Administrator Guide

AudioCodes SmartTAP™ 360°

SmartTAP 360°

SmartTAP 360° Enterprise Recording Solution

Version 5.2

audiocodes

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: October-15-2020

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 website at https://www.audiocodes.com/services-support/maintenance-and-support.

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 website at https://online.audiocodes.com/documentation-feedback.

Stay in the Loop with AudioCodes

Abbreviations and Terminology

Microsoft Skype for Business and Microsoft Lync are used interchangeably in this document unless otherwise specified. References to Microsoft Teams are explicitly indicated.

Related Documentation

Document Name
SmartTAP 360° Release Notes
SmartTAP 360° Installation Guide
SmartTAP 360° for Microsoft Teams Deployment Guide

Document Revision Record

LTRT	Description
27173	Updated Sections: Managing Recording Profiles; Searching for Calls; Timeline View; Playing Back Recorded Media; Features Overview (Multilingual support); Getting Acquainted with the GUI; License Configuration parameters; Concurrent Recording Licenses; Configuring Email Server Settings; Modifying the Media Location; Viewing Managed Devices; Announcement Server (Skype for Business); Simple Annoucement; Annoucement Server Configuration Parameters; Managing Security Profiles; Annoucement Server -Example Configurations renamed Example Announcement Server Scenarios (including PSTN and Federated Calls and All Inbound Calls); Managing Users; Using the Evaluation feature; Alarm Notifications Added Sections: Saving Search Queries; Deleting Calls and Instant Messages Removed Section: Recording Beep Tones (merged to Section "Editing Media Proxy Server" in the SmartTAP 360° Installation Guide)
27174	Updated Sections: Features Overview; About this Guide; Inter-Components Communication; Skype for Business and Teams Desktop Sharing; Configuring an LDAP User Added Sections: Adding a Microsoft Teams User Attribute; Microsoft Azure Active Directory; Microsoft Blob Storage
27175	Updated Sections: Step 5 Add Azure Active Directory Mapping in SmartTAP 360°; Determining Storage Statistics; Configuring Media

Table of Contents

1 About SmartTAP 360° ... 1

SmartTAP 360° Benefits ... 2

Competitive Advantages ... 3

Features Overview ... 3

Architecture ... 10

About this Guide ... 11

2 Logging In ... 13

Logging in with Microsoft Office 365 Credentials ... 13

3 Getting Acquainted with the GUI ... 16

Determining User/Device Status ... 18

4 Performing Initial Configuration ... 22

5 Testing the Initial Configuration ... 24

Making Sure a Recording is in Progress ... 24

Listening to a Recording and Viewing a Video ... 24

6 Configuring Advanced Features ... 26

Viewing/Searching an Audit Trail ... 26

Exporting an Audit Trail ... 28

Managing Licenses ... 29

Targeted User Licenses ... 29

Concurrent Recording Licenses ... 29

License Configuration Parameters ... 30

Viewing Managed Devices ... 31

Inter-Components Communication ... 34

Adding a Device Manually to the Application Server ... 35

Alarms ... 36

Alarm History ... 36

Alarm Notifications ... 36

Monitoring System Health ... 40

Windows Event Log ... 41

SCOM Integration ... 43

Monitoring Storage Statistics ... 44

Using Call Tagging ... 45

Adding a Call Tag ... 46

Viewing / Deleting a Call Tag ... 48

Assigning Values to a Call Tag and Applying to Call ... 48

Generating and Loading HTTPS Certificates ... 49

Browser Connection Certificate Requirements ... 49

Step 1: Generate Certificate Signing Request (CSR) ... 50

Viewing/Modifying the Certificate List ... 52

Step 2: Load Certificates ... 54

Loading Web Browser Certificate 54
Loading Digital Files Certificate 55
Configuring Call Retention 59
Save on Demand Call Retention 61
Configuring System Settings 62
Configuring a Digital Signature 62
Configuring Email Server Settings 62
Configuring Media 64
Configuring User Credentials 65
Extracting User Credentials from Microsoft Azure Fileshare Account 67
Setting up Microsoft Azure Blob Storage Account 69
Adding a Recording Location 71
Viewing and Modifying a Recording Location 76
Defining a Recording Format 77
Configure Live Monitoring Location 78
Configuring Single Sign-On 80
Validating SSO 82
Configuring Web Session Timeout 82
Configuring an LDAP Connection 82
Configuring SSL 85
Configuring an LDAP User 87
Configuring User Mappings 88
Configuring Group Mappings 93
Configuring Security Group Mappings 96
Configuring OVOC Connection 98
Managing Users 101
Sending Email 103
Managing Groups 105
Managing Security Profiles 108
Managing Recording Profiles 112
Viewing or Modifying Recording Profiles 118
Assigning Recording Profile to User or Device 119
Managing Recordable Devices 121
Recording Profile-Call Type Configuration Examples 124
Adding a Device Attribute 126
Adding a General Device Attribute 127
Adding a Device Attribute for Recording 128
Adding a Microsoft Teams User Attribute 129
View and Modify Users 130
Update an Admin User 131
Reset User Password 132
Modify a User Password 132
Uploading an Image 133
Managing Calls 134
Searching for Calls 135

Saving Search Queries ... 145
Deleting Calls and Instant Messages ... 146
Playing Back Recorded Media ... 147
Listening to Call and Viewing Call Video ... 149
Skype for Business and Teams Desktop Sharing ... 151
Time Line View ... 154
Downloading Call Recordings ... 159
Downloading an Audio Call ... 159
Downloading a Video Call ... 161
Downloading a Desktop Sharing Call ... 163
Emailing Call Recordings ... 166
Using the Evaluation Feature ... 168
Adding a New Evaluation Form ... 169
Viewing and Copying an Evaluation Form ... 171
Adding a New Section [Evaluation Forms] ... 172
Adding Questions and Answers to an Evaluation Form ... 173
Finalizing Forms ... 176
Performing an Evaluation ... 177
Managing Instant Messages ... 185
Searching for Messages ... 188
7 Single Sign-On for SmartTAP 360° ... 196
Single Sign-On Variables ... 197
Configuring Active Directory for Single Sign-On ... 200
Single Sign-On Client Browser Settings ... 203
Testing Single Sign-On ... 207
Troubleshooting Single Sign-On ... 208
8 SmartTAP 360° Skype for Business Toolbar ... 214
Toolbar Features ... 214
9 Media Exporter ... 217
10 API Integration ... 223
11 Recording Health Monitor ... 225
General Configuration ... 225
REST API Configuration ... 227
SMB Configuration ... 227
Report Formats ... 230
12 Announcement Server (Skype for Business) ... 232
Simple Annoucement ... 232
IVR ... 233
Configuring IVR Script Files ... 233
Enabling Text-to-Speech Platform ... 234
Consent to Record Calls ... 235

Example Annoucement Server Scenarios 237
PSTN and Federated Calls 237
All Inbound Calls 238
Annoucement Server Configuration Parameters 239
Annoucement Server Advanced Call Scenarios 243
13 Microsoft Azure Active Directory 247
Azure Active Directory User Mapping 247
Step 1 Application Registration in Microsoft Azure 247
Step 2 Configure API Permissions 250
Step 3 Configure Certificates & Secrets for Azure AD Mapping 253
Step 4 Configure Azure Active Directory Client in SmartTAP 360° 255
Step 5 Add Azure Active Directory Mapping in SmartTAP 360° 256
Azure Active Directory User Authentication 261
Step 1 Register App in Azure Active Directory 262
Step 2 Check API Permissions 265
Step 3 Configure Certificates & Secrets 267
Step 4 Configure OpenID Connect OIDC Client in SmartTAP 360° 268
Step 5 Assign Security profile to Azure Active Directory user in SmartTAP 360° 270

1 About SmartTAP 360°

SmartTAP 360° is an enterprise-wide compliance and liability recorder. Though most recorders in the market focus on Contact Center features, SmartTAP 360° is deployed across the enterprise to capture calls, either on-demand or, in some cases on-demand.

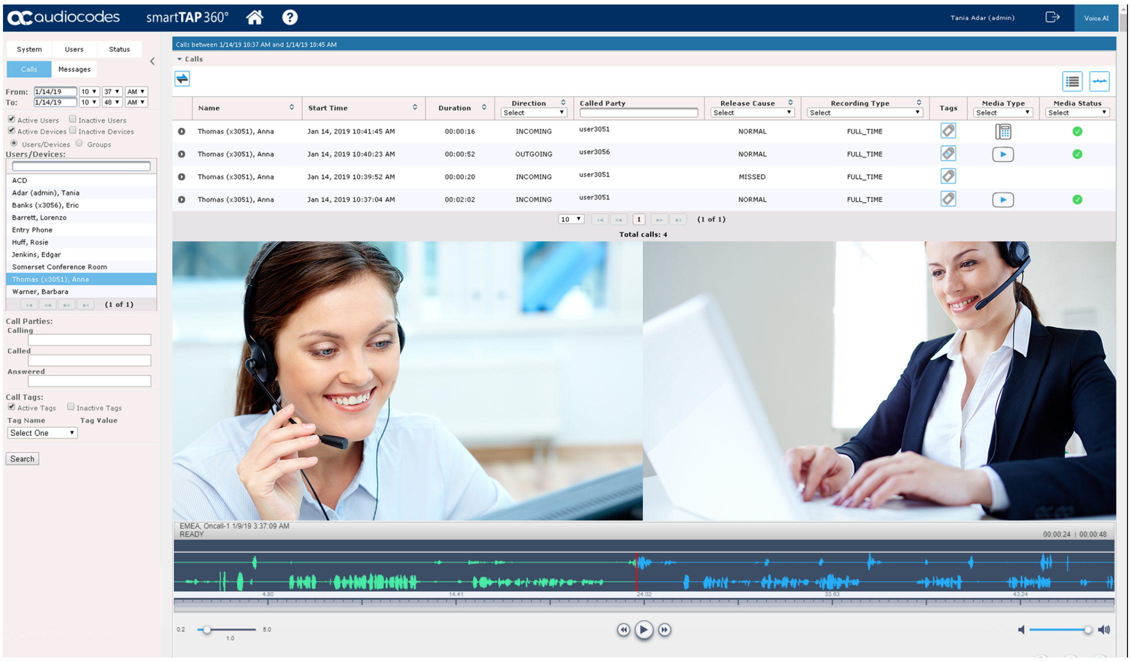
AudioCodes' SmartTAP 360° for Microsoft Teams is a secure call recording solution that enables the recording of key business interactions within a Microsoft SfB and Teams environment. SmartTAP 360° is compatible with VoIP, TDM, and hybrid telephony environments.

Using an integral Skype for Business recording toolbar, enterprise users can record with SmartTAP 360° anywhere and anytime they are on Skype for Business calls. SmartTAP 360° 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.

Figure 1-1: SmartTAP 360° Solution

CAPTURE
ANYWHERE
Supports internal, external and mobile interactions from both remote and federated users
RECORD
EVERYTHING
Full 360° capturing of enterprise voice, video and IM interactions
SIMPLIFIED
MANAGEMENT
Offers cloud, hybrid and on-premise deployments with flexible management options
smartTAP

SmartTAP 360° includes audio video and instant messaging recording capabilities.



From: 1/14/19 10 ▼ 37 ▼ AM ▼
To: 1/14/19 10 ▼ 48 ▼ AM ▼

☑ Active Users ☐ Inactive Users
☑ Active Devices ☐ Inactive Devices
● Users/Devices ○ Groups

Users/Devices:

ACD
Adar (admin), Tania
Banks (x3056), Eric
Barrett, Lorenzo
Entry Phone
Huff, Rosie
Jenkins, Edgar
Somerset Conference Room
Thomas (x3051), Anna
Warner, Barbara
(1 of 1)

Call Parties:
Calling
Called
Answered

Call Tags:
☑ Active Tags ☐ Inactive Tags
Tag Name Tag Value
Select One ▼

Search

Calls between 1/14/19 10:37 AM and 1/14/19 10:45 AM

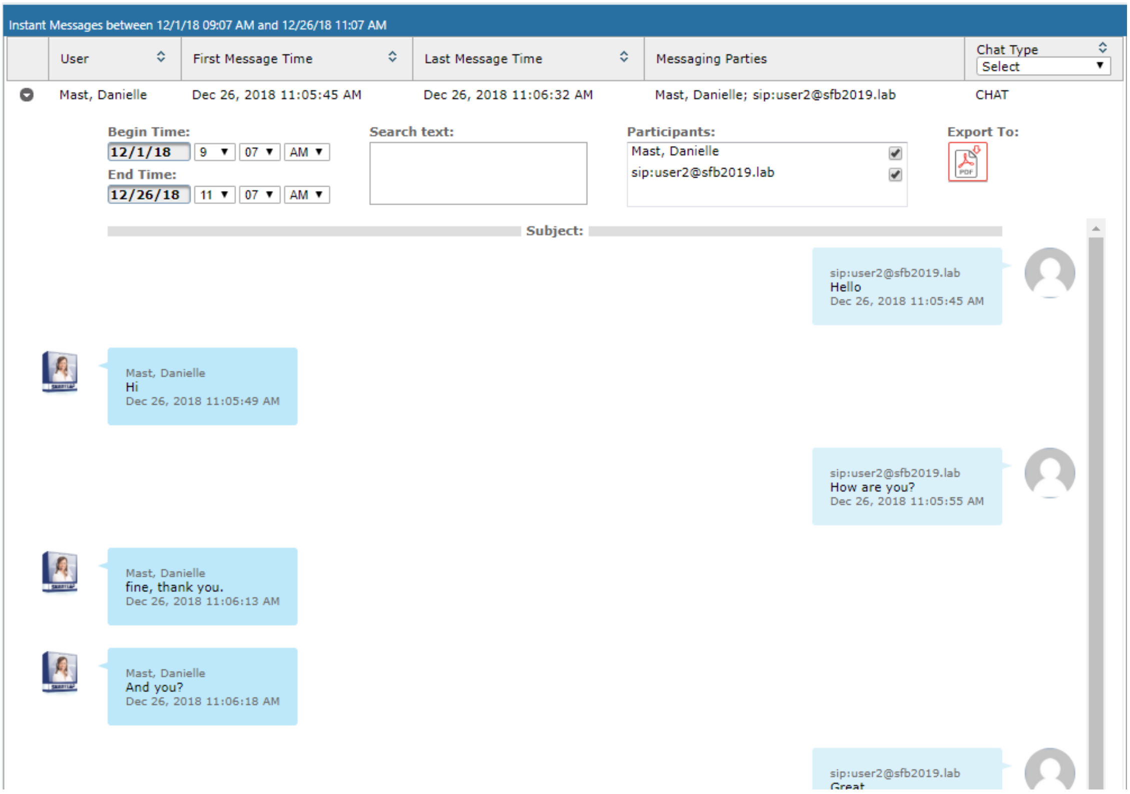
▾ Calls

	Name	Start Time	Duration	Direction Select ▼	Called Party	Release Cause Select ▼	Recording Type Select ▼	Tags	Media Type Select ▼	Media Status Select ▼
●	Thomas (x3051), Anna	Jan 14, 2019 10:41:45 AM	00:00:16	INCOMING	user3051	NORMAL	FULL_TIME			✓
●	Thomas (x3051), Anna	Jan 14, 2019 10:40:23 AM	00:00:52	OUTGOING	user3056	NORMAL	FULL_TIME		▶	✓
●	Thomas (x3051), Anna	Jan 14, 2019 10:39:52 AM	00:00:20	INCOMING	user3051	MISSED	FULL_TIME			
●	Thomas (x3051), Anna	Jan 14, 2019 10:37:04 AM	00:02:02	INCOMING	user3051	NORMAL	FULL_TIME		▶	✓

10 ▼ 1 (1 of 1)

Total calls: 4

EMEA, Oncall-1 1/9/19 3:37:09 AM
READY
00:00:24 / 00:00:48


Instant Messages between 12/1/18 09:07 AM and 12/26/18 11:07 AM

	User	First Message Time	Last Message Time	Messaging Parties	Chat Type Select ▼
●	Mast, Danielle	Dec 26, 2018 11:05:45 AM	Dec 26, 2018 11:06:32 AM	Mast, Danielle; sip:user2@sfb2019.lab	CHAT

Begin Time: 12/1/18 9 ▼ 07 ▼ AM ▼
End Time: 12/26/18 11 ▼ 07 ▼ AM ▼

Search text:

Participants:
Mast, Danielle ☑
sip:user2@sfb2019.lab ☑

Export To:

Subject:

sip:user2@sfb2019.lab
Hello
Dec 26, 2018 11:05:45 AM

Mast, Danielle
Hi
Dec 26, 2018 11:05:49 AM

sip:user2@sfb2019.lab
How are you?
Dec 26, 2018 11:05:55 AM

Mast, Danielle
fine, thank you.
Dec 26, 2018 11:06:13 AM

Mast, Danielle
And you?
Dec 26, 2018 11:06:18 AM

sip:user2@sfb2019.lab
Great

SmartTAP 360° Benefits

SmartTAP 360° 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

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.
- **Economical**
  - Large system features at a fraction of the cost.
  - Linear growth of SmartTAP 360° 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.

Features Overview

The table below lists and describes AudioCodes' SmartTAP 360° recording features.

Table 1-1: SmartTAP 360° 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	■ Record on Demand (ROD): Recording contains audio from

Feature	Details
Demand	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 Web interface or Skype for Business Conversation Window Extension (CWE) toolbar - Save on Demand – Audio or Video recording is manually triggered from the Status page in the GUI or from the Skype for Business CWE toolbar - 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 CWE toolbar. - IM recording – Automatic Instant Message recording.
Security Profiles	- Can be created and assigned to multiple parties to define security access in SmartTAP 360°. - All recordings can be performed using another user's ROD or SOD.
LDAP Integration	- Allows SmartTAP 360° to use Active Directory users, groups, and security groups - LDAP Filtering by user, group or security group.

Feature	Details
Microsoft Teams Integration	■ Record calls of Targeted Users on different devices, including Teams desktop, web, mobile applications and phones. ■ Record the calls audio and desktop sharing. ■ Allow SmartTAP 360° to use Microsoft Azure Active Directory users, groups and security groups
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. ■ 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	■ Number of retention periods can be added and applied to specific user(s).

Feature	Details
	■ 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). ■ Recording stored on Microsoft Azure Blob which is used for high-scale and secure object storage for cloud-native workloads, archives, data lakes, high-performance computing, and machine learning.
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 360° 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 360° server is capable of recording diverse call signaling and voice protocols. ■ SmartTAP 360° records PSTN, Lync, Analog, and VoIP simultaneously and transparently to end users.
Skype for Business Client Toolbar	■ Auto extended Skype for Business 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 Skype for Business CWE, or post call, from the Calls tab.

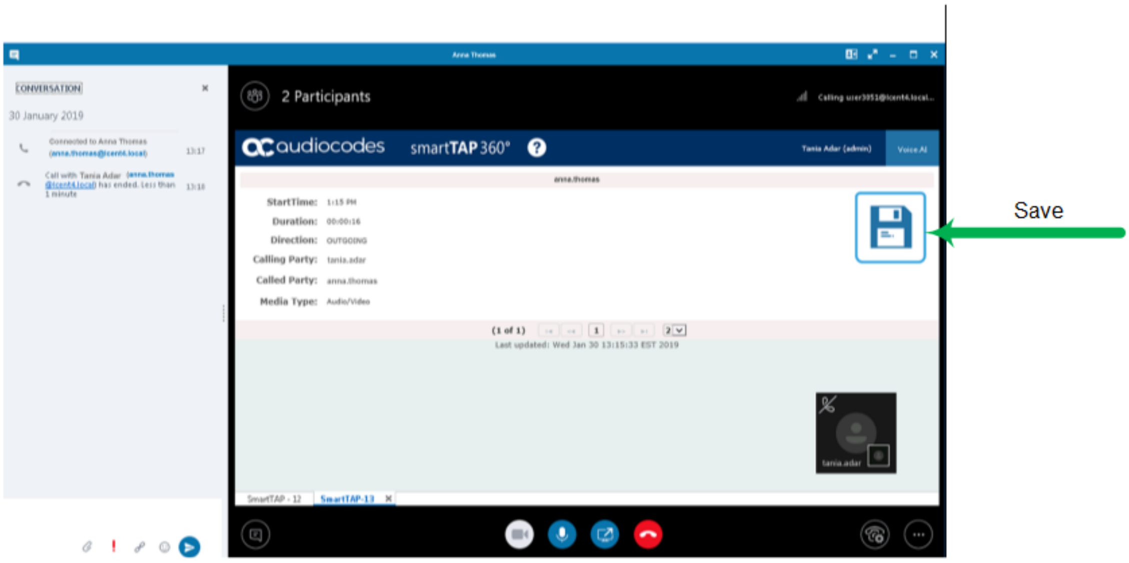
Feature	Details
Single Sign-On	■ A user gains access into the SmartTAP 360° GUI or Skype for Business client toolbar after validation of their SmartTAP 360° security profile and authentication of their credentials with LDAP Active Directory.
SIPRec	■ Session Initiation Protocol (SIP) establishes an active recording session and reporting of metadata to the SRS (SmartTAP 360°) 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 360° to add users, retrieve metadata, download recorders, target users, etc. Refer to SmartTAP REST API 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 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 360° Media Proxy (Skype for Business)	■ 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 360° to capture a copy of the SRTP conversation. ■ Advantages:

Feature	Details
	✓ 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
User / Device Attributes	A SmartTAP 360° user or device attribute has three purposes: ■ Additional information can be added to the user account within SmartTAP 360°, i.e., Ext, Tel URI, Address, etc., for informational purposes only. ■ Designates to SmartTAP 360° 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 360° triggers a recording based on the SIP_URI. ■ Mapping Active Directory attributes to user / device information on SmartTAP 360°. ■ Mapping Microsoft Azure Active Directory Teams users object ID to user properties on SmartTAP 360°.
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).
Desktop Recording	Skype for Business and Microsoft Teams 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.

Feature	Details
New User Interface Design	The SmartTAP 360° User interface design and layout has been updated to the look and feel for AudioCodes product family.
Call Type-based recording	It is now possible to define specific call types to be recorded through SmartTAP 360° recording profiles. For example, it is possible to select recording of the following call types: in domain, PSTN, external, response group calls and more.
Selective Announcement service	The Announcement service can be enabled for recording profile and activated on calls for the users that are associated with the recording profile.
Beep tone generation	Playing recording beep tone to the local call parties is possible with SmartTAP 360° Media Proxy.
Test calls	Enhanced System Health Monitoring with an option to activate periodic test calls and with alarms.
Communication status icons	SmartTAP 360° inter-components communication status shows the statuses reported by managed devices for its connections with other components in the system.
Malicious call recording enhancement	Enables users to save a call recording after the call was ended for a predefined time.
OVOC Management	SmartTAP 360° server components can be monitored from OVOC (starting from OVOC version 7.6.100) including the sending of alarms and statuses.
Support for Skype For Business 2019	SmartTAP 360° Annoucement and Application servers can be installed on the Skype For Business 2019 platform.
Original Call Reason	Original call release reason is presented as part of the call recording meta-data.
Scalability	SmartTAP 360° SIPRec solution scalability enhancement with an option to reroute a call to another recording server when the server is at the maximum capacity.
SmartTAP 360° low-end Profile	SmartTAP 360° low-end profile system can be deployed on the Mediant 1000B OSN4B 256 GB SSD alongside the SBA with up to 250 users and 8 trunks.
Multilingual support	The SmartTAP 360° interface supports the following languages: ■ English

Feature	Details
	■ German ■ Spanish ■ French

Figure 1-2: Save on Demand (SOD) in SmartTAP 360° Client (Skype for Business)



CONVERSATION

30 January 2019

Connected to Anna Thomas (anna.thomas@icent4.local) 13:17

Call with Tania Adar (anna.thomas@icent4.local) has ended. Less than 1 minute 13:18

anna.thomas

StartTime: 1:15 PM

Duration: 00:00:16

Direction: OUTGOING

Calling Party: tania.adar

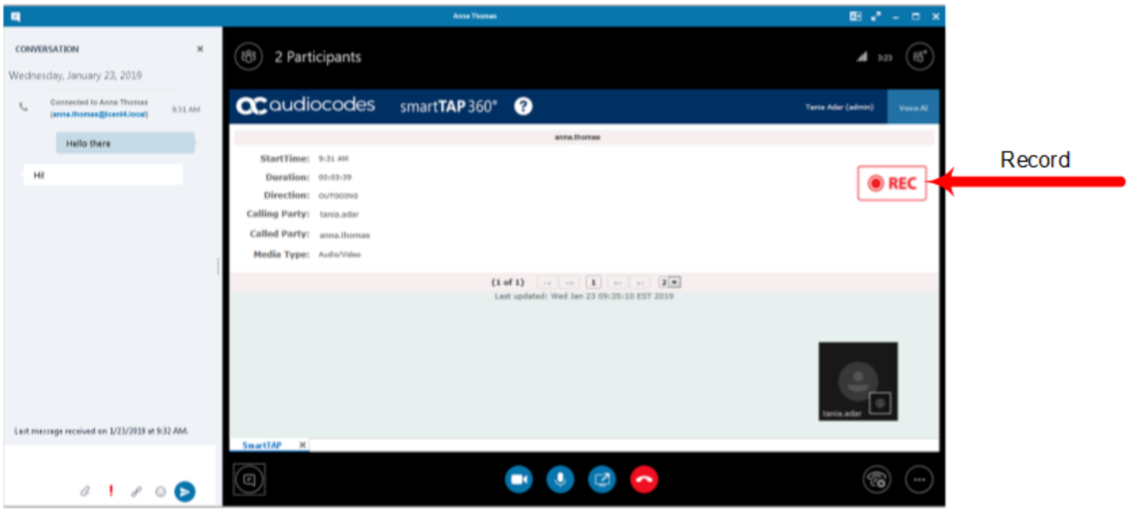
Called Party: anna.thomas

Media Type: Audio/Video

(1 of 1) 1 2

Last updated: Wed Jan 30 13:15:33 EST 2019

Figure 1-3: Record on Demand (ROD) in SmartTAP 360° Client (Skype for Business)



CONVERSATION

Wednesday, January 23, 2019

Connected to Anna Thomas (anna.thomas@icent4.local) 9:31 AM

Hello there

Hi!

