson,086812344". Default Value: "911"

For AN Server installation instructions, refer to the *SmartTAP Installation Guide*.

F.5 Examples of Configuration

Configure the System.config file system element as follows:

- Play announcement to both sides of a call:

```
<System
          inCallPlayPrompt="true"
inCallPlayPromptFilePath="rec_headphone.wma"
            outCallPlayPrompt="true"
outCallPlayPromptFilePath="ron_rec.wma"
            AnnouncementRecipients="CallingParty"
        />
```

- To play IVR to both sides of an external call, a call with a PSTN or federated parties:

```
<System
 enableIvr="true" enableMoh="true" mohFileName="music-
default.wma" playIVRToExternalCallingParty="true"
playIVRToExternalAnsweringParty="true"
AnnouncementRecipients="BothParties"

/>
```

F.6 Advanced Call Scenarios

Targeted for recording users may participate in advanced call scenarios such as call transfer, call forwarding and conferencing. This section describes whether the configured announcement function is triggered in these advanced call scenarios. The triggering of the announcement in the advanced scenarios doesn't depend on the ANN configuration except for the parameters that are mentioned in this section and therefore the configuration is not defined below.

F.6.1 Call Transfers

The following table defines call transfer scenarios and the announcements generation. For all of the scenarios, A calls B, B answers the call, B put A on hold, B calls to C (this doesn't take place in blind transfer scenario) and B transfers A to C.

Table F-2: Call Transfer Scenarios

Call Scenario	Targeted Users	Flow and expected results from AN (the second line is not applicable in case of blind transfer)
Supervised/blind transfer	A	1 A calls B, B answers: announcement is played. 2 B puts A on hold and calls C, C answers: no announcement is played. 3 A connected to C: no announcement (set AllowMultipleAnnSameUser to true to play).
Supervised/blind transfer	B	1 A calls B, B answers: announcement is played 2 B puts A on hold and calls C, C answers: announcement is played 3 A connected to C: no announcement (set AllowMultipleAnnSameUser to true to play)
Supervised/blind transfer	C	1 A calls B, B answers: no announcement is played.

Call Scenario	Targeted Users	Flow and expected results from AN (the second line is not applicable in case of blind transfer)
		2 B puts A on hold and calls C, C answers: announcement is played. **3** A is connected to C: announcement is played.
Supervised/blind transfer	A + B	**1** A calls B, B answers: announcement played **2** B puts A on hold and calls C, C answers: announcement played **3** A is connected to C: no announcement is played(set AllowMultipleAnnSameUser to true to play)
Supervised/blind transfer	A + C	**1** A calls B, B answers: announcement is played **2** B puts A on hold and calls C, C answers: announcement is played **3** A connected to C: no announcement (set AllowMultipleAnnSameUser to true to play)
Supervised/blind transfer	B + C	**1** A calls B, B answers: announcement is played **2** B puts A on hold and calls C, C answers: announcement is played **3** A connected to C: no announcement is played (set AllowMultipleAnnSameUser to true to play)
supervised transfer	A + B + C	**1** A calls B, B answers: announcement is played **2** B puts A on hold and calls C, C answers: announcement is played **3** A and C are in a conversation: no announcement (set AllowMultipleAnnSameUser to true to play)

F.6.2 Call Forward and Simultaneously Ring

The following table defines playing announcements when a call to an internal user is answered by another user/number/group on behalf of the originally called user.

Table F-3: Call Forwarding and Simultaneous Ringing

Call Scenario	Targeted Users	Flow and expected results from ANN
forward/team call	A	A calls B, C answers: announcement is played
forward/team call	B	A calls B, C answers: announcement is played
forward/team call	C	A calls B, C answers: announcement is played
forward/team call	A + B	A calls B, C answers: announcement is played
forward/team call	A + C	A calls B, C answers: announcement is played
forward/team call	B + C	A calls B, C answers: announcement is played
forward/team call	A + B + C	A calls B, C answers: announcement is played

F.6.3 Conferences

Playing announcements on the calls of targeted users with a conference bridge are not currently supported. with SmartTAP team the feature status if you need it.

F.6.4 Video calls

Video calls routed to the ANN are handled as audio-only calls, the video part of the call is stripped. Once the call is transferred to the original destination the video of the call can be reinitiated.

F.6.5 Mobile Clients and Voice Mail

Announcements are played for calls with mobile clients as defined in previous sections with an exception to the following scenarios:

- The AN is configured to play an announcement to the calling party only mode (AnnouncementRecipients=CallingParty). The mobile client calls to another party where the mobile client, another party or both are targeted users. In this scenario, the announcement is not played.
- The AN is configured to play an announcement to both parties mode (AnnouncementRecipients=BothParty). The mobile client calls to another party where the mobile client, another party or both are targeted users. The call is answered by voice mail. In this scenario, the announcement is not played.
- The AN is configured to play an announcement to both parties mode (AnnouncementRecipients=BothParty). The mobile client calls to another Skype For Business party (not including voice mail), the announcement is played and when completed, the call is disconnected. A new call is automatically created by the other party to the mobile client that needs to answer to connect the call.

This page is intentionally left blank.

International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
27 World's Fair Drive,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide
Website: www.audiocodes.com

Document #: LTRT-27169