Last message received on 1/23/2019 at 9:32 AM.

anna.thomas

StartTime: 9:31 AM

Duration: 00:03:39

Direction: OUTGOING

Calling Party: tania.adar

Called Party: anna.thomas

Media Type: Audio/Video

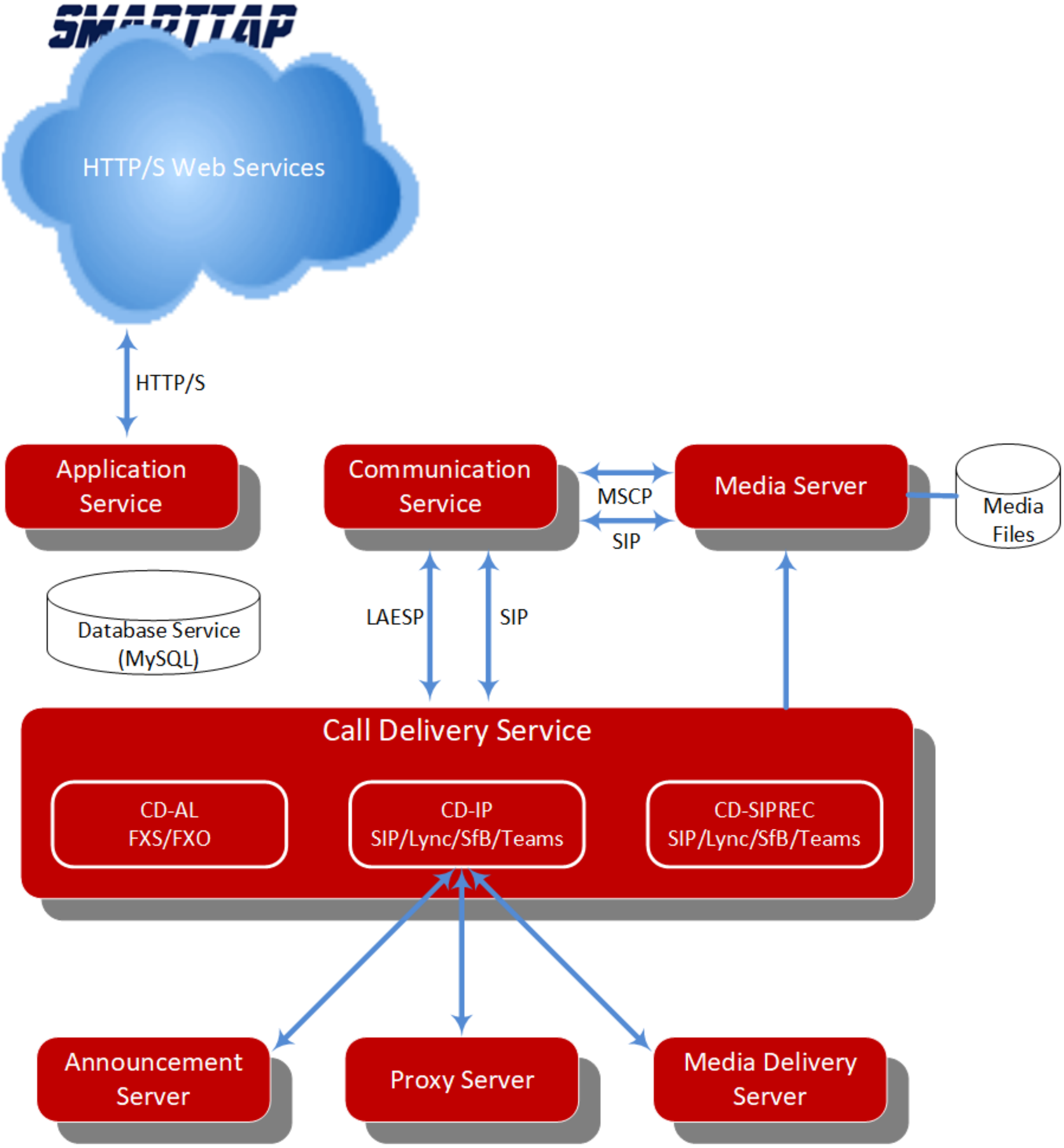
(1 of 1) 1 2

Last updated: Wed Jan 23 09:35:10 EST 2019

Architecture

The figure below illustrates SmartTAP 360° architecture.

Figure 1-4: SmartTAP 360° Architecture



About this Guide

This guide helps enterprise network administrators obtain full benefit from the SmartTAP 360° Call Recording System. The guide comprises the following sections:

Table 1-2: About this Document

Section	Description
Logging In on page 13	Shows how to log in to the SmartTAP 360° Web Interface.
Getting Acquainted with the GUI on page 16	Gets the network administrator acquainted with the SmartTAP 360° management GUI.

Section	Description
Performing Initial Configuration on page 22	Describes the steps to take to perform initial SmartTAP 360° configuration in order to record a call.
Searching for Messages on page 188	Searching for Messages
Searching for Calls on page 135	Searching for Calls
Testing the Initial Configuration on page 24	Shows how to record a call to test the initial configuration.
Configuring Advanced Features on page 26	Details the user interface, features and procedures.
Single Sign-On for SmartTAP 360° on page 196	Shows how to simplify the login process for domain users with Single Sign-On (SSO).
SmartTAP 360° Skype for Business Toolbar on page 214	Shows how to use the SmartTAP 360° Skype for Business toolbar.
Media Exporter on page 217	Describes the Bulk Media Exporter tool to download Meta Data and Call Records.
API Integration on page 223	Describes the API Reference.
Recording Health Monitor on page 225	Describes the Recording Health Monitor utility
Announcement Server (Skype for Business) on page 232	Describes the setup and use of the Annoucement Server (Skype for Business)
Microsoft Azure Active Directory on page 247	Describes the setup for Microsoft Azure Active Directory Teams user mapping and authentication.
Setting up Microsoft Azure Blob Storage Account on page 69	Describes how to configure Microsoft Blob Storage that is used for saving recorded media in the Microsoft Teams deployment.

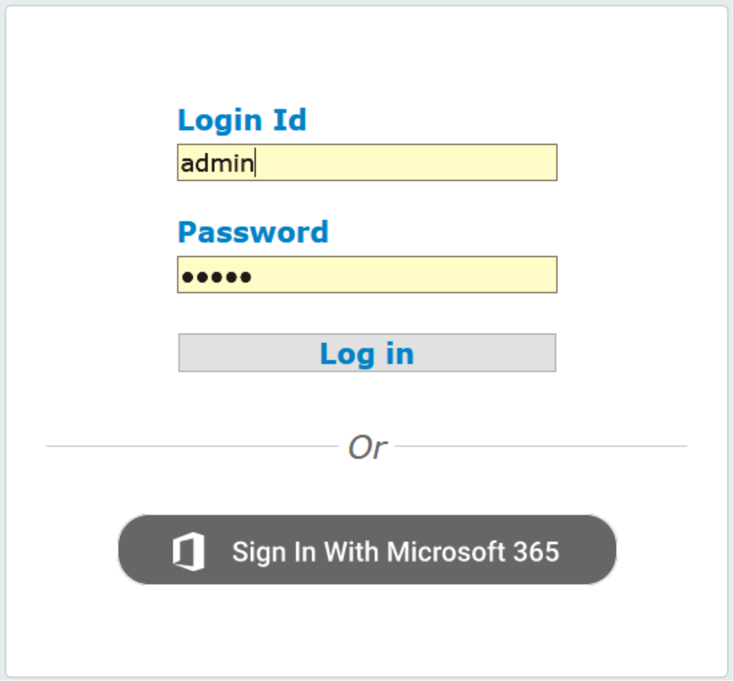
2 Logging In

After the SmartTAP 360° software is installed, an Admin user account is created by default. This user account allows the administrator to access the SmartTAP 360°'s Web-based management tool for the first time and start initial configuration and administration (see Chapter Performing Initial Configuration on page 22). Alternatively, you can log in using the credentials of the Office 365 user.

➢ **To log in:**

1. Access the SmartTAP 360° user interface from a browser.
2. Enter the SmartTAP 360° server IP address or hostname; the Login page opens.

Figure 2-1: Login Page



Login Id

admin

Password

●●●●●

3. Log in using one of the following options:
   - Enter default Login ID 'Admin' and default password 'Admin'
   - Enter the credentials of the Microsoft 365 Office user
4. Click the **Log in** button.

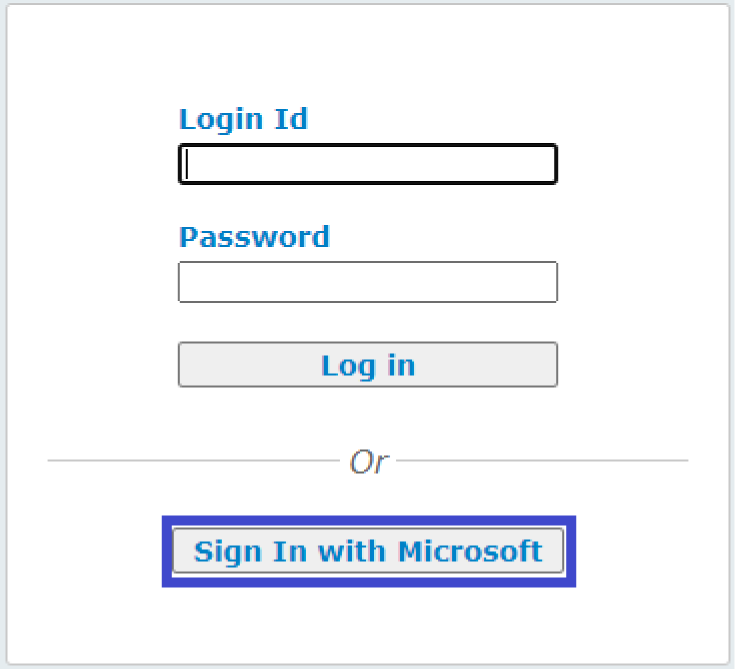
Logging in with Microsoft Office 365 Credentials

This section describes how to login with Microsoft Office 365 Credentials.

➢ **To login with Microsoft Office 365 credentials:**

1. Click **Sign-in with Microsoft** button.

Figure 2-2: Microsoft Sign In



The user is redirected to Microsoft MFC Login page:

Figure 2-3: Microsoft MFC Login Page

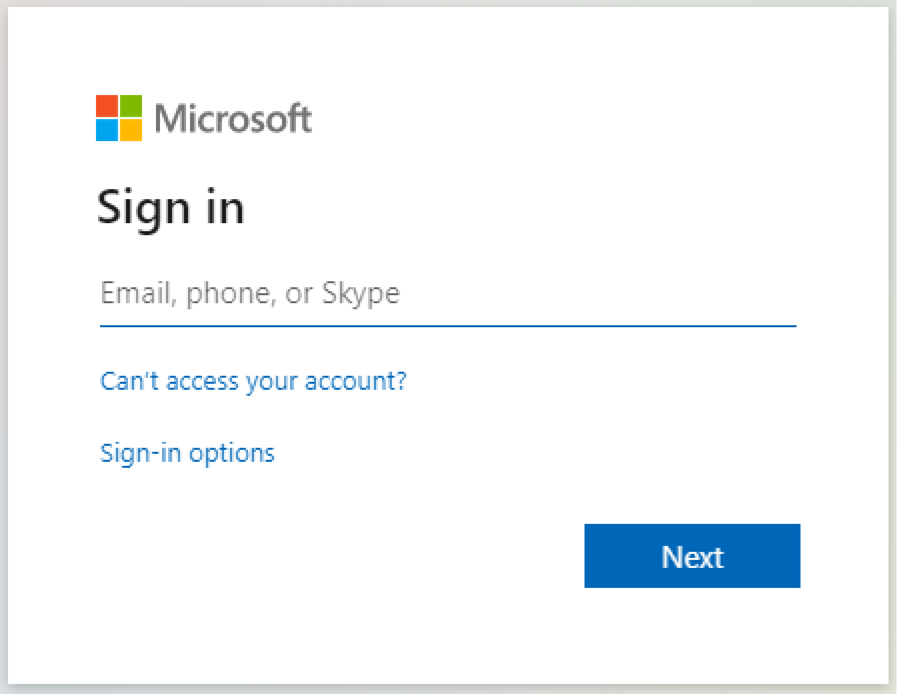
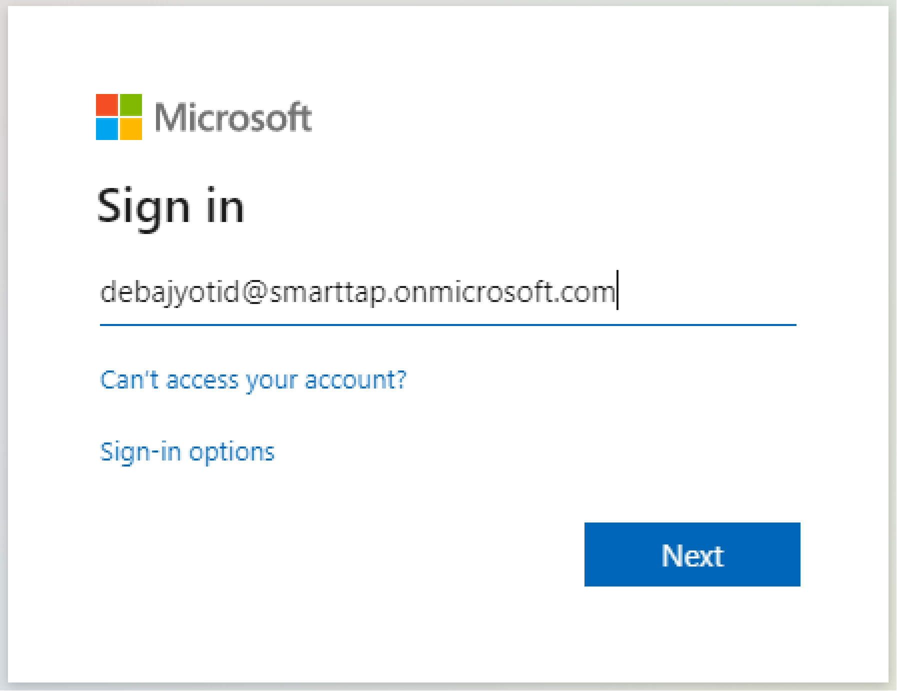


Figure 2-4: Login id

2. Enter the Sign in information and password and click **Next**.

Figure 2-5: Sign in



Microsoft

Sign in

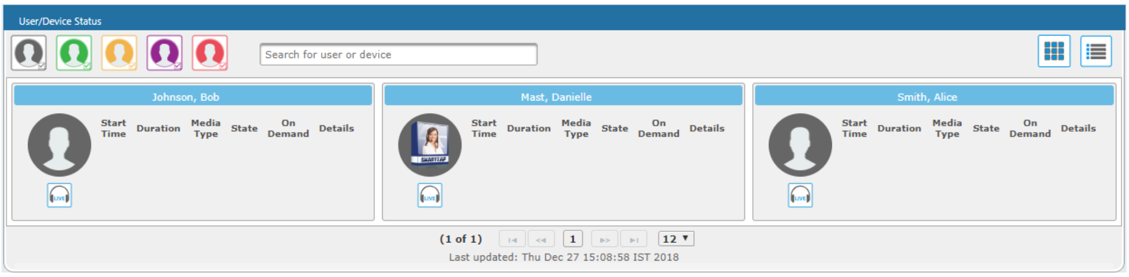
debajyotid@smarttap.onmicrosoft.com

3 Getting Acquainted with the GUI

This section introduces the SmartTAP 360° management GUI. The figure below 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 360° Main Screen – Upper Banner



The table below describes the active buttons on the toolbar.

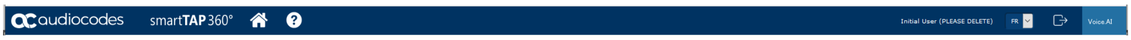
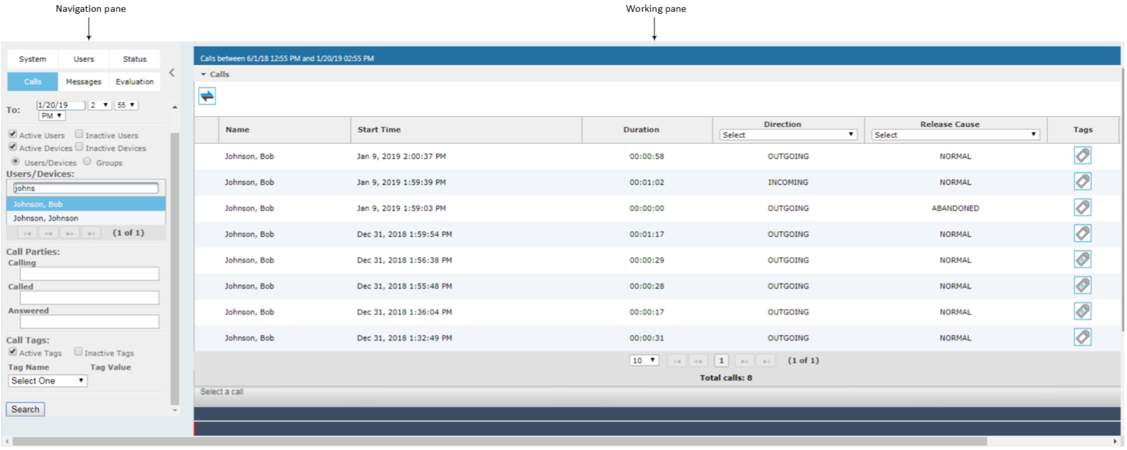


Table 3-1: SmartTAP 360° Main Screen – Active Buttons on the Toolbar

Button	Icon	Description
Home	⌂	Go to the Home Page (default start page)
Help	?	Displays help for the currently displayed content
Language Toggle	EN	Toggles between the following interface languages: - **English** - **German** - **Spanish** - **French**
Log off	⇥	Log off user (identified to the left of this button)

Figure 3-2: SmartTAP 360° Main Screen



Navigation pane

Working pane

To: 1/20/19 2 55 PM

☑ Active Users ☐ Inactive Users
☑ Active Devices ☐ Inactive Devices
● Users/Devices ○ Groups

Users/Devices: johns

Johnson, Bob
Johnson, Johnson
(1 of 1)

Call Parties:
Calling
Called
Answered

Call Tags:
☑ Active Tags ☐ Inactive Tags
Tag Name Tag Value
Select One

Calls between 6/1/18 12:55 PM and 1/20/19 02:55 PM

Calls

Name	Start Time	Duration	Direction Select	Release Cause Select	Tags
Johnson, Bob	Jan 9, 2019 2:00:37 PM	00:00:58	OUTGOING	NORMAL	
Johnson, Bob	Jan 9, 2019 1:59:39 PM	00:01:02	INCOMING	NORMAL	
Johnson, Bob	Jan 9, 2019 1:59:03 PM	00:00:00	OUTGOING	ABANDONED	
Johnson, Bob	Dec 31, 2018 1:59:54 PM	00:01:17	OUTGOING	NORMAL	
Johnson, Bob	Dec 31, 2018 1:56:38 PM	00:00:29	OUTGOING	NORMAL	
Johnson, Bob	Dec 31, 2018 1:55:48 PM	00:00:28	OUTGOING	NORMAL	
Johnson, Bob	Dec 31, 2018 1:36:04 PM	00:00:17	OUTGOING	NORMAL	
Johnson, Bob	Dec 31, 2018 1:32:49 PM	00:00:31	OUTGOING	NORMAL	

10 1 (1 of 1)

Total calls: 8

Select a call

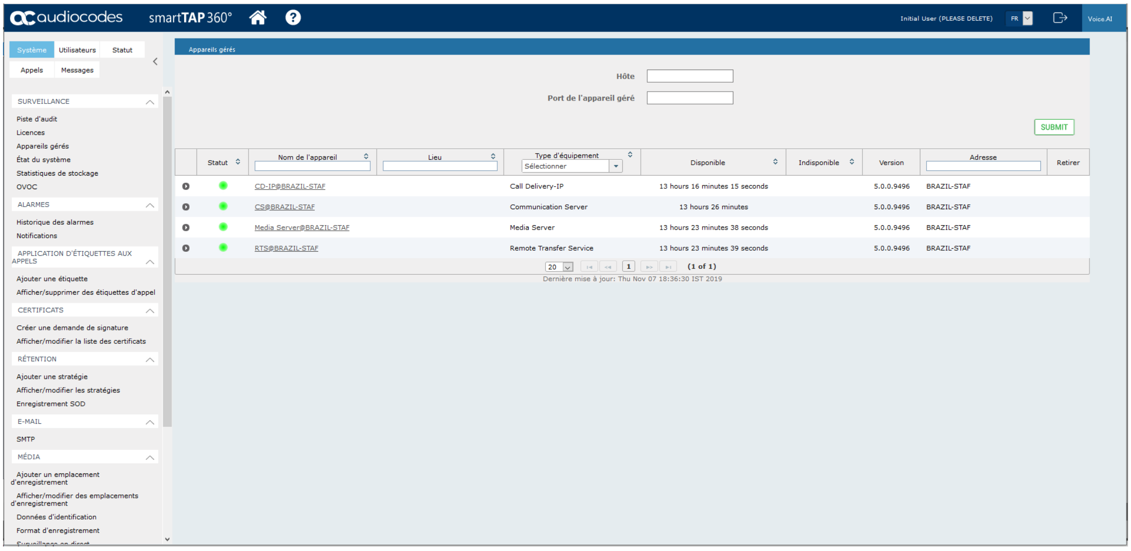
The figure above shows the following three areas below the upper banner:

- 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 failure/success:
  - Green font = successful execution
  - Red font = failed execution, with the reason for the failure
- Multilingual support:

  You can toggle in the Toolbar to display the user interface in the following languages:
  - **English (default)**
  - **German**
  - **Spanish**
  - **French**

Figure 3-3: Multilingual Support

Figure 3-4:



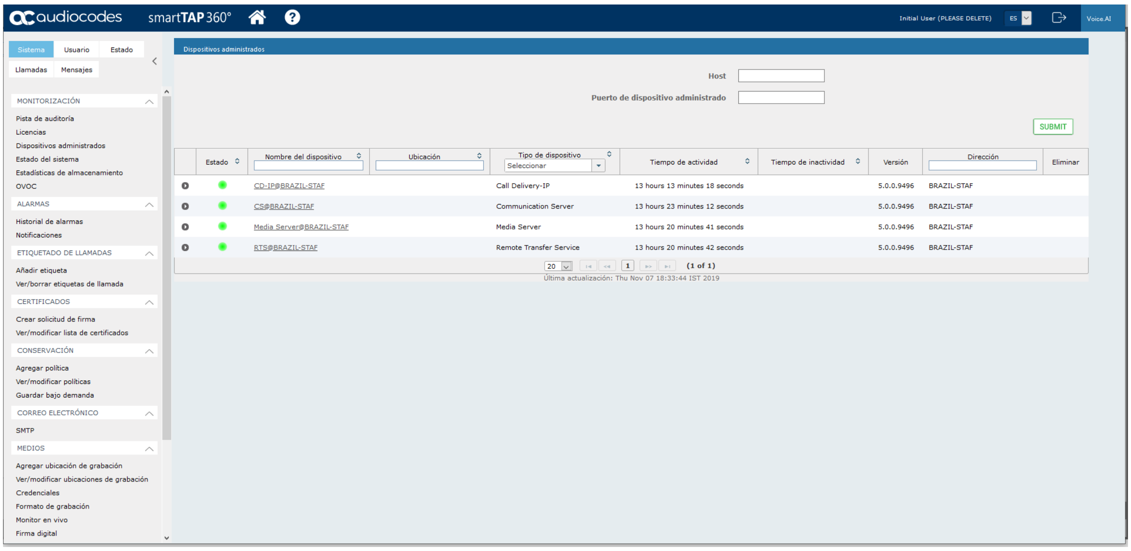
Hôte

Port de l'appareil géré

	Statut	Nom de l'appareil	Lieu	Type d'équipement Sélectionner	Disponible	Indisponible	Version	Adresse	Retirer
●	●	CD-IP@BRAZIL-STAF		Call Delivery-IP	13 hours 16 minutes 15 seconds		5.0.0.9496	BRAZIL-STAF	
●	●	CS@BRAZIL-STAF		Communication Server	13 hours 26 minutes		5.0.0.9496	BRAZIL-STAF	
●	●	Media Server@BRAZIL-STAF		Media Server	13 hours 23 minutes 38 seconds		5.0.0.9496	BRAZIL-STAF	
●	●	RTS@BRAZIL-STAF		Remote Transfer Service	13 hours 23 minutes 39 seconds		5.0.0.9496	BRAZIL-STAF	

20 1 (1 of 1)

Dernière mise à jour: Thu Nov 07 18:36:30 IST 2019



Host

Puerto de dispositivo administrado

	Estado	Nombre del dispositivo	Ubicación	Tipo de dispositivo Seleccionar	Tiempo de actividad	Tiempo de inactividad	Versión	Dirección	Eliminar
●	●	CD-IP@BRAZIL-STAF		Call Delivery-IP	13 hours 13 minutes 18 seconds		5.0.0.9496	BRAZIL-STAF	
●	●	CS@BRAZIL-STAF		Communication Server	13 hours 23 minutes 12 seconds		5.0.0.9496	BRAZIL-STAF	
●	●	Media Server@BRAZIL-STAF		Media Server	13 hours 20 minutes 41 seconds		5.0.0.9496	BRAZIL-STAF	
●	●	RTS@BRAZIL-STAF		Remote Transfer Service	13 hours 20 minutes 42 seconds		5.0.0.9496	BRAZIL-STAF	

20 1 (1 of 1)

Última actualización: Thu Nov 07 18:33:44 IST 2019

Determining User/Device Status

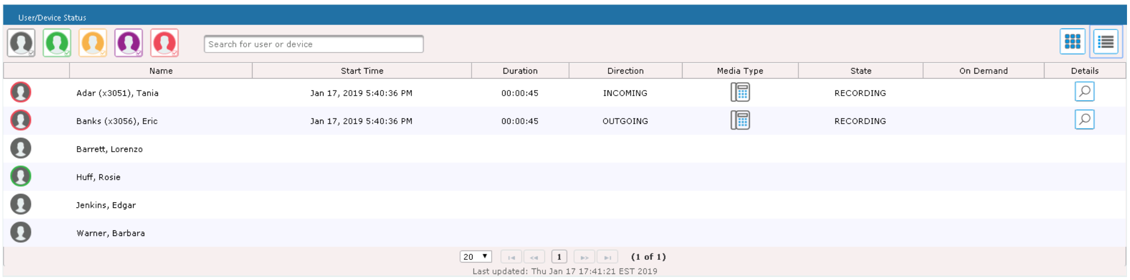
The User/Device Status screen is accessible by clicking the Home button on the upper banner, or by selecting **Status** tab > **User Call Status**. The screen features two views:

- **Grid**
- **List**

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

The figure below shows the List View ☰

Figure 3-5: List View



User/Device Status

Search for user or device

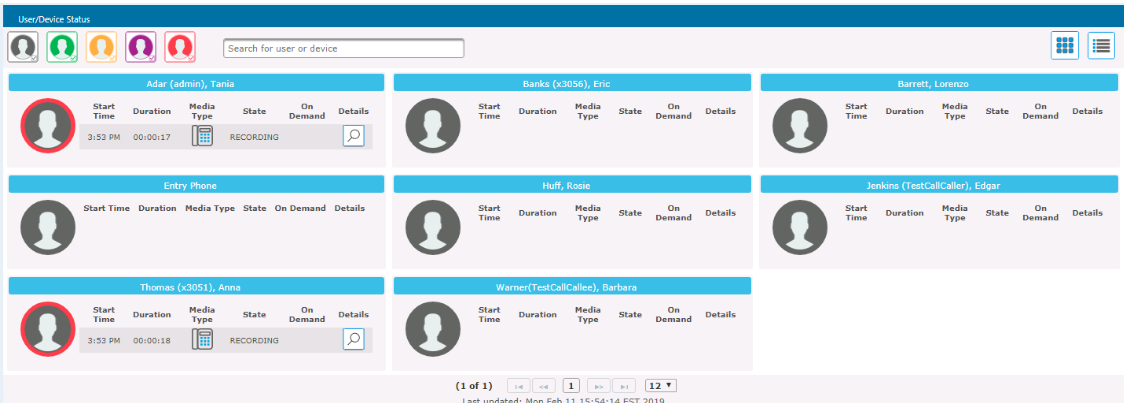
	Name	Start Time	Duration	Direction	Media Type	State	On Demand	Details
	Adar (x3051), Tania	Jan 17, 2019 5:40:36 PM	00:00:45	INCOMING	☎	RECORDING		⌕
	Banks (x3056), Eric	Jan 17, 2019 5:40:36 PM	00:00:45	OUTGOING	☎	RECORDING		⌕
	Barrett, Lorenzo							
	Huff, Rosie							
	Jenkins, Edgar							
	Warner, Barbara							

20 ▼ 1 (1 of 1)

Last updated: Thu Jan 17 17:41:21 EST 2019

The figure below shows the Grid View ▦

Figure 3-6: Grid View



User/Device Status

Search for user or device

Adar (admin), Tania

Start Time	Duration	Media Type	State	On Demand	Details
3:53 PM	00:00:17	☎	RECORDING		⌕

Banks (x3056), Eric

Start Time Duration Media Type State On Demand Details

Barrett, Lorenzo

Start Time Duration Media Type State On Demand Details

Entry Phone

Start Time Duration Media Type State On Demand Details

Huff, Rosie

Start Time Duration Media Type State On Demand Details

Jenkins (TestCallCaller), Edgar

Start Time Duration Media Type State On Demand Details

Thomas (x3051), Anna

Start Time	Duration	Media Type	State	On Demand	Details
3:53 PM	00:00:18	☎	RECORDING		⌕

Warner(TestCallCallee), Barbara

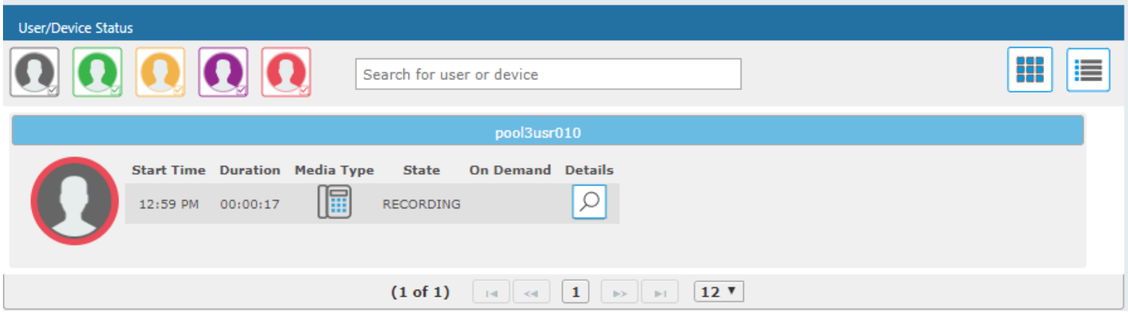
Start Time Duration Media Type State On Demand Details

(1 of 1) 1 12 ▼

Last updated: Mon Feb 11 15:54:14 EST 2019

The figure below shows a user status with an active call:

Figure 3-7: User/Device Status with an Active Call



User/Device Status

Search for user or device

pool3usr010

Start Time	Duration	Media Type	State	On Demand	Details
12:59 PM	00:00:17	☎	RECORDING		⌕

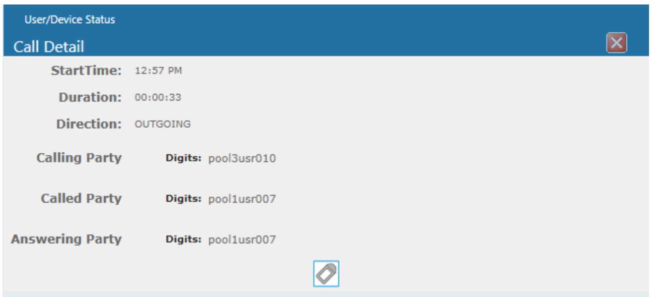
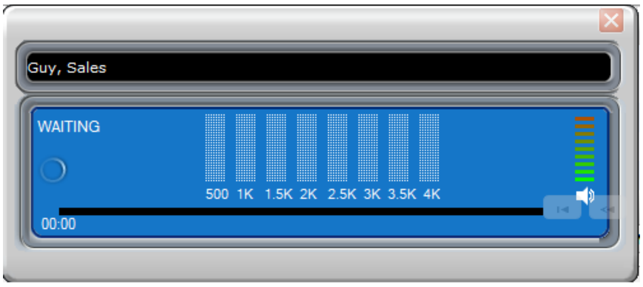
(1 of 1) 1 12 ▼

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	The duration of the call. Sortable by clicking the up/down arrows.

Field	Description		
Duration			
Call Direction	One of the following values: ■ **Incoming** ■ **Outgoing** ■ **Conference** Sortable by clicking the up/down arrows. Call Direction drop-down 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.	

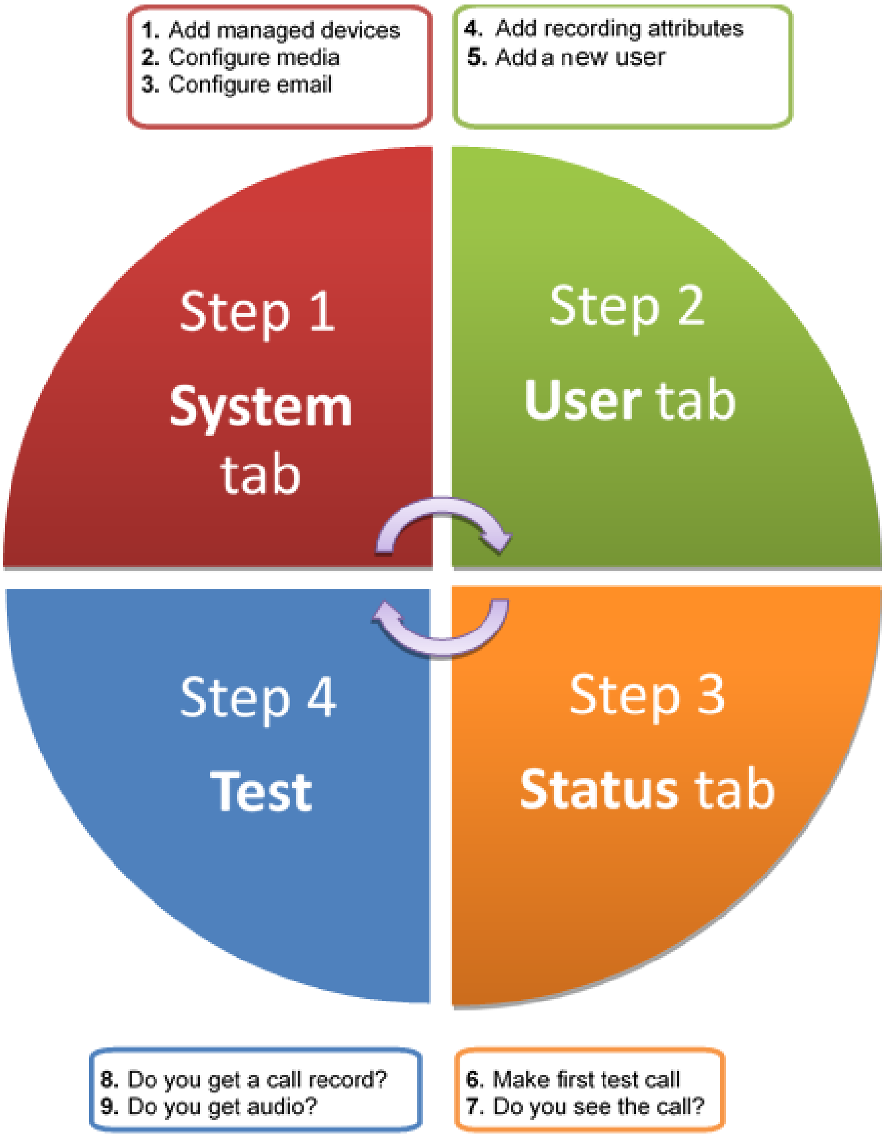
Field	Description		
		 User/Device Status Call Detail StartTime: 12:57 PM Duration: 00:00:33 Direction: OUTGOING Calling Party Digits: pool3usr010 Called Party Digits: pool1usr007 Answering Party Digits: pool1usr007	
Call Notes	🏷	Add a tag - live call or post call. Tags are defined by the system administrator and can be applied during a call or post call.	
Pause / Resume Recording	⏸ PAUSE	Select to pause the recording (for PCI compliance).	
	● REC	Select to Resume the recording (for PCI compliance).	
ROD / SOD	● REC	ROD (Record on Demand)	Click to start recording from the current point in the call. The audio file will contain audio from the trigger point on.
	💾	SOD (Save on Demand)	Click to save the recording of the complete call.
Live Monitor	LIVE	Users with 'Live Monitoring' privilege can listen to active calls by clicking the Live Monitor microphone button. The following popup player launches:  Guy, Sales WAITING 500 1K 1.5K 2K 2.5K 3K 3.5K 4K 00:00	
Page Navigation buttons	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.		

4 Performing Initial Configuration

The figure below shows the steps to take to perform initial SmartTAP 360° configuration (Step 1-Step 2) in order to record a call. Detailed instructions follow below it.

It's assumed SmartTAP 360° software components were installed on the servers necessary for your environment, and were configured based on the SmartTAP 360° Installation Guide.

Figure 4-1: Performing Initial Setup



➢ **To perform initial setup:**

1. Log in for the first time (see Chapter Logging In on page 13for more information)
2. Configure media (see Configuring Media on page 64 for more information).
3. Configure email (see Configuring Email Server Settings on page 62Configuring Email Server Settings on page 62 for more information).

4. Add a user attribute for recording purposes (see page Managing Users on page 101 for details).

5. Add a user (see under Managing Users on page 101Managing Users for more information).

6. Make sure the new user is assigned a recording profile (see under Managing Recording Profiles on page 112 for more information).

7. Make sure the user’s recording attribute field is populated (for more information, see Managing Recording Profiles on page 112).

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 Performing Initial Configuration on page 22). The objective is to validate the configuration and the recording functionality.

After making sure recording is functioning correctly, continue to Chapter Configuring Advanced Features on page 26 to set up advanced features such as LDAP and Single Sign-On.

➢ To test the initial configuration:

1. Navigate to the Status page (**Status** tab >**Status** folder > **User Status**).
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?

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 (**Status** tab > **Status** folder > **User Status**):
   - Click 🏠 on the upper banner

     -or-
   - Click the **Status** tab > **User Call Status**

■ The icon indicates that a recording is in progress.

Listening to a Recording and Viewing 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 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 ▶.
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.

6 Configuring Advanced Features

After performing initial setup and then testing it, n configure the advanced SmartTAP 360° features described in this section.

Viewing/Searching an Audit Trail

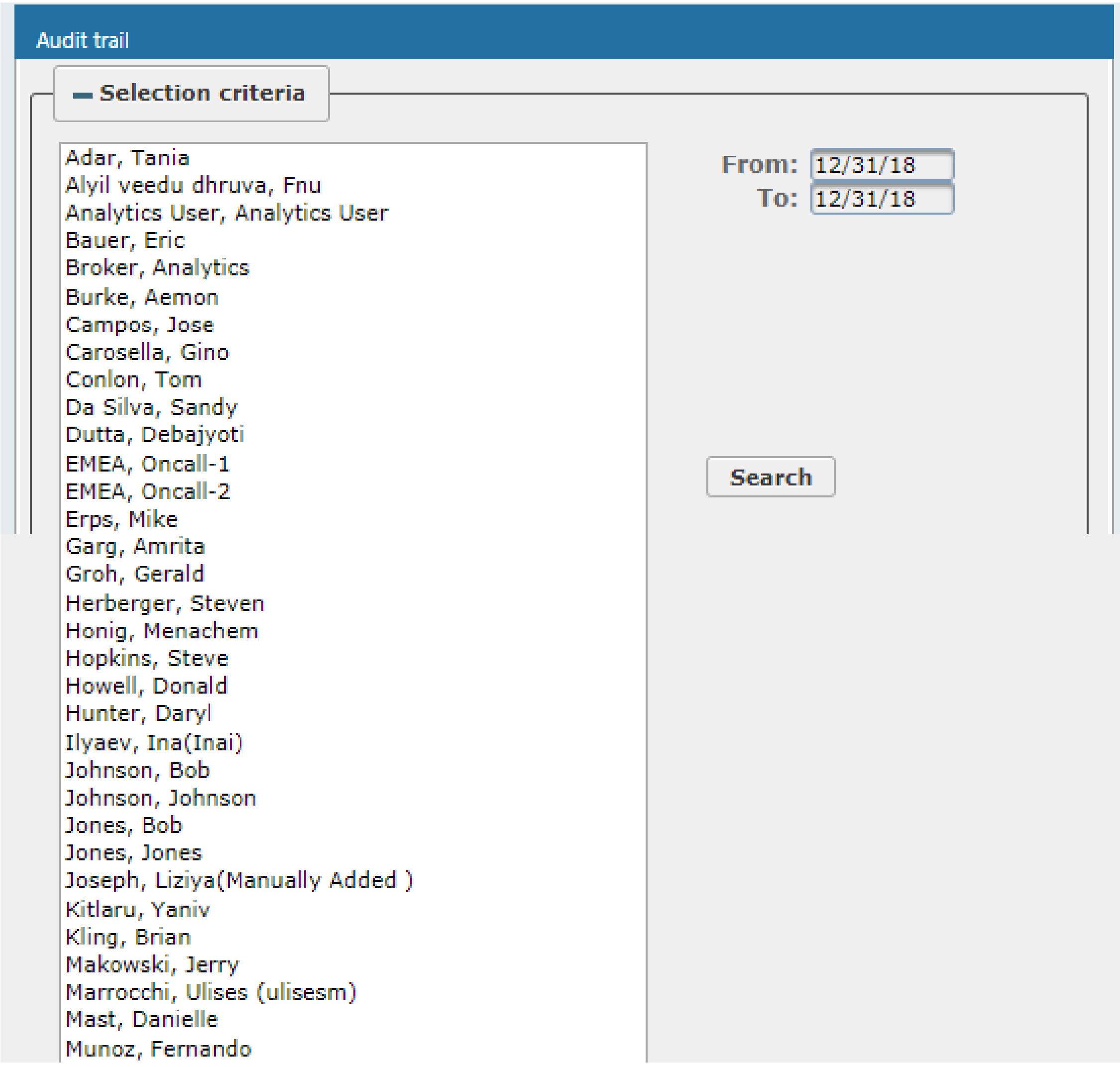
The Audit Trail feature allows the administrator to search the history of all user activity on SmartTAP 360°. The Audit Trail is searchable but cannot be edited or deleted. You can view / search the user changes made to the SmartTAP 360° database.

➢ To view / search user activities:

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

⚠ The System tab is only accessible to administrators assigned the Configure System option in their security profile.

Figure 6-1: Audit Trail



Audit trail

− Selection criteria

Adar, Tania
Alyil veedu dhruva, Fnu
Analytics User, Analytics User
Bauer, Eric
Broker, Analytics
Burke, Aemon
Campos, Jose
Carosella, Gino
Conlon, Tom
Da Silva, Sandy
Dutta, Debajyoti
EMEA, Oncall-1
EMEA, Oncall-2
Erps, Mike
Garg, Amrita
Groh, Gerald
Herberger, Steven
Honig, Menachem
Hopkins, Steve
Howell, Donald
Hunter, Daryl
Ilyaev, Ina(Inai)
Johnson, Bob
Johnson, Johnson
Jones, Bob
Jones, Jones
Joseph, Liziya(Manually Added)
Kitlaru, Yaniv
Kling, Brian
Makowski, Jerry
Marrocchi, Ulises (ulisesm)
Mast, Danielle
Munoz, Fernando

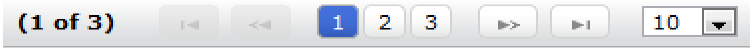
From: 12/31/18
To: 12/31/18

Search

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.

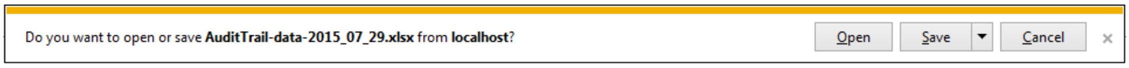
Field	Description
Search	Click to perform the search and display the results.
Name	Sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.
Action	Sorted ascending/descending by clicking header up/down arrows. Default is 'All Actions'. 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 the 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 drop-down list allows changing the number of entries that are displayed per page.	

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 > **Monitoring** Folder > **Audit Trail**).
2. Select the User or Users to view and date range.
3. Click Search to see the results.
4. Click the Excel icon.



Do you want to open or save **AuditTrail-data-2015_07_29.xlsx** from **localhost**?

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

Managing Licenses

This section describes how to manage the SmartTAP 360° licenses. This interface displays data on the purchased and loaded license items:

- Targeted user licenses
- Concurrent recording licenses

Targeted User Licenses

The targeted user licenses enable SmartTAP 360° 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.

- 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.

Concurrent Recording Licenses

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

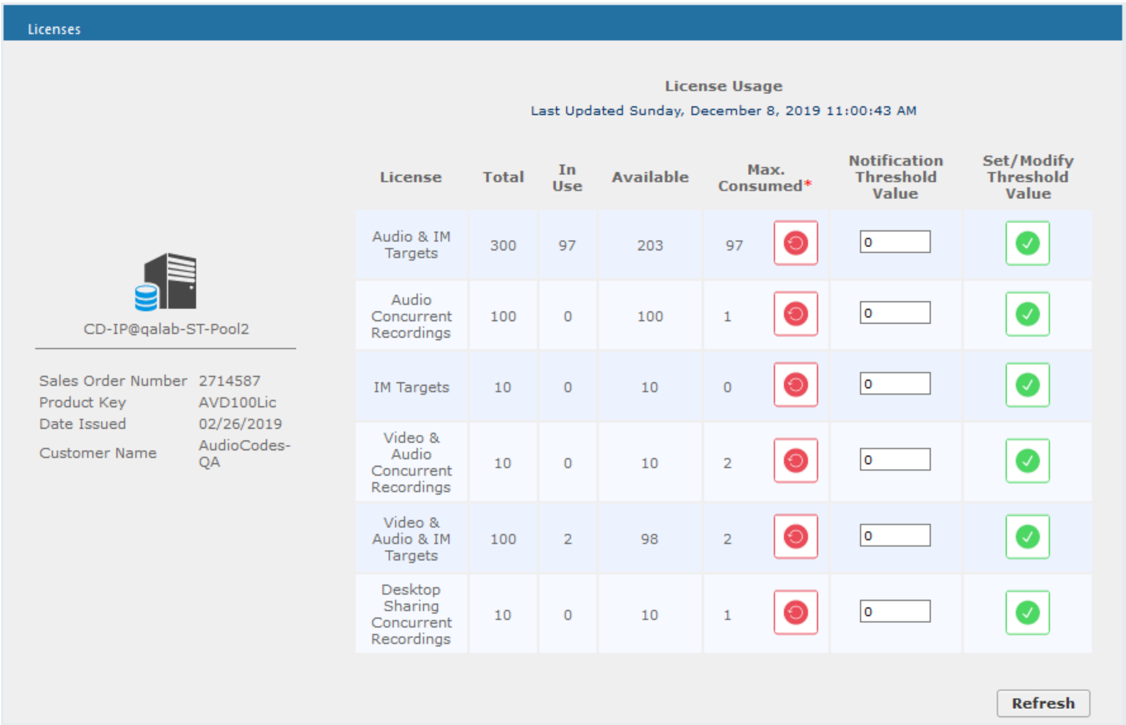
- **Audio Concurrent Recordings:** this license determines the maximum number of concurrent Audio recordings of users that are assigned to an Audio enabled recording profile (Video disabled) .
- **Video & Audio Concurrent Recordings**: this license determine the maximum number of concurrent Video and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

➢ To view Managed Licenses:

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

Figure 6-2: License Menu



Licenses

License Usage

Last Updated Sunday, December 8, 2019 11:00:43 AM

CD-IP@qalab-ST-Pool2

Sales Order Number	2714587
Product Key	AVD100Lic
Date Issued	02/26/2019
Customer Name	AudioCodes-QA

License	Total	In Use	Available	Max. Consumed*		Notification Threshold Value	Set/Modify Threshold Value
Audio & IM Targets	300	97	203	97	⟲	0	✓
Audio Concurrent Recordings	100	0	100	1	⟲	0	✓
IM Targets	10	0	10	0	⟲	0	✓
Video & Audio Concurrent Recordings	10	0	10	2	⟲	0	✓
Video & Audio & IM Targets	100	2	98	2	⟲	0	✓
Desktop Sharing Concurrent Recordings	10	0	10	1	⟲	0	✓

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.
- **Max Consumed:** The maximum number of concurrently used licenses to date. Each counter can be manually reset by selecting the reset counter button ⟲ adjacent to each license entry. The counter is reset after the Call Delivery server is restarted and the screen is refreshed.

> ⚠ Following reset, the value for "Max Consumed" is equal to the value for "In Use" for the selected entry.

- **The Notification Threshold Value:** this value is measured in terms of the number of licenses; zero implies that no notifications are sent. For example, if the Notification Threshold Value 3 is configured for the “Audio & IM Targets” item, 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 Alarms on page 36.
- **Set/Modify Threshold Value:** Set or modify the Threshold value by selecting the adjacent SUBMIT 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, Product Key, Date Issued and Customer Name.

Viewing Managed Devices

SmartTAP 360° 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 360° to record calls.

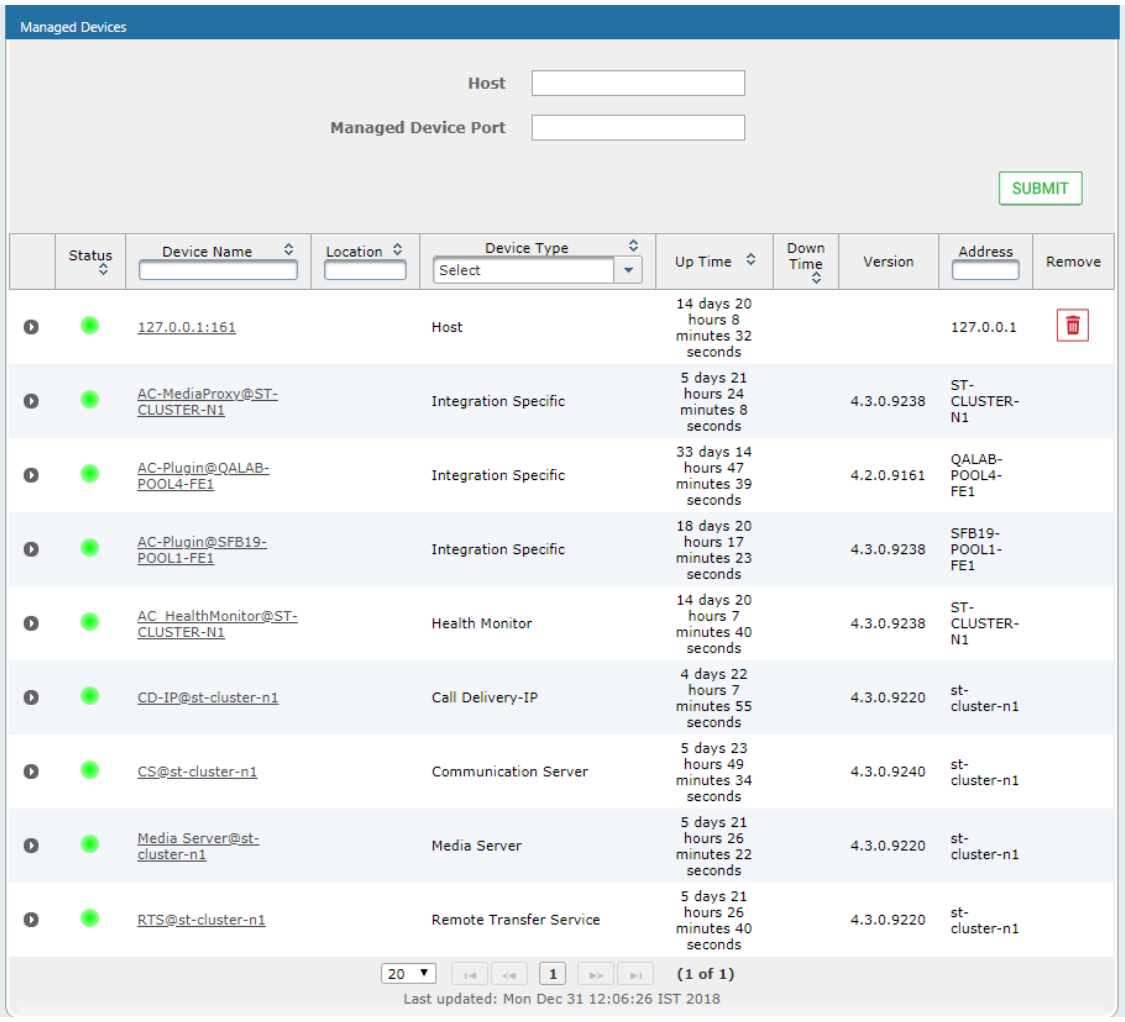
A managed device other than of type 'Host' will register automatically with the application server. Such devices update their status by sending periodic heartbeats to the application server. Devices also update their connection status information whenever the connection state changes. A device of type '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.

> ⚠ In a correctly setup deployment, all device types are added automatically, except for devices of type “Host”. See Adding a Device Manually to the Application Server on page 35 Adding a Device Manually to the Application Server on page 35 for the procedure to add Host devices.

➢ **To view managed devices:**

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

Figure 6-3: Managed Devices



Managed Devices

Host

Managed Device Port

SUBMIT

	Status	Device Name	Location	Device Type	Up Time	Down Time	Version	Address	Remove
				Select					
▶	●	127.0.0.1:161		Host	14 days 20 hours 8 minutes 32 seconds			127.0.0.1	🗑
▶	●	AC-MediaProxy@ST-CLUSTER-N1		Integration Specific	5 days 21 hours 24 minutes 8 seconds		4.3.0.9238	ST-CLUSTER-N1	
▶	●	AC-Plugin@QALAB-POOL4-FE1		Integration Specific	33 days 14 hours 47 minutes 39 seconds		4.2.0.9161	QALAB-POOL4-FE1	
▶	●	AC-Plugin@SFB19-POOL1-FE1		Integration Specific	18 days 20 hours 17 minutes 23 seconds		4.3.0.9238	SFB19-POOL1-FE1	
▶	●	AC_HealthMonitor@ST-CLUSTER-N1		Health Monitor	14 days 20 hours 7 minutes 40 seconds		4.3.0.9238	ST-CLUSTER-N1	
▶	●	CD-IP@st-cluster-n1		Call Delivery-IP	4 days 22 hours 7 minutes 55 seconds		4.3.0.9220	st-cluster-n1	
▶	●	CS@st-cluster-n1		Communication Server	5 days 23 hours 49 minutes 34 seconds		4.3.0.9240	st-cluster-n1	
▶	●	Media Server@st-cluster-n1		Media Server	5 days 21 hours 26 minutes 22 seconds		4.3.0.9220	st-cluster-n1	
▶	●	RTS@st-cluster-n1		Remote Transfer Service	5 days 21 hours 26 minutes 40 seconds		4.3.0.9220	st-cluster-n1	

20 ▾ 1 (1 of 1)

Last updated: Mon Dec 31 12:06:26 IST 2018

- 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.

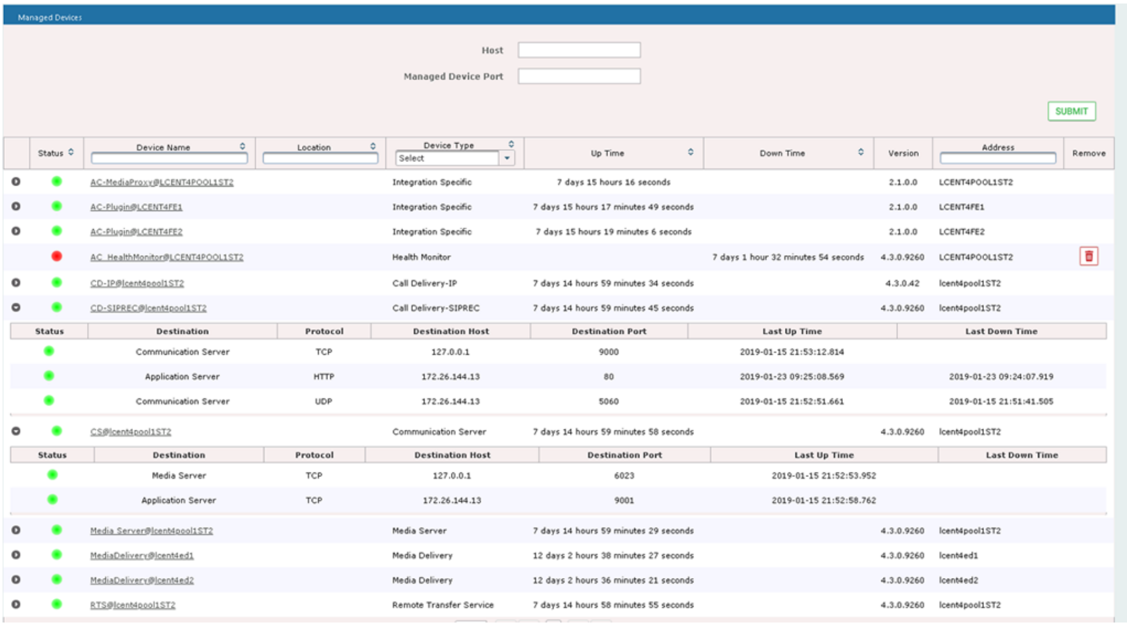
Field	Description	
Status	Indicates the status of the managed device.	
	🟢	Device status is UP: the device has registered and is sending heartbeats periodically at regular 30 second intervals.
	⚪	Device status is UNKNOWN: the device has registered but has not yet send any heartbeat message.
	🟡	Device 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.
	🟠	One of the connected devices is DOWN.
	🔴	Device status is DOWN: the device stops sending heartbeat messages.
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 360°, 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.	

Field	Description
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.

Inter-Components Communication

SmartTAP 360° inter-components communication status helps to quickly detect connection issues and to take the appropriate actions. Each managed device reports the status of its its connections with other components in the system.

Figure 6-4: Inter-Component Communications



Managed Devices

Host

Managed Device Port

SUBMIT

Status	Device Name	Location	Device Type Select	Up Time	Down Time	Version	Address	Remove
●	AC-MediaProxy@LCENT4POOL1ST2		Integration Specific	7 days 15 hours 16 seconds		2.1.0.0	LCENT4POOL1ST2	
●	AC-Plugin@LCENT4FE1		Integration Specific	7 days 15 hours 17 minutes 49 seconds		2.1.0.0	LCENT4FE1	
●	AC-Plugin@LCENT4FE2		Integration Specific	7 days 15 hours 19 minutes 6 seconds		2.1.0.0	LCENT4FE2	
●	AC_HealthMonitor@LCENT4POOL1ST2		Health Monitor		7 days 1 hour 32 minutes 54 seconds	4.3.0.9260	LCENT4POOL1ST2	🗑
●	CD-IP@lcent4pool1ST2		Call Delivery-IP	7 days 14 hours 59 minutes 34 seconds		4.3.0.42	lcent4pool1ST2	
●	CD-SIPREC@lcent4pool1ST2		Call Delivery-SIPREC	7 days 14 hours 59 minutes 45 seconds		4.3.0.9260	lcent4pool1ST2	

Status	Destination	Protocol	Destination Host	Destination Port	Last Up Time	Last Down Time
●	Communication Server	TCP	127.0.0.1	9000	2019-01-15 21:53:12.814	
●	Application Server	HTTP	172.26.144.13	80	2019-01-23 09:25:08.569	2019-01-23 09:24:07.919
●	Communication Server	UDP	172.26.144.13	5060	2019-01-15 21:52:51.661	2019-01-15 21:51:41.505

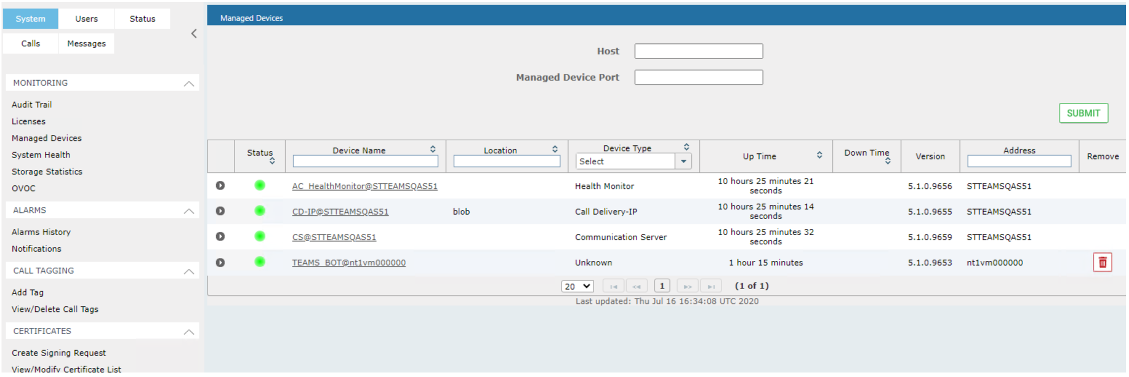
Status	Device Name	Location	Device Type	Up Time	Down Time	Version	Address	Remove
●	CS@lcent4pool1ST2		Communication Server	7 days 14 hours 59 minutes 58 seconds		4.3.0.9260	lcent4pool1ST2	

Status	Destination	Protocol	Destination Host	Destination Port	Last Up Time	Last Down Time
●	Media Server	TCP	127.0.0.1	6023	2019-01-15 21:52:53.952	
●	Application Server	TCP	172.26.144.13	9001	2019-01-15 21:52:58.762	

Status	Device Name	Location	Device Type	Up Time	Down Time	Version	Address	Remove
●	Media Server@lcent4pool1ST2		Media Server	7 days 14 hours 59 minutes 29 seconds		4.3.0.9260	lcent4pool1ST2	
●	MediaDelivery@lcent4ed1		Media Delivery	12 days 2 hours 38 minutes 27 seconds		4.3.0.9260	lcent4ed1	
●	MediaDelivery@lcent4ed2		Media Delivery	12 days 2 hours 36 minutes 21 seconds		4.3.0.9260	lcent4ed2	
●	RTS@lcent4pool1ST2		Remote Transfer Service	7 days 14 hours 58 minutes 55 seconds		4.3.0.9260	lcent4pool1ST2	

The following screen shows example components in a Microsoft Teams deployment.

Figure 6-5: Microsoft Teams SmartTAP 360° BOT Deployment



Host

Managed Device Port

	Status	Device Name	Location	Device Type	Up Time	Down Time	Version	Address	Remove
				Select					
▶	●	AC_HealthMonitor@STTEAMSQAS51		Health Monitor	10 hours 25 minutes 21 seconds		5.1.0.9656	STTEAMSQAS51	
▶	●	CD-IP@STTEAMSQAS51	blob	Call Delivery-IP	10 hours 25 minutes 14 seconds		5.1.0.9655	STTEAMSQAS51	
▶	●	CS@STTEAMSQAS51		Communication Server	10 hours 25 minutes 32 seconds		5.1.0.9659	STTEAMSQAS51	
▶	●	TEAMS_BOT@nt1vm000000		Unknown	1 hour 15 minutes		5.1.0.9653	nt1vm000000	🗑

20 1 (1 of 1)

Last updated: Thu Jul 16 16:34:08 UTC 2020

Adding a Device Manually to the Application Server

The Application Server's Web service manages all devices (software elements). It must be configured with one of the following software elements performing specialized tasks in the SmartTAP 360° environment:

- 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.

> ⚠ As mentioned in Viewing Managed Devices on page 31 , 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.

> ⚠ For a standalone SmartTAP 360° recorder, all managed devices reside on 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.

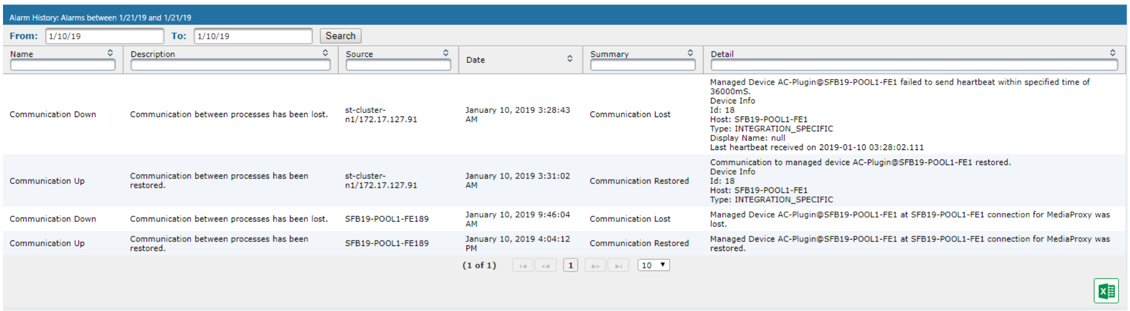
Alarms

This section describes the Alarms History and Alarm Notification screens.

Alarm History

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

Figure 6-6: Alarm History



Alarm History: Alarms between 1/21/19 and 1/21/19

From: 1/10/19 To: 1/10/19

Name	Description	Source	Date	Summary	Detail
Communication Down	Communication between processes has been lost.	st-cluster-n1/172.17.127.91	January 10, 2019 3:28:43 AM	Communication Lost	Managed Device AC-Plugin@SFB19-POOL1-FE1 failed to send heartbeat within specified time of 36000mS. Device Info Id: 18 Host: SFB19-POOL1-FE1 Type: INTEGRATION_SPECIFIC Display Name: null Last heartbeat received on 2019-01-10 03:28:02.111
Communication Up	Communication between processes has been restored.	st-cluster-n1/172.17.127.91	January 10, 2019 3:31:02 AM	Communication Restored	Communication to managed device AC-Plugin@SFB19-POOL1-FE1 restored. Device Info Id: 18 Host: SFB19-POOL1-FE1 Type: INTEGRATION_SPECIFIC
Communication Down	Communication between processes has been lost.	SFB19-POOL1-FE189	January 10, 2019 9:46:04 AM	Communication Lost	Managed Device AC-Plugin@SFB19-POOL1-FE1 at SFB19-POOL1-FE1 connection for MediaProxy was lost.
Communication Up	Communication between processes has been restored.	SFB19-POOL1-FE189	January 10, 2019 4:04:12 PM	Communication Restored	Managed Device AC-Plugin@SFB19-POOL1-FE1 at SFB19-POOL1-FE1 connection for MediaProxy was restored.

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

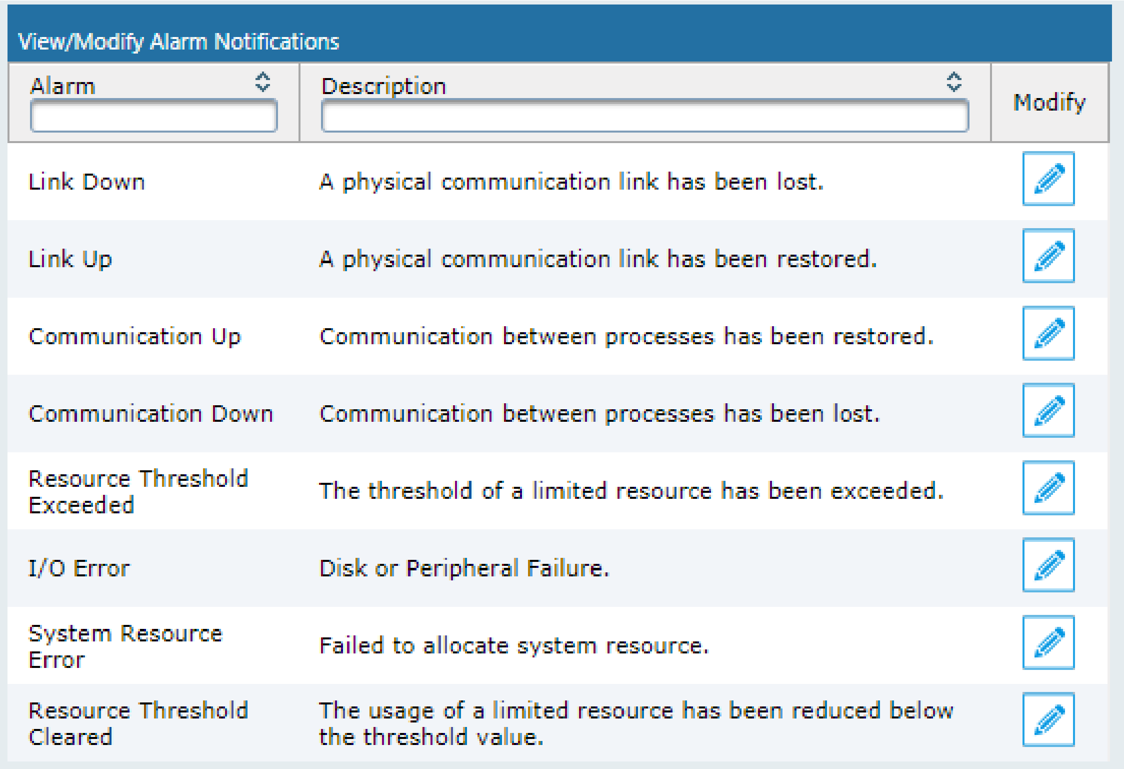
Alarm Notifications

SmartTAP 360° 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 > **Alarms** Folder > **Notifications**).

Figure 6-7: View/Modify Alarm Modifications



View/Modify Alarm Notifications

Alarm	Description	Modify
Link Down	A physical communication link has been lost.	✎
Link Up	A physical communication link has been restored.	✎
Communication Up	Communication between processes has been restored.	✎
Communication Down	Communication between processes has been lost.	✎
Resource Threshold Exceeded	The threshold of a limited resource has been exceeded.	✎
I/O Error	Disk or Peripheral Failure.	✎
System Resource Error	Failed to allocate system resource.	✎
Resource Threshold Cleared	The usage of a limited resource has been reduced below the threshold value.	✎

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'.

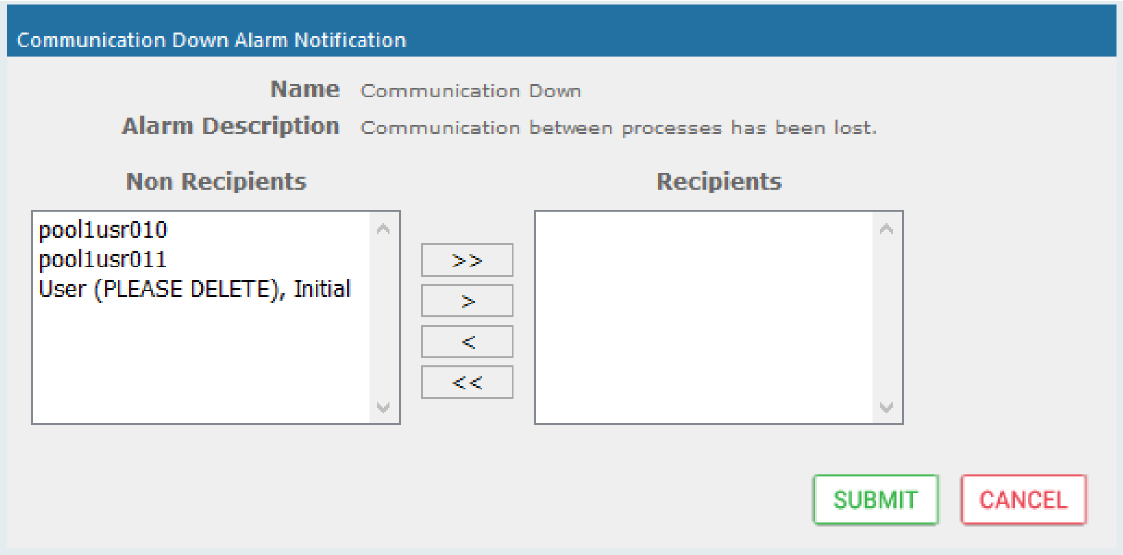
4. Use the assignment keys to assign recipients of the alarm notifications:

   - 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.

5. Click SUBMIT.

Figure 6-8: Link Up Alarm Notification



Name: Communication Down

Alarm Description: Communication between processes has been lost.

Non Recipients:
pool1usr010
pool1usr011
User (PLEASE DELETE), Initial

6. 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.
✎	Click to modify the list of users receiving this alarm notification.

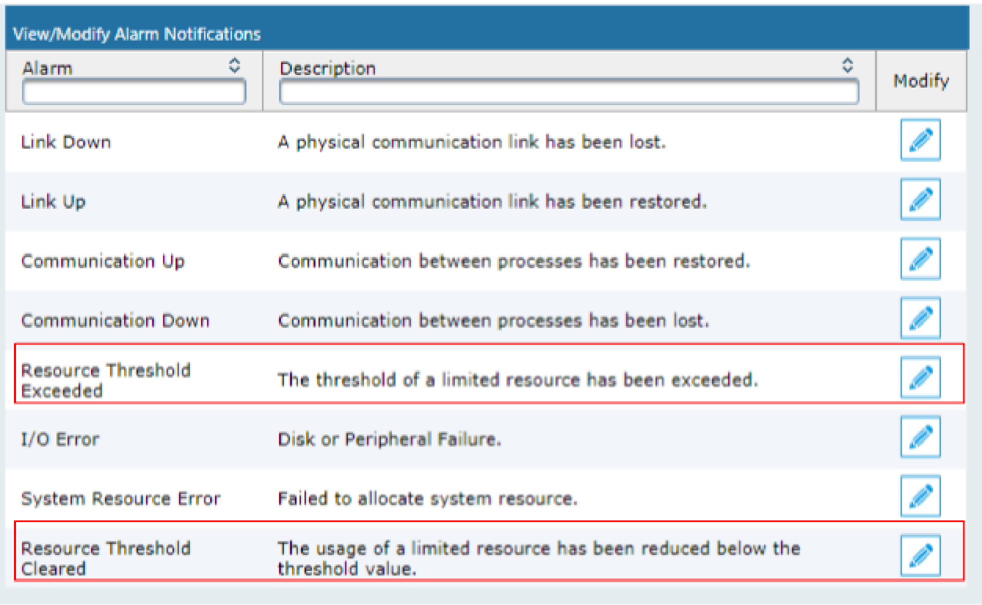
Table 6-5: List of Alarms and Possible Causes with Recommended Remedial Action

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 360° software elements has been lost	■ Run system_profile.exe (..\AUDIOCODES\Tools) ■ Contact AudioCodes Support with the notification received. ✔ If the notification is the result of a failure of the Application Server polling the

Alarm	Explanation	Remedial Action
		managed devices, it will indicate the address and port of the managed device to which it was trying to communicate. ✔ If it is from a trap from another device, the trap OID will indicate between which devices the specific failure occured.
Resource Threshold Exceeded	The peak number of concurrent calls has exceeded the number of available licenses.	SmartTAP 360° 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 Managing Licenses on page 29 Managing Licenses on page 29).
	The media storage location threshold has been reached.	■ Check the resource threshold setting. It's possible that sufficient storage still remains and that the threshold needs to be adjusted. ■ For additional media files (recordings) add additional storage capacity to the file server. This file server is external to SmartTAP 360°.
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 360°. ■ 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 6-9: View/Modify Alarm Notifications



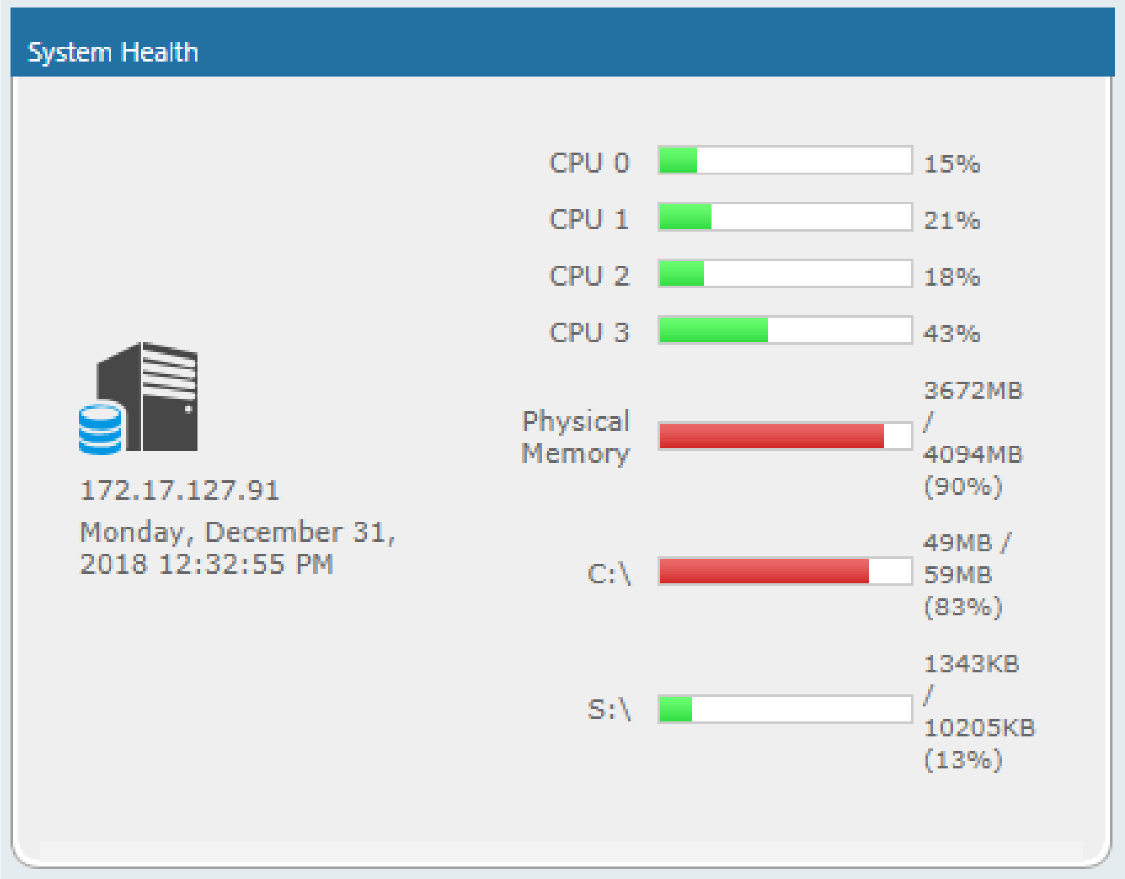
View/Modify Alarm Notifications

Alarm	Description	Modify
Link Down	A physical communication link has been lost.	🖉
Link Up	A physical communication link has been restored.	🖉
Communication Up	Communication between processes has been restored.	🖉
Communication Down	Communication between processes has been lost.	🖉
Resource Threshold Exceeded	The threshold of a limited resource has been exceeded.	🖉
I/O Error	Disk or Peripheral Failure.	🖉
System Resource Error	Failed to allocate system resource.	🖉
Resource Threshold Cleared	The usage of a limited resource has been reduced below the threshold value.	🖉

Monitoring System Health

The health of the SmartTAP 360° 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 6-10: System Health



System Health

172.17.127.91

Monday, December 31, 2018 12:32:55 PM

CPU 0 15%

CPU 1 21%

CPU 2 18%

CPU 3 43%

Physical Memory 3672MB / 4094MB (90%)

C:\ 49MB / 59MB (83%)

S:\ 1343KB / 10205KB (13%)

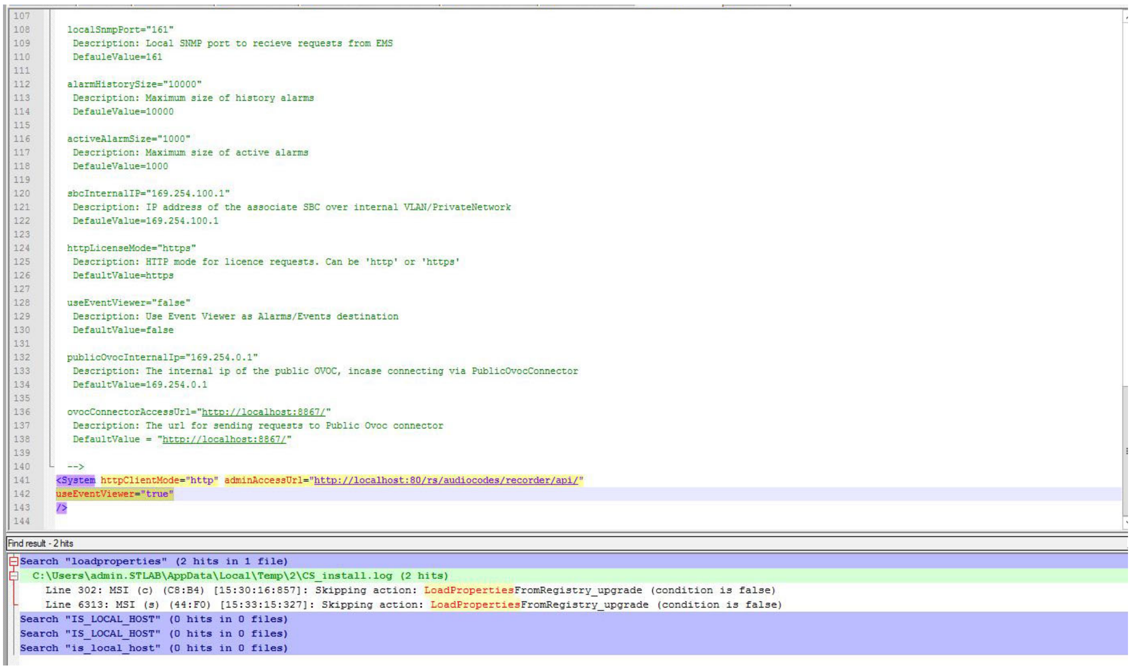
Windows Event Log

By default alarms and events raised on SmartTAP 360° are sent to the OVOC server as SNMP traps (see Configuring OVOC Connection on page 98) and are not sent by default to the Windows Event Log.

➢ **To enable sending SmartTAP 360° alarms and events to the Windows Event Log:**

1. Using a text editor, open the MainAgent configuration file "System.config" from directory ...MainAgent\Config.
2. Search for string "useEventViewer="false" and change to "useEventViewer="true".
3. Save changes and exit.
4. Restart the **OVOC Main Agent** service.

Figure 6-11: useEventViewer



```
   localSnmpPort="161"
    Description: Local SNMP port to recieve requests from EMS
    DefauleValue=161

   alarmHistorySize="10000"
    Description: Maximum size of history alarms
    DefauleValue=10000

   activeAlarmSize="1000"
    Description: Maximum size of active alarms
    DefauleValue=1000

   sbcInternalIP="169.254.100.1"
    Description: IP address of the associate SBC over internal VLAN/PrivateNetwork
    DefauleValue=169.254.100.1

   httpLicenseMode="https"
    Description: HTTP mode for licence requests. Can be 'http' or 'https'
    DefaultValue=https

   useEventViewer="false"
    Description: Use Event Viewer as Alarms/Events destination
    DefaultValue=false

   publicOvocInternalIp="169.254.0.1"
    Description: The internal ip of the public OVOC, incase connecting via PublicOvocConnector
    DefaultValue=169.254.0.1

   ovocConnectorAccessUrl="http://localhost:8867/"
    Description: The url for sending requests to Public Ovoc connector
    DefaultValue = "http://localhost:8867/"

   -->
 <System httpClientMode="http" adminAccessUrl="http://localhost:80/rs/audiocodes/recorder/api/"
 useEventViewer="true"
 />
```

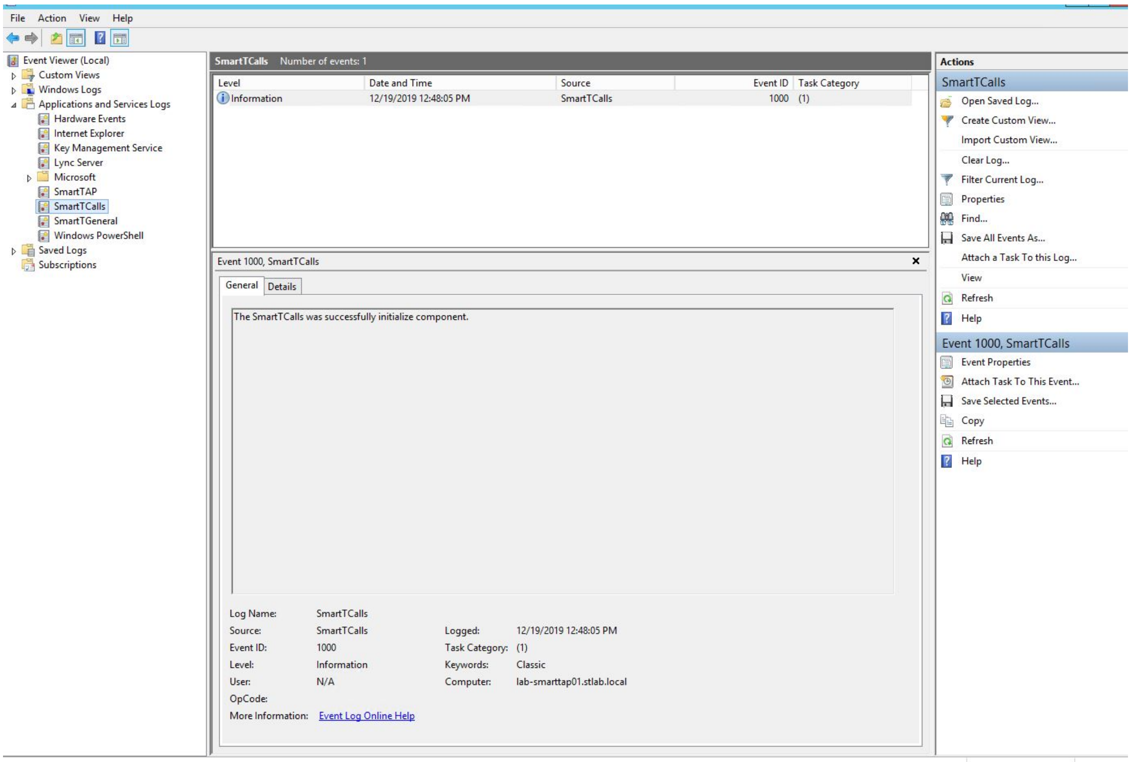
Find result - 2 hits

```
Search "loadproperties" (2 hits in 1 file)
  C:\Users\admin.STLAB\AppData\Local\Temp\2\CS_install.log (2 hits)
    Line 302: MSI (c) (C8:B4) [15:30:16:857]: Skipping action: LoadPropertiesFromRegistry_upgrade (condition is false)
    Line 6313: MSI (s) (44:F0) [15:33:15:327]: Skipping action: LoadPropertiesFromRegistry_upgrade (condition is false)
Search "IS_LOCAL_HOST" (0 hits in 0 files)
Search "IS_LOCAL_HOST" (0 hits in 0 files)
Search "is_local_host" (0 hits in 0 files)
```

When the Alarm Notification is written to the Windows Event Log, the Application Server creates two types of log files under “Applications and Services Logs” category in the Windows Event Log:

- **SmartTAPCalls**: this log includes all alarms and events related to call recording that were logged while running according to the logging configuration. The source attribute of these alarms is “SmartTCalls” and Event ID=<EventID> <Task Category> where 1-Alarm and 2-Event.
- **SmartTGeneral**: this log includes all otheralarm and events that were logged while running according to the logging configuration. The source attribute of these alarms is “SmartTGeneral” and Event ID=<EventID> <Task Category> where 1-Alarm and 2-Event .

Figure 6-12: Event Viewer SmartTCalls



SmartTCalls Number of events: 1

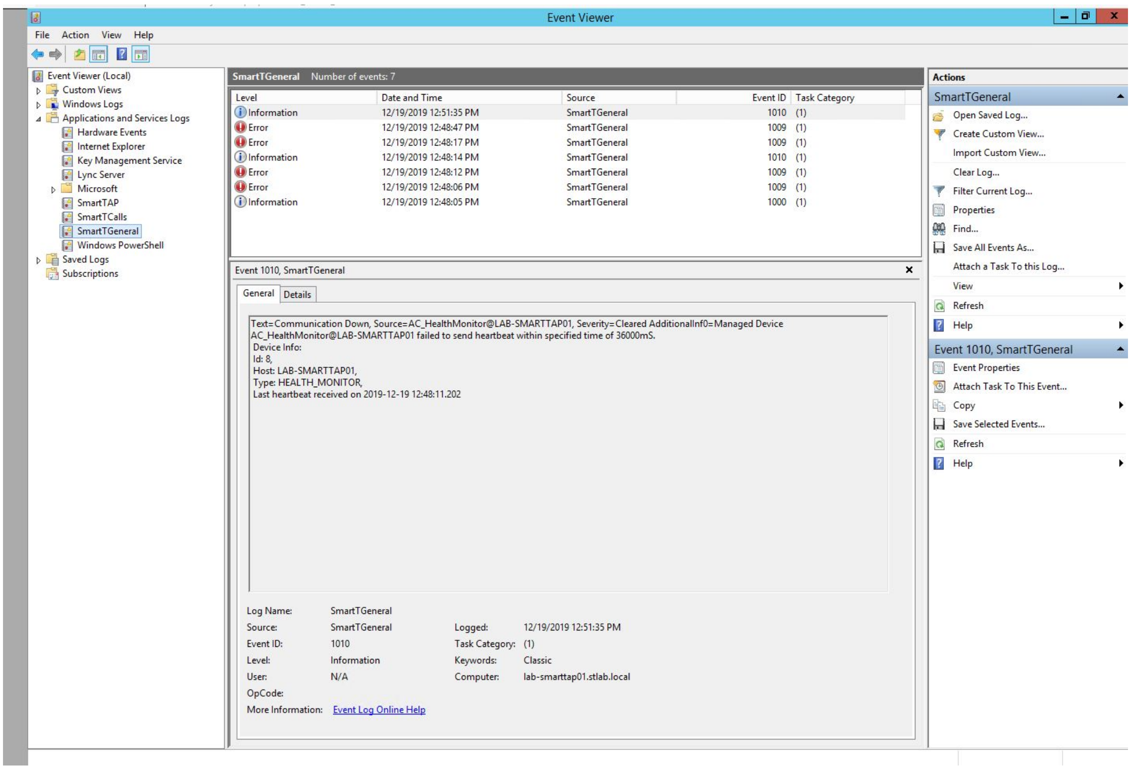
Level	Date and Time	Source	Event ID	Task Category
Information	12/19/2019 12:48:05 PM	SmartTCalls	1000	(1)

Event 1000, SmartTCalls

```
The SmartTCalls was successfully initialize component.
```

Log Name: SmartTCalls
Source: SmartTCalls Logged: 12/19/2019 12:48:05 PM
Event ID: 1000 Task Category: (1)
Level: Information Keywords: Classic
User: N/A Computer: lab-smarttap01.stlab.local
OpCode:
More Information: Event Log Online Help

Figure 6-13: Event Viewer SmartTGeneral



SmartTGeneral Number of events: 7

Level	Date and Time	Source	Event ID	Task Category
Information	12/19/2019 12:51:35 PM	SmartTGeneral	1010	(1)
Error	12/19/2019 12:48:47 PM	SmartTGeneral	1009	(1)
Error	12/19/2019 12:48:17 PM	SmartTGeneral	1009	(1)
Information	12/19/2019 12:48:14 PM	SmartTGeneral	1010	(1)
Error	12/19/2019 12:48:12 PM	SmartTGeneral	1009	(1)
Error	12/19/2019 12:48:06 PM	SmartTGeneral	1009	(1)
Information	12/19/2019 12:48:05 PM	SmartTGeneral	1000	(1)

Event 1010, SmartTGeneral

```
Text=Communication Down, Source=AC_HealthMonitor@LAB-SMARTTAP01, Severity=Cleared AdditionalInf0=Managed Device
AC_HealthMonitor@LAB-SMARTTAP01 failed to send heartbeat within specified time of 36000mS.
 Device Info:
 Id: 8,
 Host: LAB-SMARTTAP01,
 Type: HEALTH_MONITOR,
 Last heartbeat received on 2019-12-19 12:48:11.202
```

Log Name: SmartTGeneral
Source: SmartTGeneral Logged: 12/19/2019 12:51:35 PM
Event ID: 1010 Task Category: (1)
Level: Information Keywords: Classic
User: N/A Computer: lab-smarttap01.stlab.local
OpCode:
More Information: Event Log Online Help

SCOM Integration

The SmartTAP 360° 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 360°, the monitored events source should be configured to "SmartTAP 360°" with Event ID 4096.

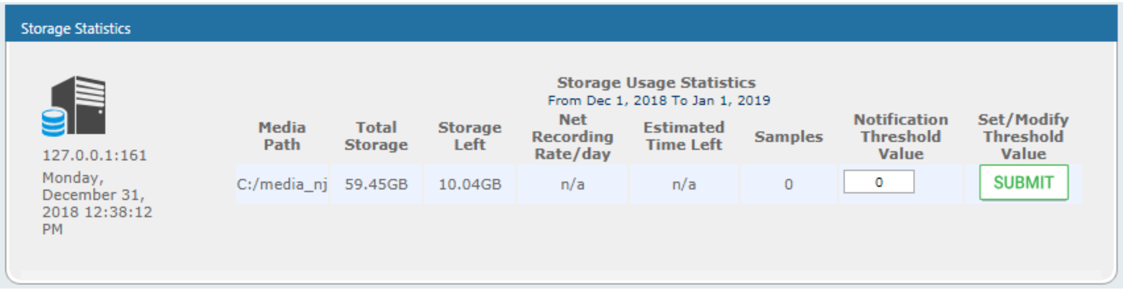
For more information, see the following link: Monitor Event Log

Monitoring Storage Statistics

The SmartTAP 360° 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 not only takes account of size and rate of the new recordings, but also the size and rate for which older recordings (that exceeded 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.

⚠ This functionality is not supported for all types of Azure storage.

Figure 6-14: Storage Statistics Screen



Storage Statistics

127.0.0.1:161

Monday, December 31, 2018 12:38:12 PM

Storage Usage Statistics
From Dec 1, 2018 To Jan 1, 2019

Media Path	Total Storage	Storage Left	Net Recording Rate/day	Estimated Time Left	Samples	Notification Threshold Value	Set/Modify Threshold Value
C:/media_nj	59.45GB	10.04GB	n/a	n/a	0	0	SUBMIT

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.

Field	Description
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 > **Monitoring** 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 ✎ 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.

Using Call Tagging

Call Tagging can be implemented by either the network administrator defining 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. Call Tagging provides the following 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.
SUBMIT	Applies changes.
CANCEL	Cancels changes.

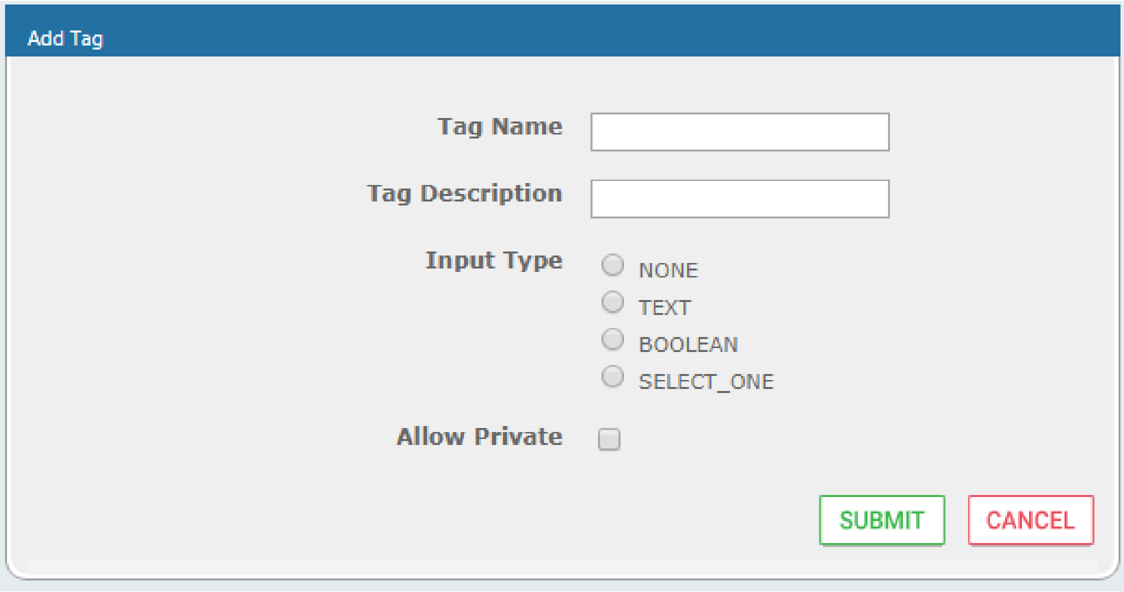
Adding a Call Tag

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 6-15: Add Call Tag Screen



Add Tag

Tag Name

Tag Description

Input Type

○ NONE

○ TEXT

○ BOOLEAN

○ SELECT_ONE

Allow Private □

Table 6-8: Call Tagging Fields

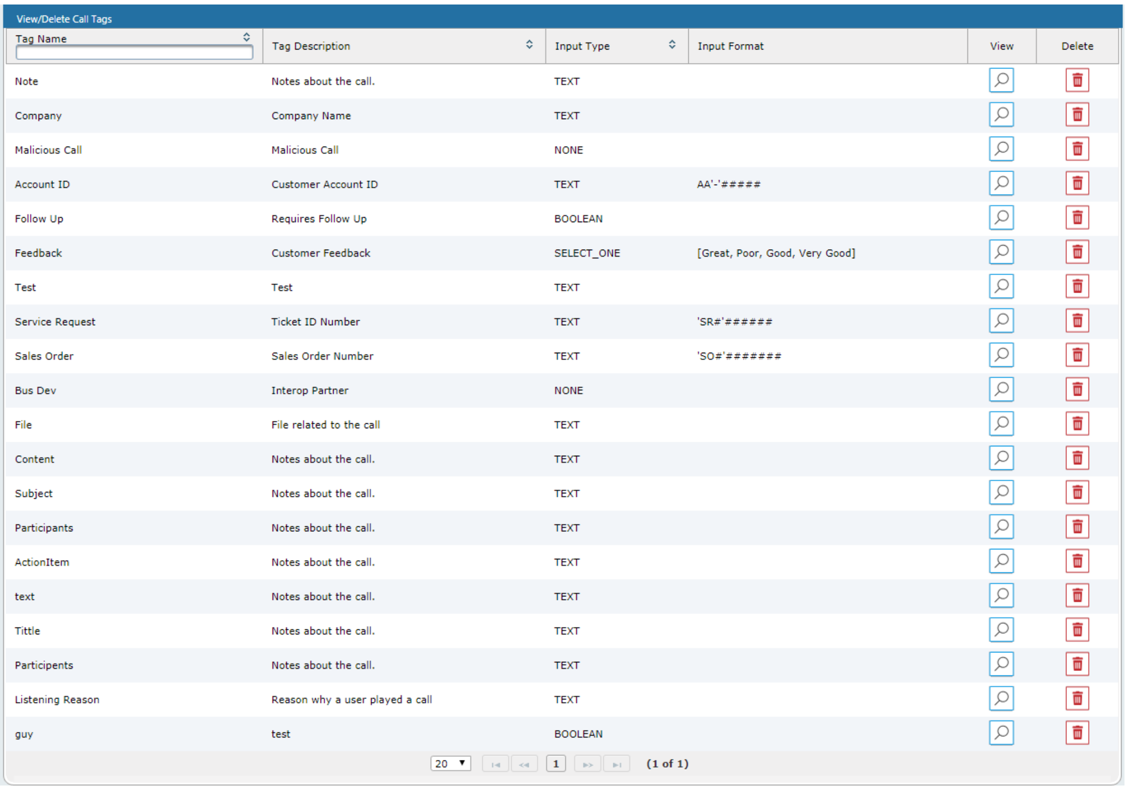
Field	Description
Tag Name	Administrator-defined Tag name. Enter the tag name to the filter list.
Tag Description	Administrator-defined description of the purpose of the tag, to expedite management efficiency. Easily sorts column A-Z or Z-A.
Input Type	Tag Type: ■ **None** (Tag requires no user input) ■ **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

Field	Description
	accept user inputs like Sales-1234567QA OR Sales-9876543P2, etc.
🔍	Click to view tag details.
🗑	Click to delete tag.
SUBMIT	Apply changes.
CANCEL	Cancel changes.

Viewing / Deleting a Call Tag

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

Figure 6-16: 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	[Great, Poor, Good, Very Good]	🔍	🗑
Test	Test	TEXT		🔍	🗑
Service Request	Ticket ID Number	TEXT	'SR#'######	🔍	🗑
Sales Order	Sales Order Number	TEXT	'SO#'#######	🔍	🗑
Bus Dev	Interop Partner	NONE		🔍	🗑
File	File related to the call	TEXT		🔍	🗑
Content	Notes about the call.	TEXT		🔍	🗑
Subject	Notes about the call.	TEXT		🔍	🗑
Participants	Notes about the call.	TEXT		🔍	🗑
ActionItem	Notes about the call.	TEXT		🔍	🗑
text	Notes about the call.	TEXT		🔍	🗑
Tittle	Notes about the call.	TEXT		🔍	🗑
Participents	Notes about the call.	TEXT		🔍	🗑
Listening Reason	Reason why a user played a call	TEXT		🔍	🗑
guy	test	BOOLEAN		🔍	🗑

Assigning Values to a Call Tag and Applying to Call

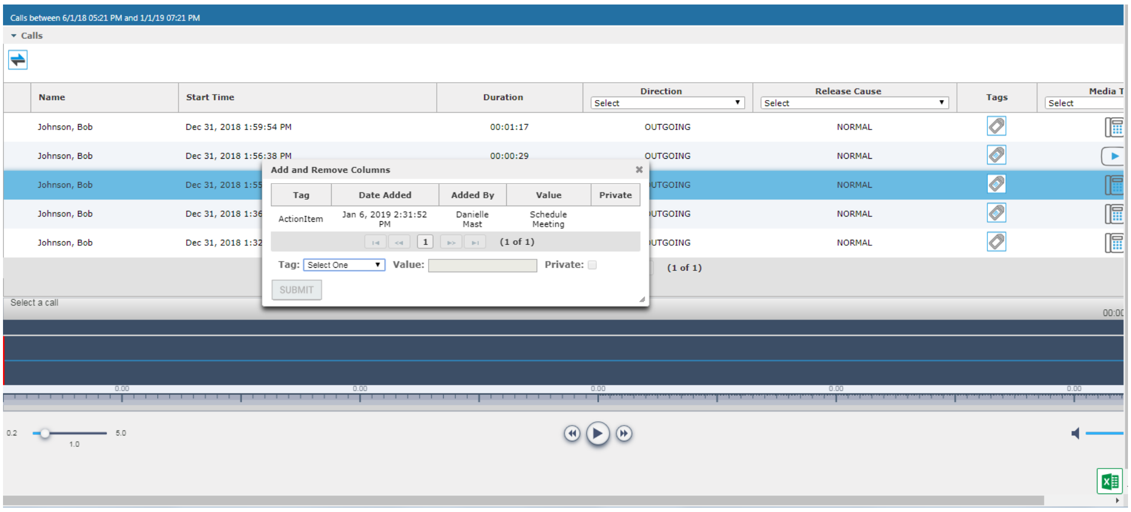
This section describes how to apply a call tag to a call.

➢ To apply a call tag:

1. Search for call records (as described in Searching for Calls on page 135)

2. Select the call record to tag and ensure that the Tags column is displayed.
3. Double-click the Tags icon in the call record.
4. In the Tag field, select the type of tag that you wish to add and enter the desired value in the Value field.
5. Select the Private check box to list a personal reminder (only visible to the person defining the tag).
6. In the Value field, enter the text note that you wish to assign to the tag. In the example below “Schedule Meeting” (see highlighted in the figure below).
7. Click SUBMIT.

Figure 6-17: Assigning a Call Tag



Calls between 6/1/18 05:21 PM and 1/1/19 07:21 PM

Calls

Name	Start Time	Duration	Direction	Release Cause	Tags	Media T
			Select	Select		Select
Johnson, Bob	Dec 31, 2018 1:59:54 PM	00:01:17	OUTGOING	NORMAL		
Johnson, Bob	Dec 31, 2018 1:56:38 PM	00:00:29	OUTGOING	NORMAL		
Johnson, Bob	Dec 31, 2018 1:55		UTGOING	NORMAL		
Johnson, Bob	Dec 31, 2018 1:36		UTGOING	NORMAL		
Johnson, Bob	Dec 31, 2018 1:32		UTGOING	NORMAL		

(1 of 1)

Select a call

Add and Remove Columns

Tag	Date Added	Added By	Value	Private
ActionItem	Jan 6, 2019 2:31:52 PM	Danielle Mast	Schedule Meeting	

(1 of 1)

Tag: Select One Value: Private: □

SUBMIT

Generating and Loading HTTPS Certificates

SmartTAP 360° 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 360° server
- Digitally signing audio files

SmartTAP 360° supports HTTPS/TLS 1.2.

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 are not members of the forest where Microsoft Enterprise CA is installed, and house SmartTAP 360° components or used to manage SmartTAP 360° 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 and intermediate certificates should be imported to certificate local store (Root certificate to 'Trusted Root Certificates', Intermediate certificate to 'Intermediate certificates') on all servers where SmartTAP 360° components reside, and all computers used to manage SmartTAP 360° via its web interface.

Step 1: Generate Certificate Signing Request (CSR)

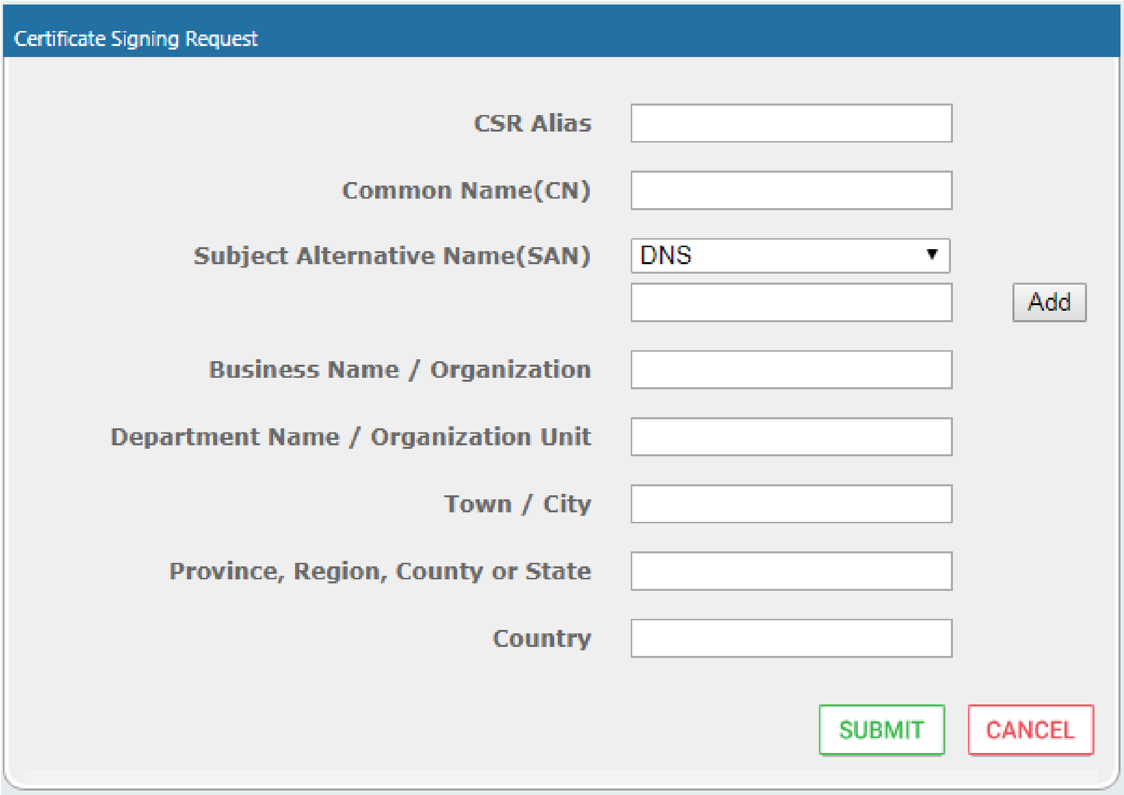
To obtain a certificate, first generate a CSR (Certificate Signing Request) from the SmartTAP 360° server. A CSR is an encoded file that provides you with a standardized way to send the necessary details to a trusted authority in order to have the certificate created. When you generate a CSR, the software prompts for the following information - common name (e.g., www.example.com), organization name, location (country, state/province, city/town).

- 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 360° 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 6-18: Certificate Signing Request Screen



Certificate Signing Request

CSR Alias	
Common Name(CN)	
Subject Alternative Name(SAN)	DNS
Business Name / Organization	
Department Name / Organization Unit	
Town / City	
Province, Region, County or State	
Country	

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.
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.

Field	Description
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 360°.

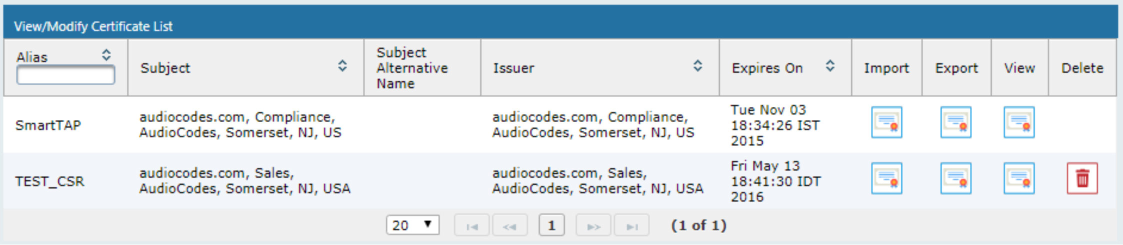
⚠ It's inadvisable to abbreviate any information except for the country codes (i.e., enter New Jersey rather than NJ), to make sure there are no issues when you send the CSR to a trusted authority in order to generate the certificate, else it may be rejected.

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.

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

Viewing/Modifying the Certificate List

Figure 6-19: Viewing/Modifying the Certificate List



View/Modify Certificate List

Alias	Subject	Subject Alternative Name	Issuer	Expires On	Import	Export	View	Delete
SmartTAP	audiocodes.com, Compliance, AudioCodes, Somerset, NJ, US		audiocodes.com, Compliance, AudioCodes, Somerset, NJ, US	Tue Nov 03 18:34:26 IST 2015	📜	📜	📜	
TEST_CSR	audiocodes.com, Sales, AudioCodes, Somerset, NJ, USA		audiocodes.com, Sales, AudioCodes, Somerset, NJ, USA	Fri May 13 18:41:30 IDT 2016	📜	📜	📜	🗑

Table 6-10: Viewing/Modifying the Certificate List

Field	Description
📜	Import signed Certificate 'filename.cer' from trusted authority
📜	Export Certificate to file to the local machine 'filename.cer'
📜	View Certificate

➢ To import a certificate:

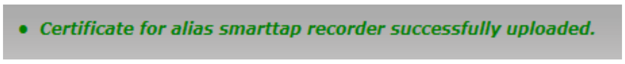
1. Open the View/Modify Certificate List page (**System** tab > **Certificates** folder > **View/Modify Certificate List**).

2. Click the **Import** icon and then the Browse button ✚ Choose to navigate to the location of the appropriate certificate file: 'filename.cer'

Figure 6-20: Import Certificate

3. Once selected, click the **Upload** link.

4. Once the upload completes, you should see a success message in the 'Command Execution Results' area.

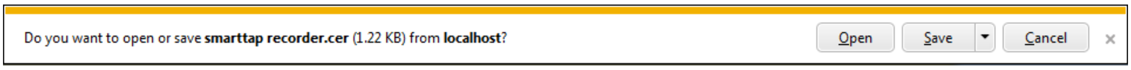


- *Certificate for alias smarttap recorder successfully uploaded.*

➢ To export a certificate:

1. Open the View/Modify Certificate List page (**System** tab > **Certificates** folder > **View/Modify Certificate List**).

2. Click the **Export** icon; the Certificate should now be available for download to the local PC.

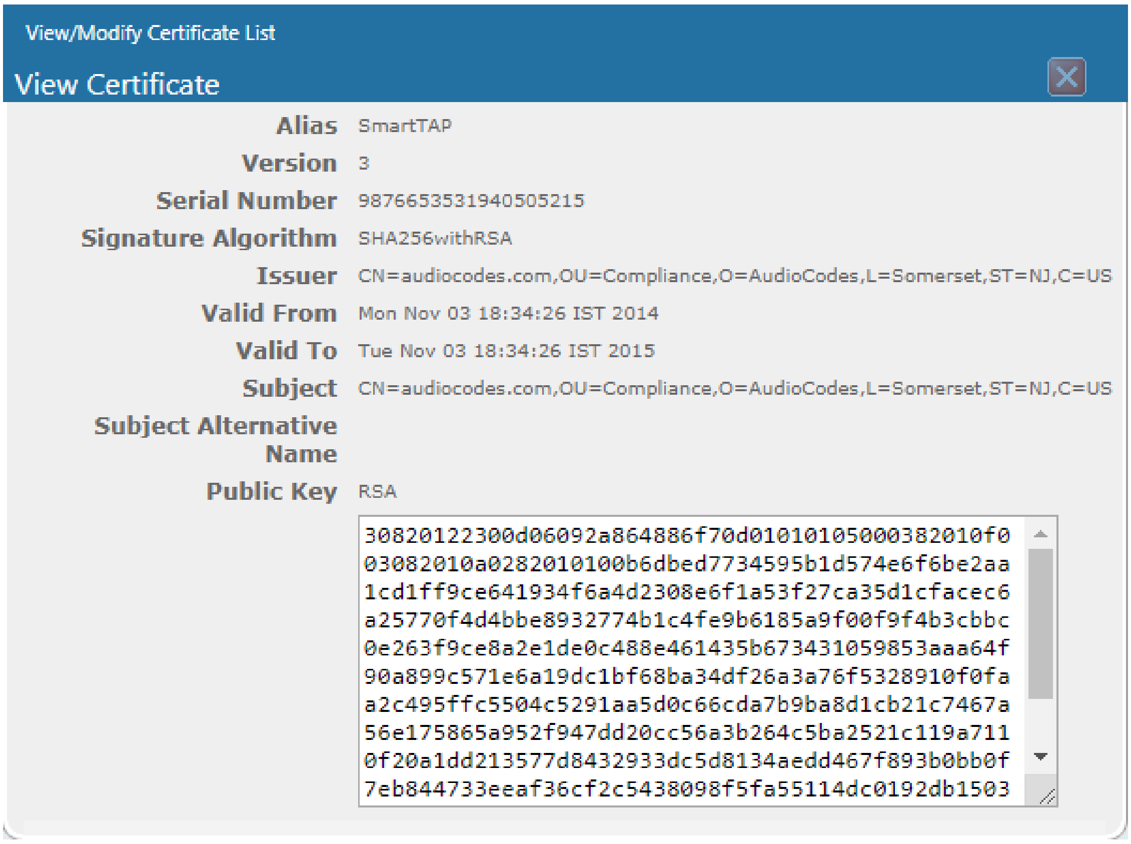


Do you want to open or save **smarttap recorder.cer** (1.22 KB) from **localhost**?

➢ To view a certificate:

1. Open the View/Modify Certificate List page (**System** tab > **Certificates** folder > **View/Modify Certificate List**), click the **View** icon.

Figure 6-21: View Certificate



View/Modify Certificate List

View Certificate

Alias	SmartTAP
Version	3
Serial Number	9876653531940505215
Signature Algorithm	SHA256withRSA
Issuer	CN=audiocodes.com,OU=Compliance,O=AudioCodes,L=Somerset,ST=NJ,C=US
Valid From	Mon Nov 03 18:34:26 IST 2014
Valid To	Tue Nov 03 18:34:26 IST 2015
Subject	CN=audiocodes.com,OU=Compliance,O=AudioCodes,L=Somerset,ST=NJ,C=US
Subject Alternative Name	
Public Key	RSA

```
30820122300d06092a864886f70d0101010500038201Of0
03082010a0282010100b6dbed7734595b1d574e6f6be2aa
1cd1ff9ce641934f6a4d2308e6f1a53f27ca35d1cfacec6
a25770f4d4bbe8932774b1c4fe9b6185a9f00f9f4b3cbbc
0e263f9ce8a2e1de0c488e461435b673431059853aaa64f
90a899c571e6a19dc1bf68ba34df26a3a76f5328910f0fa
a2c495ffc5504c5291aa5d0c66cda7b9ba8d1cb21c7467a
56e175865a952f947dd20cc56a3b264c5ba2521c119a711
0f20a1dd213577d8432933dc5d8134aedd467f893b0bb0f
7eb844733eeaf36cf2c5438098f5fa55114dc0192db1503
```

Step 2: Load Certificates

Once certificates are available, load them to secure the connection between a Web browser and the SmartTAP 360° server and for securing digital files.

Loading Web Browser Certificate

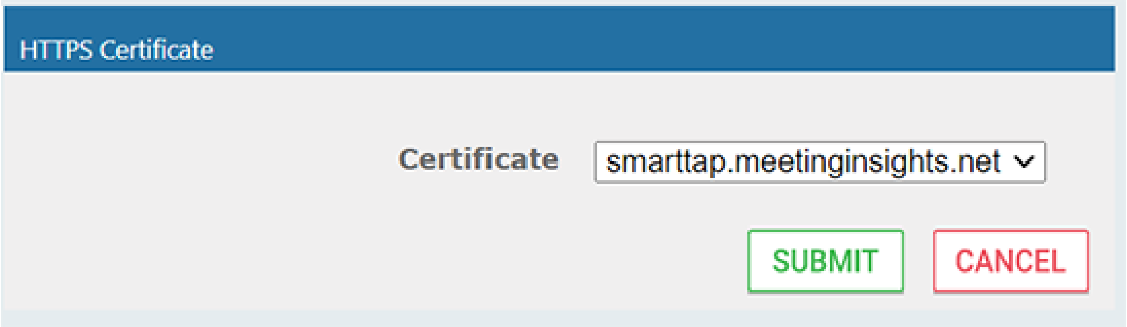
This section describes how to load the certificate to secure the connection between your Web browser and the SmartTAP 360° server.

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

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

Figure 6-22: HTTPS Certificate

Figure 6-23:



HTTPS Certificate

Certificate: smarttap.meetinginsights.net

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

3. Restart the SmartTAP 360° server.

Loading Digital Files Certificate

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

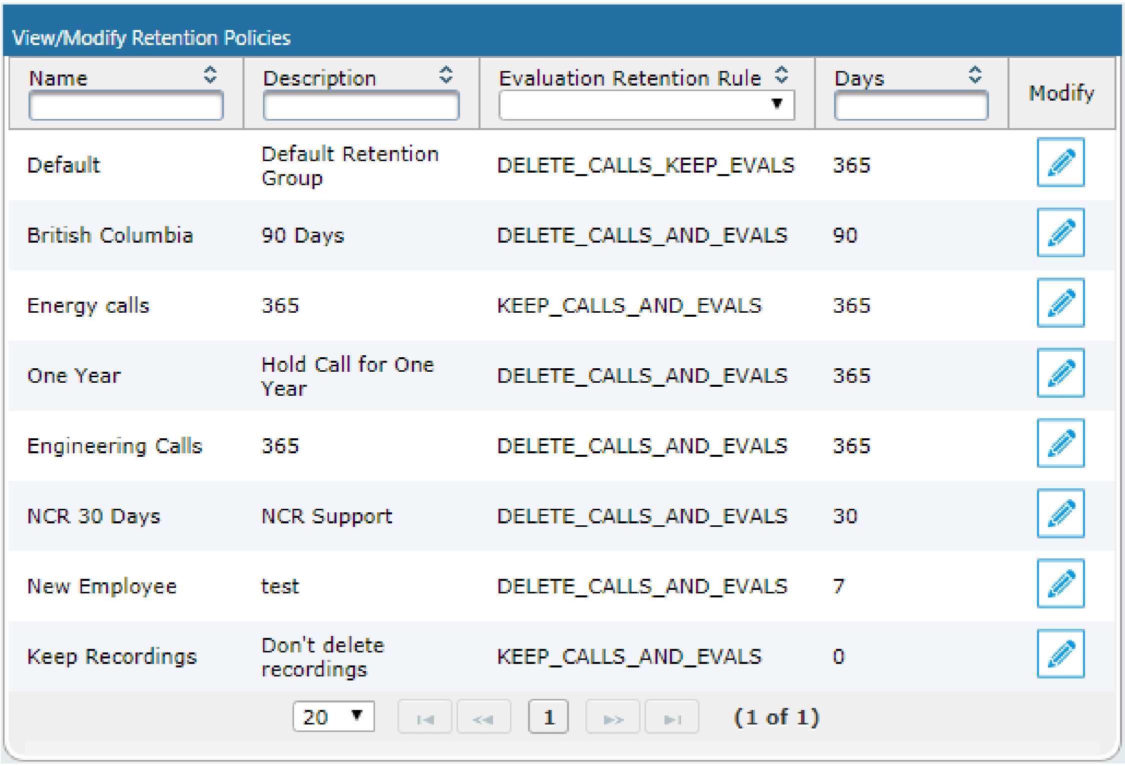
➢ **To load the digital files certificate:**

1. Open the Digital Signature page (**System** tab > **Media** folder > **Digital Signature**).

2. Select the appropriate certificate from the Certificate list box.

3. Click SUBMIT.

Figure 6-24: Digital Signature



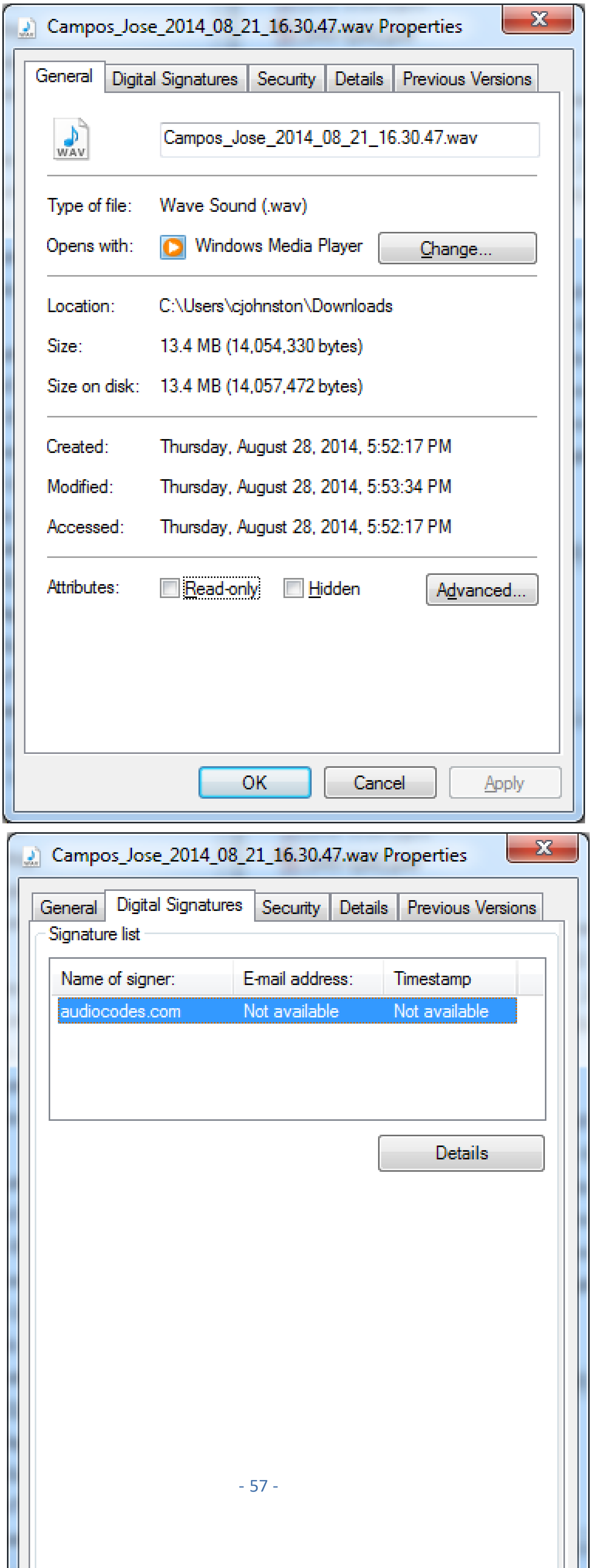
View/Modify Retention Policies

Name	Description	Evaluation Retention Rule	Days	Modify
Default	Default Retention Group	DELETE_CALLS_KEEP_EVALS	365	✎
British Columbia	90 Days	DELETE_CALLS_AND_EVALS	90	✎
Energy calls	365	KEEP_CALLS_AND_EVALS	365	✎
One Year	Hold Call for One Year	DELETE_CALLS_AND_EVALS	365	✎
Engineering Calls	365	DELETE_CALLS_AND_EVALS	365	✎
NCR 30 Days	NCR Support	DELETE_CALLS_AND_EVALS	30	✎
New Employee	test	DELETE_CALLS_AND_EVALS	7	✎
Keep Recordings	Don't delete recordings	KEEP_CALLS_AND_EVALS	0	✎

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 360° 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 6-25: Digital Signature Details



Campos_Jose_2014_08_21_16.30.47.wav

Type of file: Wave Sound (.wav)

Opens with: Windows Media Player

Location: C:\Users\cjohnston\Downloads

Size: 13.4 MB (14,054,330 bytes)

Size on disk: 13.4 MB (14,057,472 bytes)

Created: Thursday, August 28, 2014, 5:52:17 PM

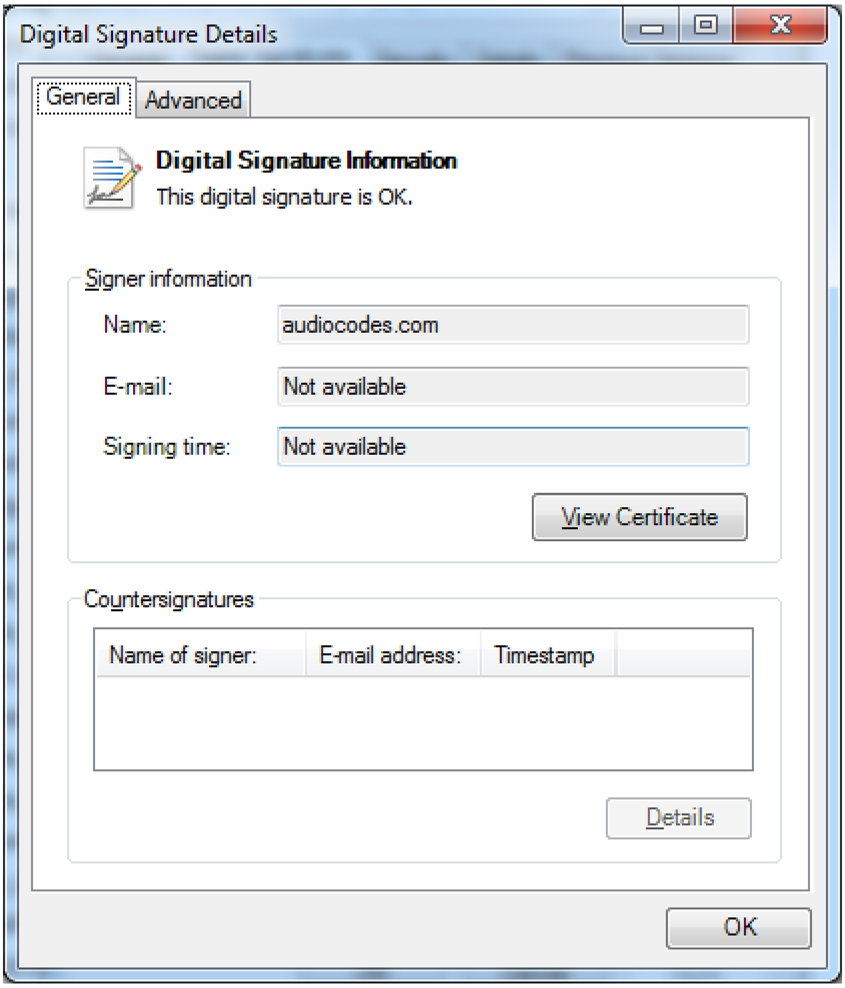
Modified: Thursday, August 28, 2014, 5:53:34 PM

Accessed: Thursday, August 28, 2014, 5:52:17 PM

Attributes: □ Read-only □ Hidden

Signature list

Name of signer:	E-mail address:	Timestamp
audiocodes.com	Not available	Not available



Digital Signature Information

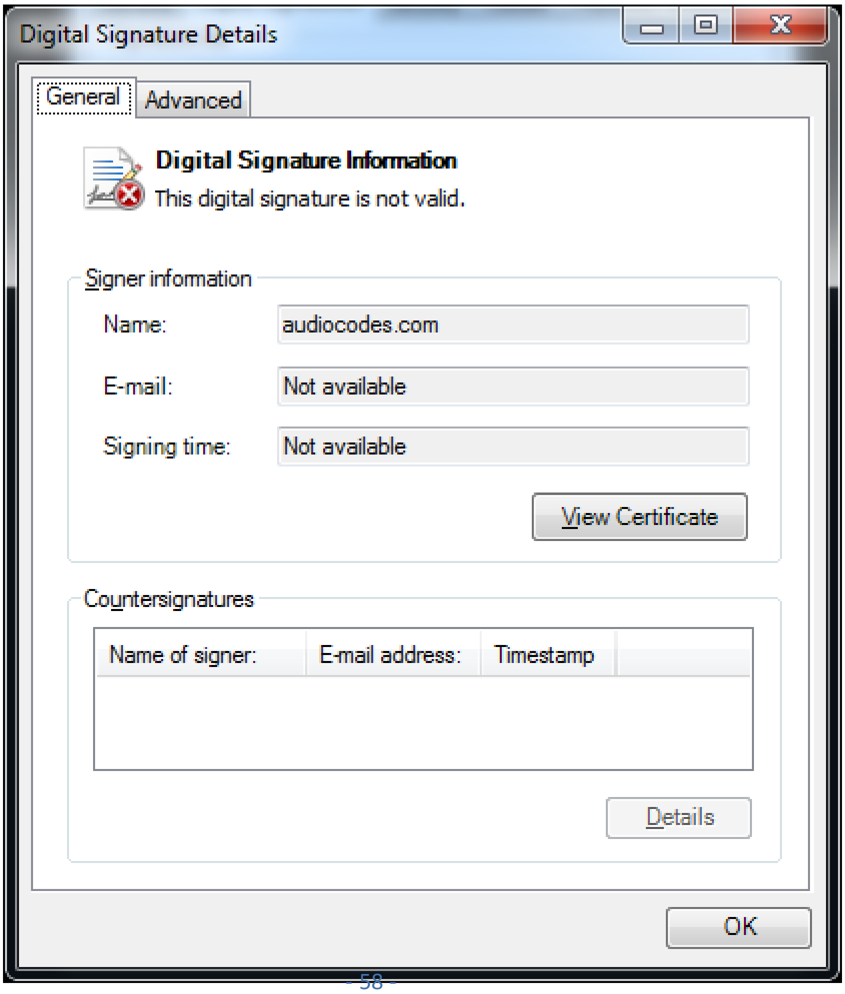
This digital signature is OK.

Signer information

Name:	audiocodes.com
E-mail:	Not available
Signing time:	Not available

Countersignatures

Name of signer:	E-mail address:	Timestamp



Digital Signature Information

This digital signature is not valid.

Signer information

Name:	audiocodes.com
E-mail:	Not available
Signing time:	Not available

Countersignatures

Name of signer:	E-mail address:	Timestamp

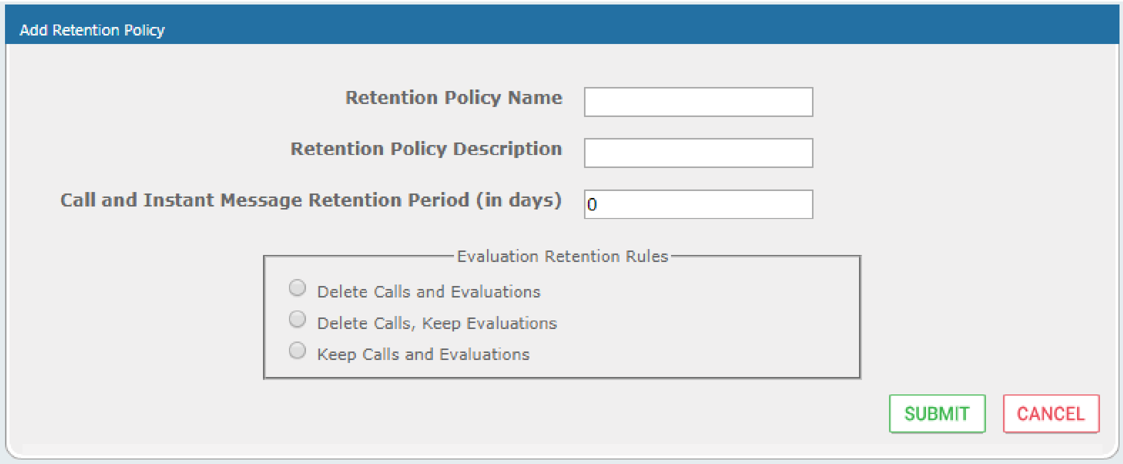
⚠ For instructions on how to install the add-on, refer to the *SmartTAP 360° Installation Guide* .

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 360° 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 6-26: Call Retention Screen – Add Retention Policy



Add Retention Policy

Retention Policy Name

Retention Policy Description

Call and Instant Message Retention Period (in days) 0

Evaluation Retention Rules

○ Delete Calls and Evaluations

○ Delete Calls, Keep Evaluations

○ Keep Calls and Evaluations

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.
SUBMIT	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.

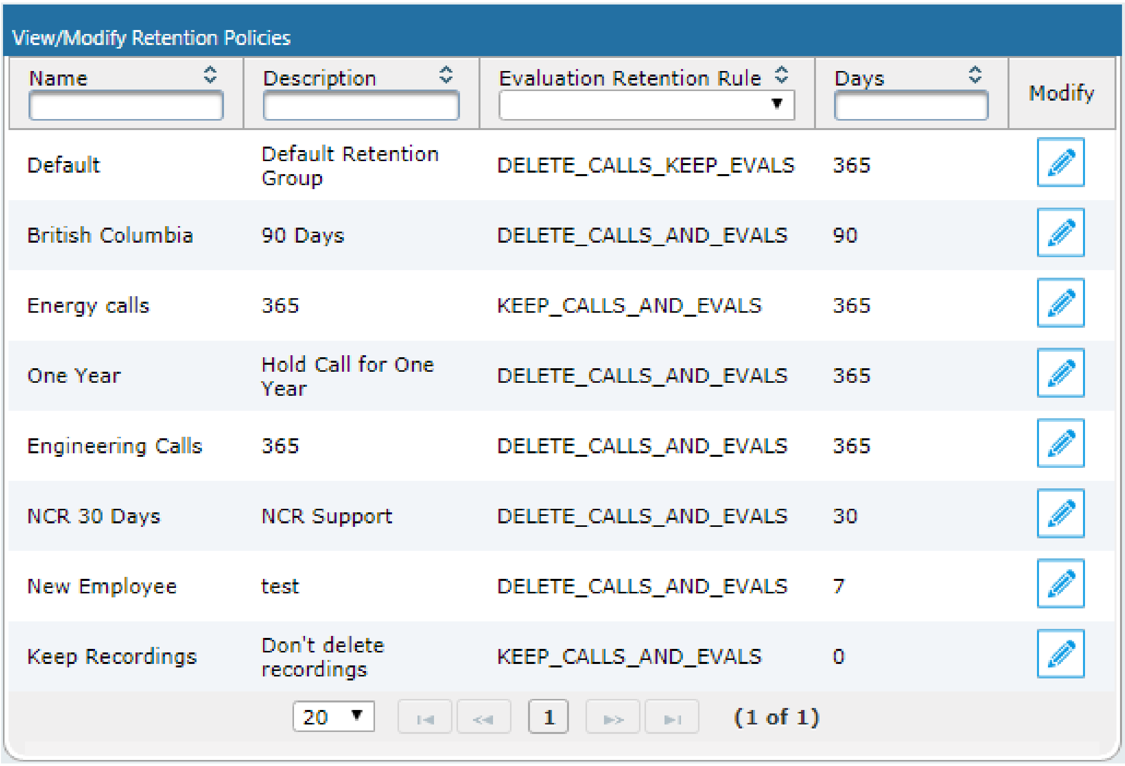
➢ To add a new retention policy:

1. Open the Call Retention screen (**System** tab > **Retention** folder > **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 Modify ✎ for a specific policy and modify the necessary fields.
3. Click SUBMIT to apply changes.

Figure 6-27: View / Modify Retention Screen



View/Modify Retention Policies

Name	Description	Evaluation Retention Rule	Days	Modify
Default	Default Retention Group	DELETE_CALLS_KEEP_EVALS	365	✎
British Columbia	90 Days	DELETE_CALLS_AND_EVALS	90	✎
Energy calls	365	KEEP_CALLS_AND_EVALS	365	✎
One Year	Hold Call for One Year	DELETE_CALLS_AND_EVALS	365	✎
Engineering Calls	365	DELETE_CALLS_AND_EVALS	365	✎
NCR 30 Days	NCR Support	DELETE_CALLS_AND_EVALS	30	✎
New Employee	test	DELETE_CALLS_AND_EVALS	7	✎
Keep Recordings	Don't delete recordings	KEEP_CALLS_AND_EVALS	0	✎

Save on Demand Call Retention

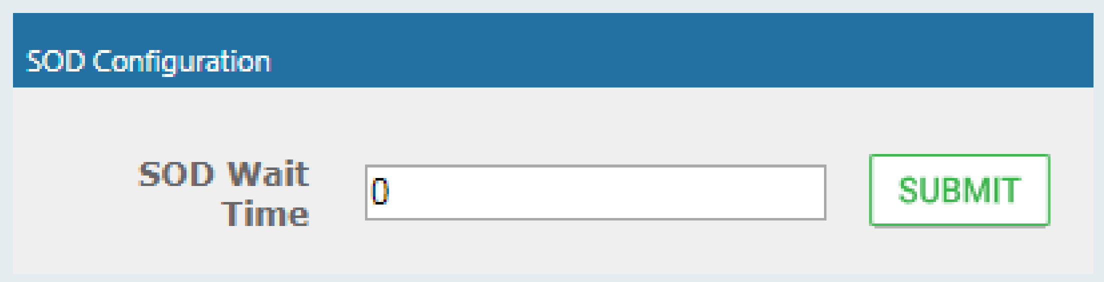
This features enables the recording of a Save on Demand call after the call is no longer active. Such a call can be recorded after an elapsed time period of up to 10 minutes. By default, this parameter is set to 0 (a Save on Demand call cannot be recorded after it is no longer active). This feature is designed to prevent hoax callers from compromising the security and integrity of the Enterprise or Call Center.

➢ To configure a time elapse for the recording of Save on Demand calls:

1. Open the SOD Configuration screen (**System** tab > **Retention** folder > **Save on Demand**).

2. Configure the SOD Threshold value in seconds (up to 10 minutes-600 seconds)

Figure 6-28: SOD Configuration



SOD Configuration

SOD Wait Time: 0

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:

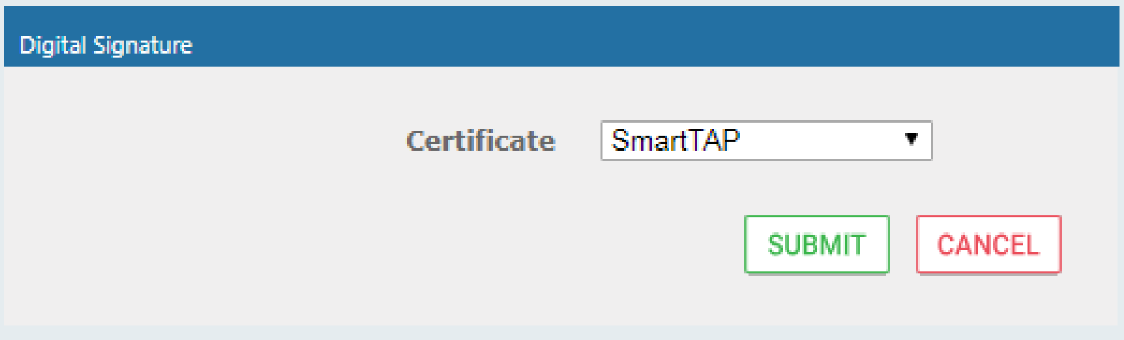
- Digital Signature to ensure that an electronic document (e-mail, spreadsheet, audio file, etc.) is authentic.
- SMTP interface to allow the SmartTAP 360° server to send outbound emails
- LDAP interface to allow SmartTAP 360° to use Active Directory users, groups, and security profiles
- Media storage location which may be stored on a network device
- End-user Web timeout

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 Generating and Loading HTTPS Certificates on page 49.

Figure 6-29: Digital Signature



Certificate: SmartTAP ▼

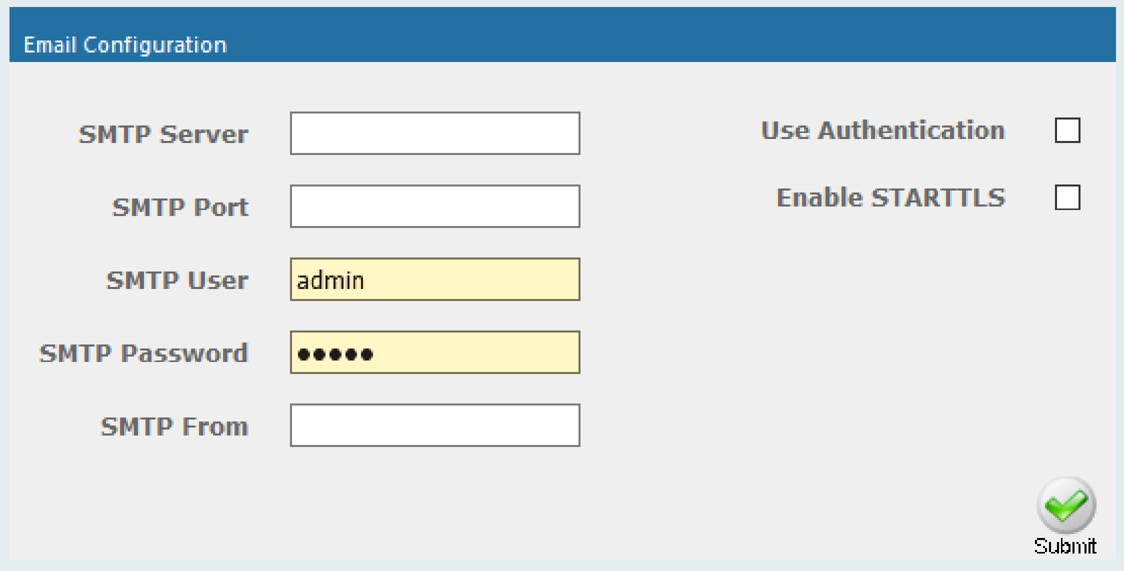
Configuring Email Server Settings

SmartTAP 360° sends automated email notifications and allows users to send emails directly from the user interface. The Email Configuration screen configures the SMTP mail server settings.

➢ **To configure email:**

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

Figure 6-30: Email



Email Configuration

SMTP Server

SMTP Port

SMTP User: admin

SMTP Password: ●●●●●

SMTP From

Use Authentication □

Enable STARTTLS □

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

3. 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. By default, SmartTAP 360° will send emails from CallRecording@<SNMPServerDomain>.com. To make sure an email is sent from your domain, set the SMTP User to username@YourDomain.com. In addition, you can instead customize an email address from which to send emails in the SMTP From field (see below).
SMTP Password	Email user password.
SMTP From	Custom User-defined source email address (must be a valid email address defined on the SMTP server above). When this field is defined, all emails are sent from this email address instead of the default address described above in 'SMTP User'.
Use Authentication	Select the option if the SMTP server requires authentication.
Enable	Select the option when the SMTP server requires TLS.

Field	Description
STARTTLS	
SUBMIT	Applies the changes.

4. Apply changes (SmartTAP 360° 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.

⚠ Email must be set up for SmartTAP 360° to send email notifications, new user passwords, reset passwords, email recordings, email messages, etc.

Configuring Media

This section shows how to configure the items under the 'Media' folder shown in the figure below. Use the table below as a reference when accessing the items in the Media folder.

Table 6-14: Media Folder

Item	Description
Credentials	Sets the credentials to access the media recording locations. The credentials should be valid for all defined locations. See Configuring User Credentials on the next page. See also Configuring User Credentials for Microsoft Teams Deployments on page 66.
Add Recording Location	Defines and adds a new media storage location. See Adding a Recording Location on page 71. See also Adding a Recording Location for Microsoft Teams Deployments on page 73
View/Modify Rec. Locations	Allows viewing and modifying an existing media location. SmartTAP 360° 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 Viewing and Modifying a Recording Location on page 76
Recording Format	Defines a recording format, e.g., encryption and compression. See Defining a Recording Format on page 77
Live Monitoring	The Live monitoring feature allows users to listen to calls in real time. See Configure Live Monitoring Location on page 78

Item	Description
Location	

Configuring User Credentials

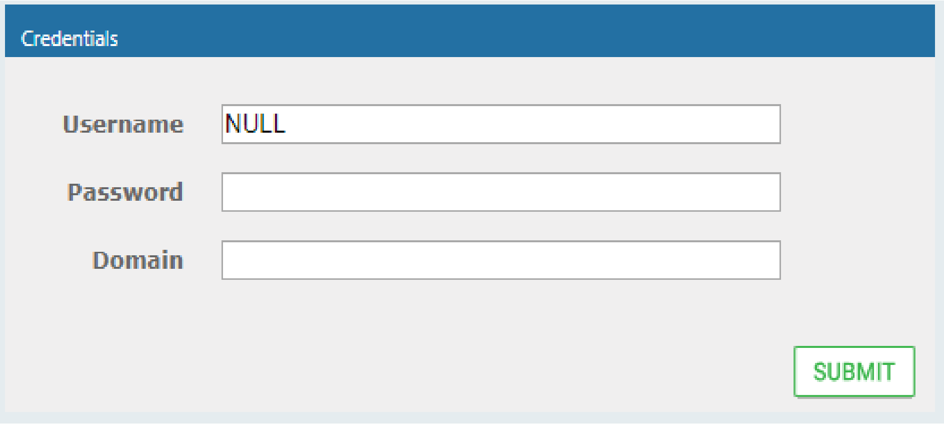
This section shows how to define credentials for accessing shared resources. Whenever you add or modify the location for saving recording or live monitoring files, SmartTAP 360° verifies whether this location is accessible to the user defined in this procedure.

- You must define credentials before adding an SMB recording location (as described in Adding a Recording Location on page 71) otherwise the attempt to add the location will fail.
- If you are deploying with Microsoft Teams, see Configuring User Credentials for Microsoft Teams Deployments on the next page.

➢ To define credentials:

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

Figure 6-31: Credentials



Credentials

Username: NULL

Password:

Domain:

2. Use the table below as a reference when defining credentials.

Table 6-15: 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.

3. Click SUBMIT.

Configuring User Credentials for Microsoft Teams Deployments

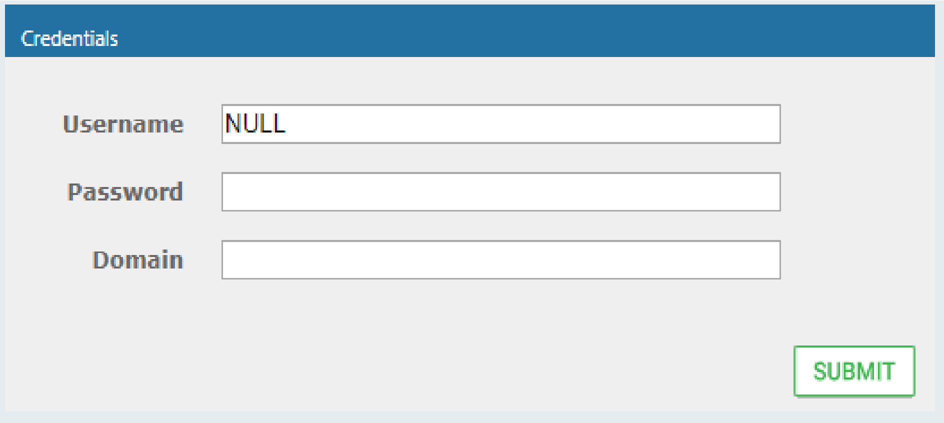
This section describes how to configure credentials for accessing shared resources when media files are shared with a Microsoft Azure deployment implementing either a Microsoft Blob or Fileshare storage account. Whenever you add or modify the location for saving recordings, SmartTAP 360° verifies whether this location is accessible to the user defined in this procedure.

> ⚠ You must define credentials before adding an SMB recording location (as described in Adding a Recording Location for Microsoft Teams Deployments on page 73), otherwise, the attempt to add the location will fail.

➢ **To configure credentials:**

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

Figure 6-32: Credentials



Username: NULL

Password:

Domain:

2. Use the tables below as references when defining credentials.

Table 6-16: Credentials for Accessing a Microsoft Azure SMB Fileshare Account

Parameter	Description
Username	Specify the Storage username defined for the Fileshare storage account.
Password	Specify the Storage Password defined for the Fileshare storage account.
Domain	Specify the Azure domain used to authenticate the username and password for accessing shared resources.

For extracting these credentials, see Extracting User Credentials from Microsoft Azure Fileshare Account on the next page

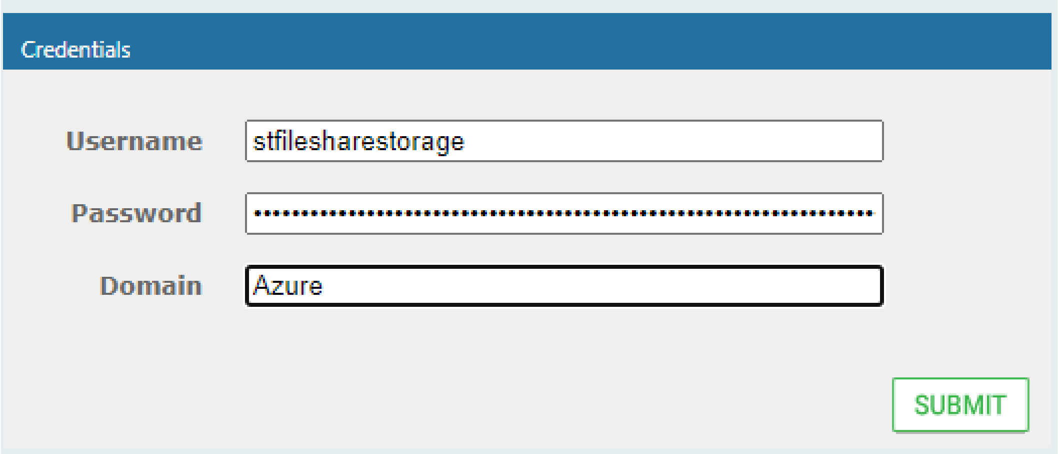
Table 6-17: Credentials for Accessing a Microsoft Blob Account

Parameter	Description
Username	Specify the storage account name where the Blob container was created.

Parameter	Description
Password	Specify the “access key” for the Blob storage account
Domain	Specify the Azure domain used to authenticate the username and password for accessing shared resources.

For extracting these credentials, see Setting up Microsoft Azure Blob Storage Account on page 69

Figure 6-33: Microsoft Azure Storage Credentials



Credentials

Username: stfilesharestorage

Password: •••

Domain: Azure

3. Click SUBMIT.

Extracting User Credentials from Microsoft Azure Fileshare Account

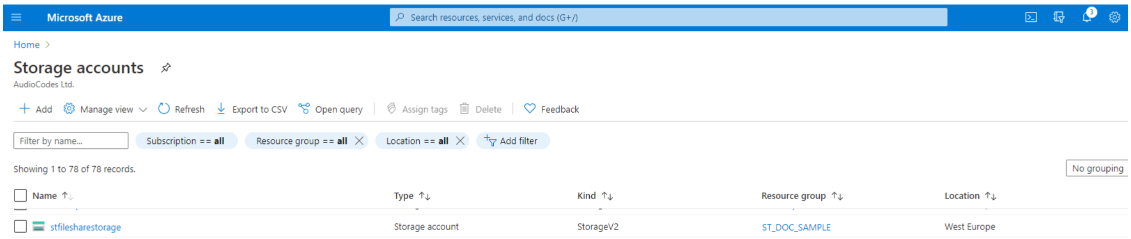
To use Azure Fileshare storage as a media location, the following Azure information must be extracted:

- Azure Storage Address
- Storage Domain\Username
- Storage password
- Fileshare name

➢ To extract these credentials from Microsoft Azure:

1. Go to **Azure Portal** > **Storage Accounts**.

Figure 6-34: Storage Accounts

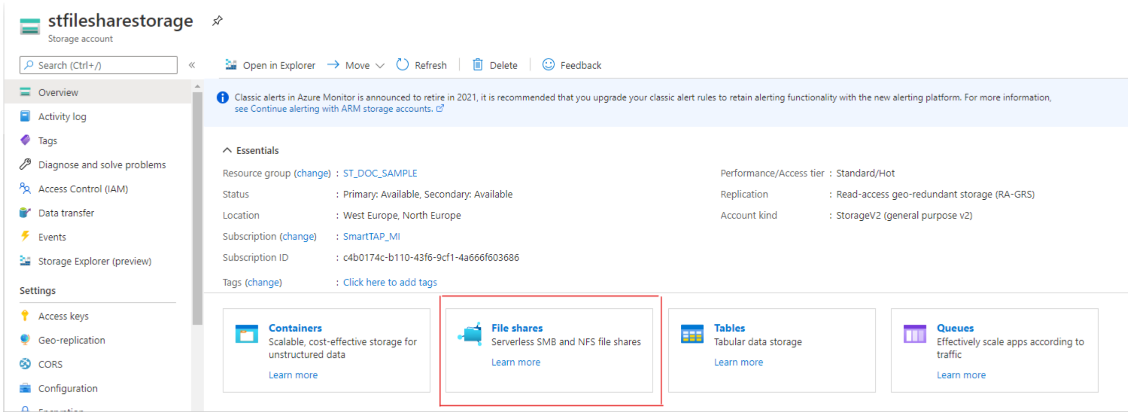


Showing 1 to 78 of 78 records.

Name	Type	Kind	Resource group	Location
stfilesharestorage	Storage account	StorageV2	ST_DOC_SAMPLE	West Europe

2. Double-click the relevant storage account.

Figure 6-35: File Shares

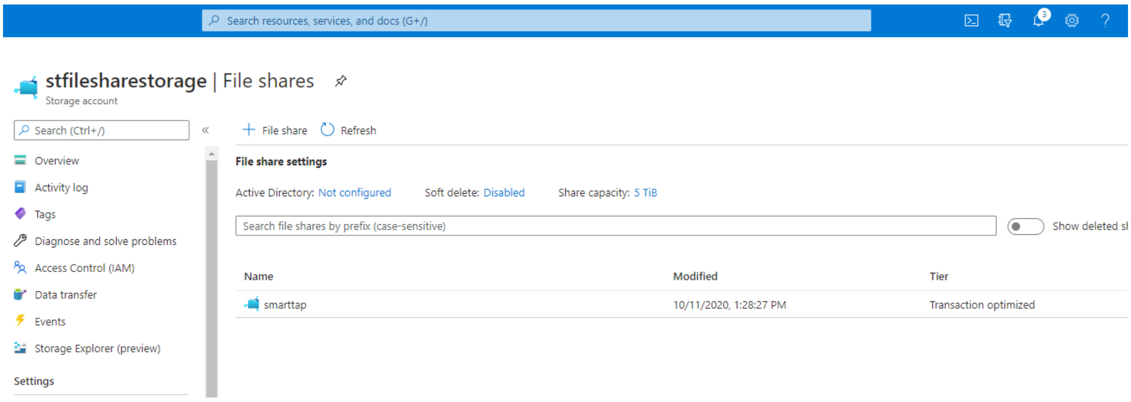


Classic alerts in Azure Monitor is announced to retire in 2021, it is recommended that you upgrade your classic alert rules to retain alerting functionality with the new alerting platform. For more information, see Continue alerting with ARM storage accounts.

Resource group (change) : ST_DOC_SAMPLE
Status : Primary: Available, Secondary: Available
Location : West Europe, North Europe
Subscription (change) : SmartTAP_MI
Subscription ID : c4b0174c-b110-43f6-9cf1-4a666f603686
Tags (change) : Click here to add tags
Performance/Access tier : Standard/Hot
Replication : Read-access geo-redundant storage (RA-GRS)
Account kind : StorageV2 (general purpose v2)

3. Click **File shares**; the File Shares screen is displayed.

Figure 6-36: File Share Settings


Search resources, services, and docs (G+/)
stfilesharestorage | File shares
Storage account
Search (Ctrl+/)
File share
Refresh
Overview
Activity log
Tags
Diagnose and solve problems
Access Control (IAM)
Data transfer
Events
Storage Explorer (preview)
Settings
Search file shares by prefix (case-sensitive)
Show deleted sl

File share settings

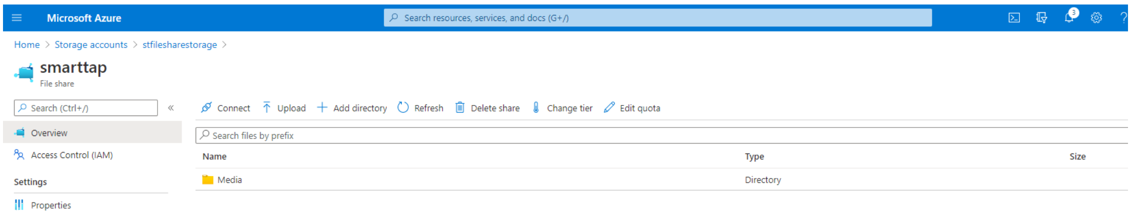
Active Directory: Not configured Soft delete: Disabled Share capacity: 5 TiB

Name	Modified	Tier
smarttap	10/11/2020, 1:28:27 PM	Transaction optimized

4. Copy the relevant File share name and click on it.

Example: Fileshare name=”smarttap”

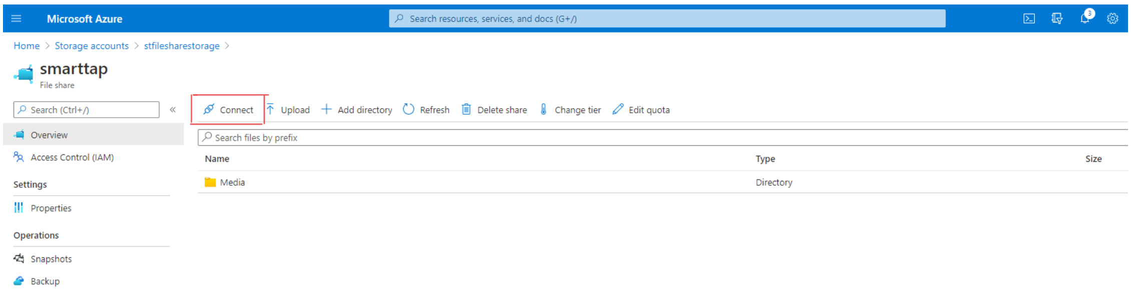
Figure 6-37: Media Directory Name



Name	Type	Size
Media	Directory	

5. 5. Copy the Media Directory name

Example: Media directory name=”Media”



The Connection script opens.

```
cmd.exe /C "cmdkey /add:`"stfilesharestorage.file.core.windows.net`"
/user:`"Azure\stfilesharestorage`"
/pass:`"RM13Fp6N8VmPZ/P1bgN+4M3Gg5CT7+ALbc6i7DUX/fbeB7tR3CF
BCX7lJWCQgj9xdJmBmX38fcAsnOEioGTaEw==`""
```

6. Copy the following password values:

- Azure Storage Address=add
- Storage Domain\Username=user
- Storage password=pass

Example:

```
Azure Storage Address= stfilesharestorage.file.core.windows.net
```

```
Storage Domain\Username=Azure\ stfilesharestorage
```

```
Storage Password=
RM13Fp6N8VmPZ/P1bgN+4M3Gg5CT7+ALbc6i7DUX/fbeB7tR3CFBCX7lJ
WCQgj9xdJmBmX38fcAsnOEioGTaEw==
```

Setting up Microsoft Azure Blob Storage Account

This procedure describes how to configure Microsoft Azure Blob Storage for storing media recorded by the SmartTAP 360° BOT in the Microsoft Teams deployment.

When the Microsoft Teams deployment is hosted in the customer's Azure subscription, the SmartTAP Server can be deployed On-premises, utilizing the On-premises Server Message Block (SMB) storage for media storage (described in Viewing and Modifying a Recording Location on page 76). You cannot configure both On-Premises and Blob Storage.

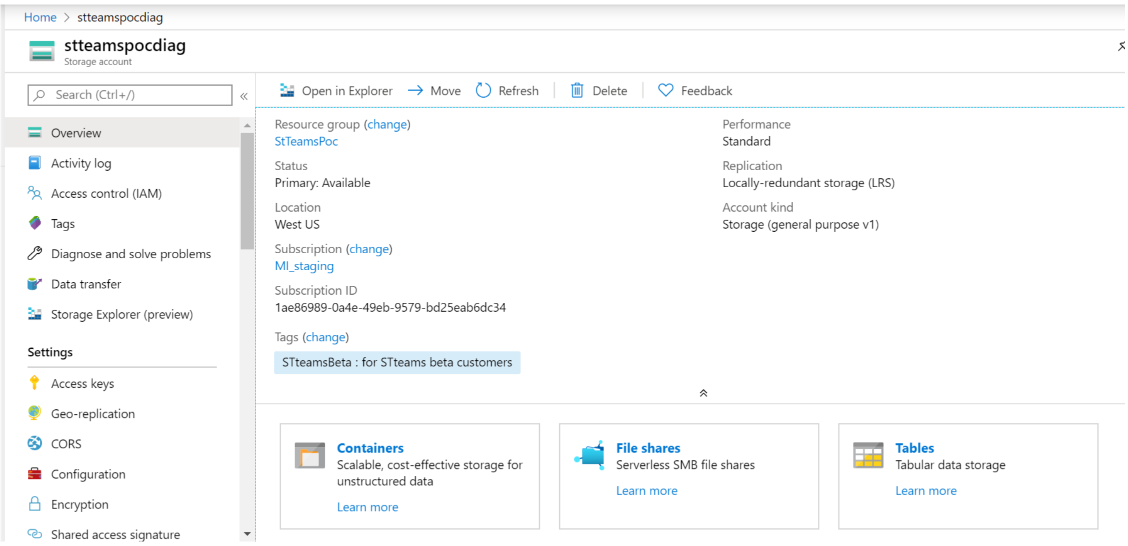
➢ To configure Microsoft Blob:

1. Login to the Microsoft Azure portal (https://portal.azure.com/).

2. Open the Storage account settings page.

3. Create or use existing storage account.

Figure 6-38: Microsoft Blob Storage Account



Resource group (change)
StTeamsPoc

Status
Primary: Available

Location
West US

Subscription (change)
MI_staging

Subscription ID
1ae86989-0a4e-49eb-9579-bd25eab6dc34

Tags (change)
STteamsBeta : for STteams beta customers

Performance
Standard

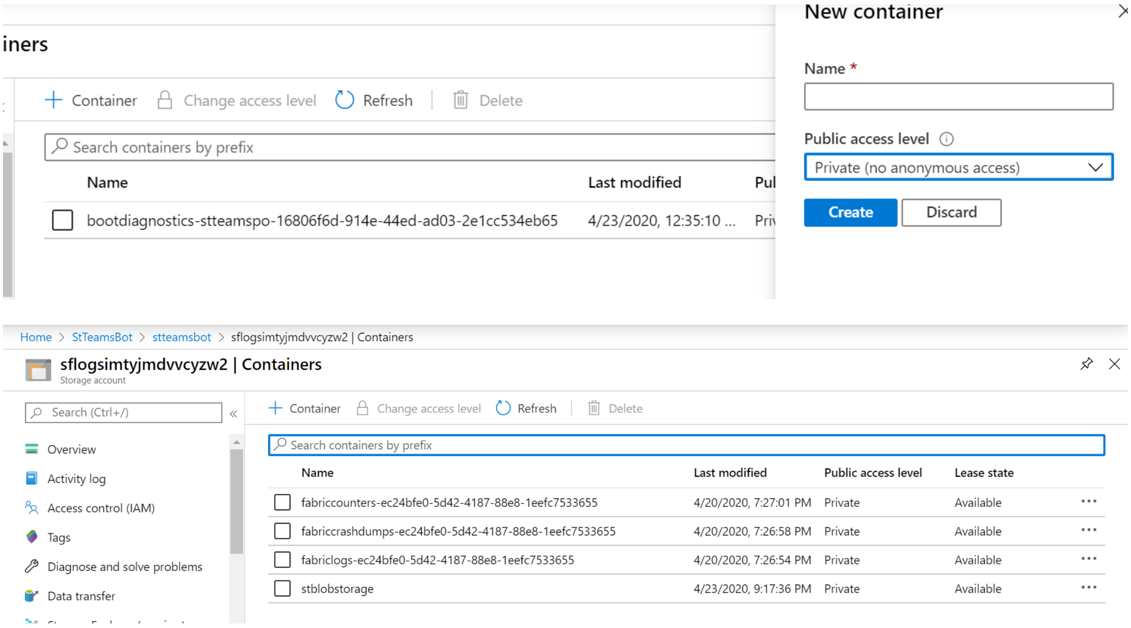
Replication
Locally-redundant storage (LRS)

Account kind
Storage (general purpose v1)

4. Save the storage name for SmartTAP 360° settings.

5. Create anew container for BLOB media storage and save the name.

Figure 6-39: Create New Blob Container



Name	Last modified	Pu
□ bootdiagnostics-stteamspo-16806f6d-914e-44ed-ad03-2e1cc534eb65	4/23/2020, 12:35:10 ...	Pri

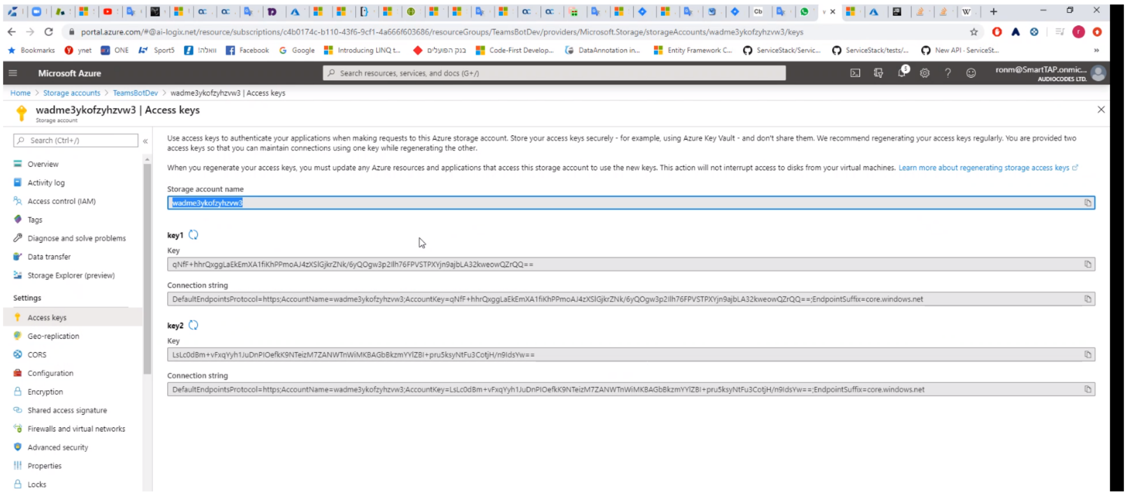
Name *

Public access level: Private (no anonymous access)

Name	Last modified	Public access level	Lease state
□ fabriccounters-ec24bfe0-5d42-4187-88e8-1eefc7533655	4/20/2020, 7:27:01 PM	Private	Available
□ fabriccrashdumps-ec24bfe0-5d42-4187-88e8-1eefc7533655	4/20/2020, 7:26:58 PM	Private	Available
□ fabriclogs-ec24bfe0-5d42-4187-88e8-1eefc7533655	4/20/2020, 7:26:54 PM	Private	Available
□ stblobstorage	4/23/2020, 9:17:36 PM	Private	Available

6. Save the storage name and credentials.

Figure 6-40: Storage Name and Credentials



portal.azure.com/#@ai-logix.net/resource/subscriptions/c4b0174c-b110-43f6-9cf1-4a666f603686/resourceGroups/TeamsBotDev/providers/Microsoft.Storage/storageAccounts/wadme3ykofzyhzvw3/keys
Microsoft Azure
Search resources, services, and docs (G+/)
ronm@SmartTAP.onmic...
AUDIOCODES LTD.
Home > Storage accounts > TeamsBotDev > wadme3ykofzyhzvw3 | Access keys
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Data transfer
Storage Explorer (preview)
Settings
Access keys
Geo-replication
CORS
Configuration
Encryption
Shared access signature
Firewalls and virtual networks
Advanced security
Properties
Locks

wadme3ykofzyhzvw3 | Access keys

Storage account

Use access keys to authenticate your applications when making requests to this Azure storage account. Store your access keys securely - for example, using Azure Key Vault - and don't share them. We recommend regenerating your access keys regularly. You are provided two access keys so that you can maintain connections using one key while regenerating the other.

When you regenerate your access keys, you must update any Azure resources and applications that access this storage account to use the new keys. This action will not interrupt access to disks from your virtual machines. Learn more about regenerating storage access keys

Storage account name

wadme3ykofzyhzvw3

key1

Key

qNfF+hhrQxggLaEkEmXA1fiKhPPmoAJ4zXSlGjkrZNk/6yQOgw3p2Ilh76FPVSTPXYjn9ajbLA32kweowQZrQQ==

Connection string

DefaultEndpointsProtocol=https;AccountName=wadme3ykofzyhzvw3;AccountKey=qNfF+hhrQxggLaEkEmXA1fiKhPPmoAJ4zXSlGjkrZNk/6yQOgw3p2Ilh76FPVSTPXYjn9ajbLA32kweowQZrQQ==;EndpointSuffix=core.windows.net

key2

Key

LsLc0dBm+vFxqYyh1JuDnPIOefkK9NTeizM7ZANWTnWiMKBAGbBkzmYYlZBI+pru5ksyNtFu3CotjH/n9IdsYw==

Connection string

DefaultEndpointsProtocol=https;AccountName=wadme3ykofzyhzvw3;AccountKey=LsLc0dBm+vFxqYyh1JuDnPIOefkK9NTeizM7ZANWTnWiMKBAGbBkzmYYlZBI+pru5ksyNtFu3CotjH/n9IdsYw==;EndpointSuffix=core.windows.net

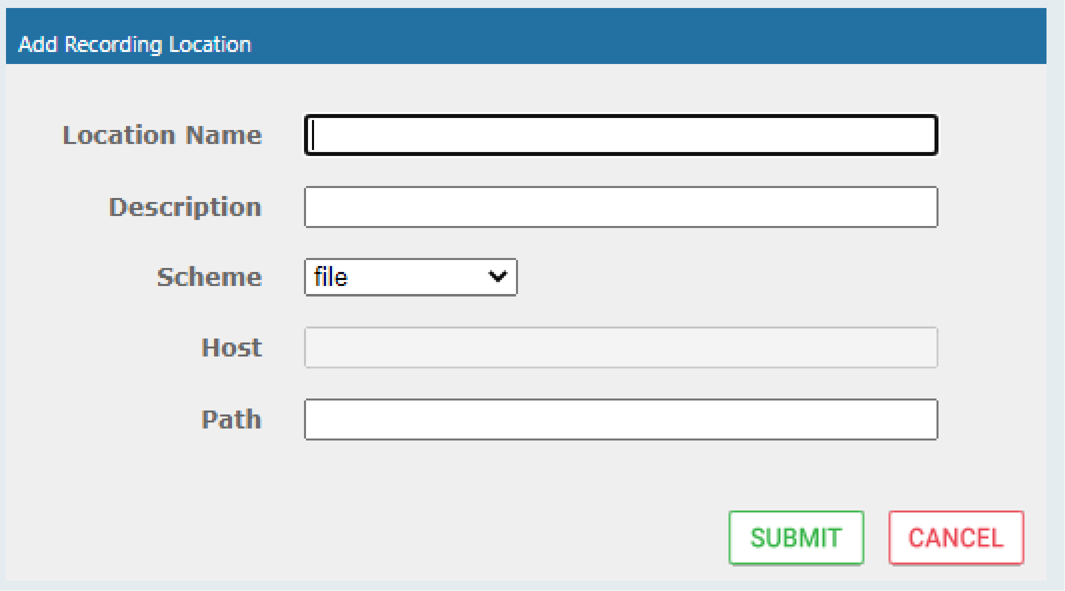
Adding a Recording Location

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 360° server (on the Call Delivery Server), or on an SMB network accessible drive, i.e., Windows shared drive for accessing files over the SMB protocol.

1. Open the Add Recording Location screen (**System** tab > **Media** folder > **Add Recording Location**).

- The default location cannot be modified.
- If you are defining shared resources 'SMB Scheme", before adding a new location, ensure that you have defined user credentials for accessing the shared resources (see Configuring User Credentials on page 65) otherwise the attempt to add the location will fail.
- If you are deploying with Microsoft Teams, see Adding a Recording Location for Microsoft Teams Deployments on page 73

Figure 6-41: Add Recording Location


Add Recording Location

Location Name

Description

Scheme: file

Host

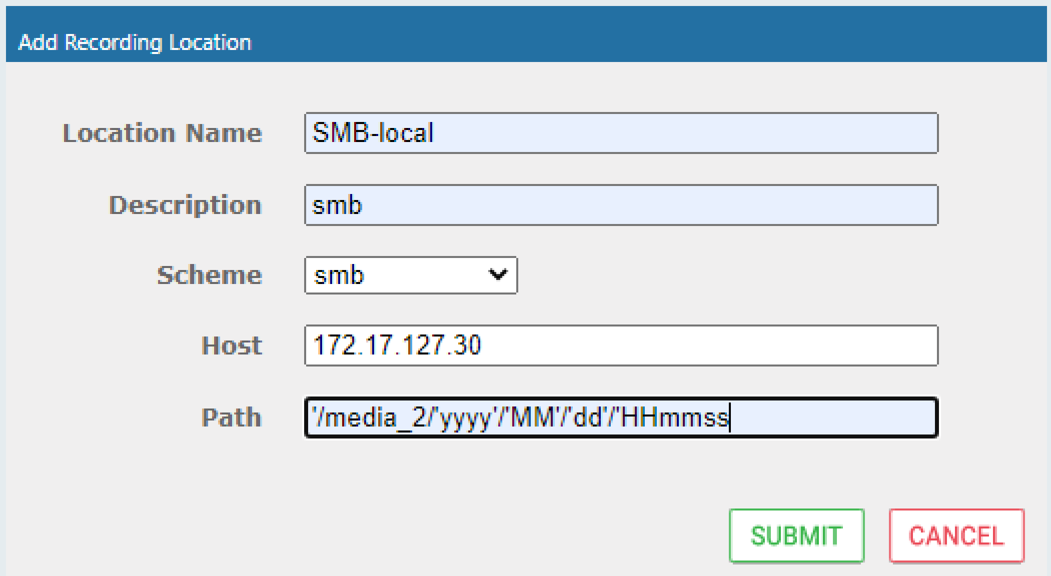
Path

2. Use the table below as a reference when adding a recording location.

Table 6-18: Add Recording Location

Parameter	Description
Location Name	Defines a name for the media location. The Location Name of Default cannot be modified.
Description	Description of the location name.
Scheme	Defines the type of database scheme: ■ Server Message Block (SMB) Shared File ■ File (local)
Host	The IP address or FQDN of the SMB Scheme host machine.
Path	Defines the media path pattern.

Figure 6-42: Add Recording Location



Add Recording Location

Location Name	SMB-local
Description	smb
Scheme	smb
Host	172.17.127.30
Path	'/media_2/'yyyy'/'MM'/'dd'/'HHmmss

3. Click SUBMIT.

- Its recommended to define the SMB Scheme host machine with an FQDN instead of an IP address. This prevents situations where the System administrator changes the IP address of the SmartTAP 360° application server and as a consequence, the media files can no longer be accessed.
- If you define the media location in a different domain to the SmartTAP 360° AS, ensure that write permissions are set for the directory to which you wish to save the media files.

Adding a Recording Location for Microsoft Teams Deployments

For Microsoft Teams deployments, media recordings can be saved according to the following scenarios:

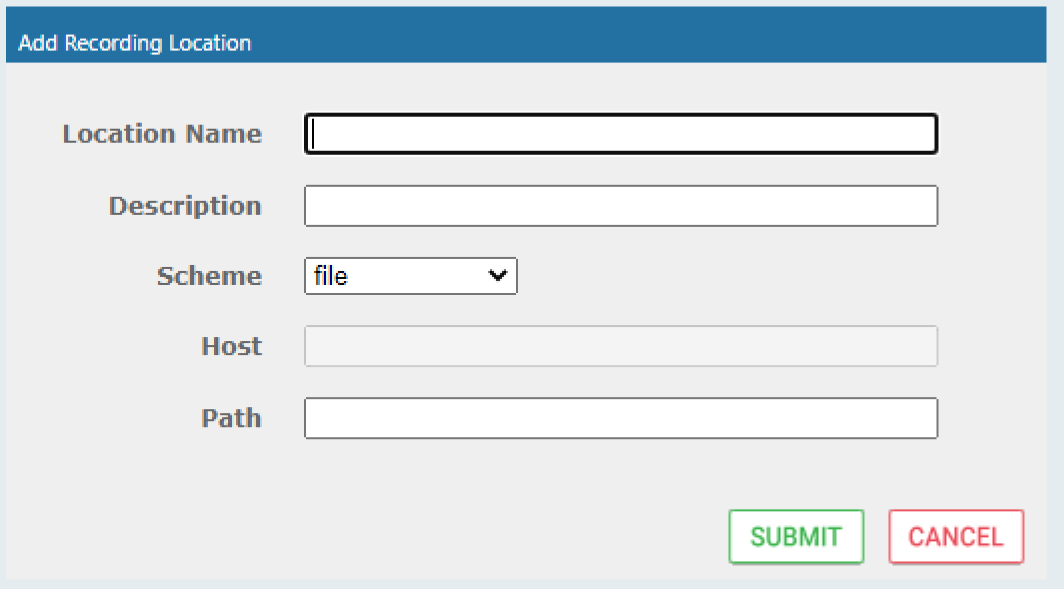
- **Local Storage (Hybrid Model):** Media files are stored locally On-premises for compliance and policy reasons. Media files are accessed via the Microsoft Azure Fileshare Storage account. For this mode, you must configure a **local** host address On-premises and configure **SMB** scheme.
- **Remote Storage on Azure Fileshare:** Media files are accessed from the Azure Fileshare storage account. For this mode you must configure a **remote** Host address and configure **SMB** scheme.
- **Remote Storage on Azure Blob:** Media files are accessed from the Azure Blob storage account. For this mode, you must configure a **remote** Host address and configure **HTTPS** scheme.

➢ To add a recording location:

1. Open the Add Recording Location screen (**System** tab > **Media** folder > **Add Recording Location**).

- The default location cannot be modified.
- Before adding a new location ensure that you have defined user credentials for accessing the shared resources (see Configuring User Credentials for Microsoft Teams Deployments on page 66)

Figure 6-43: Add Recording Location



Add Recording Location

Location Name

Description

Scheme: file

Host

Path

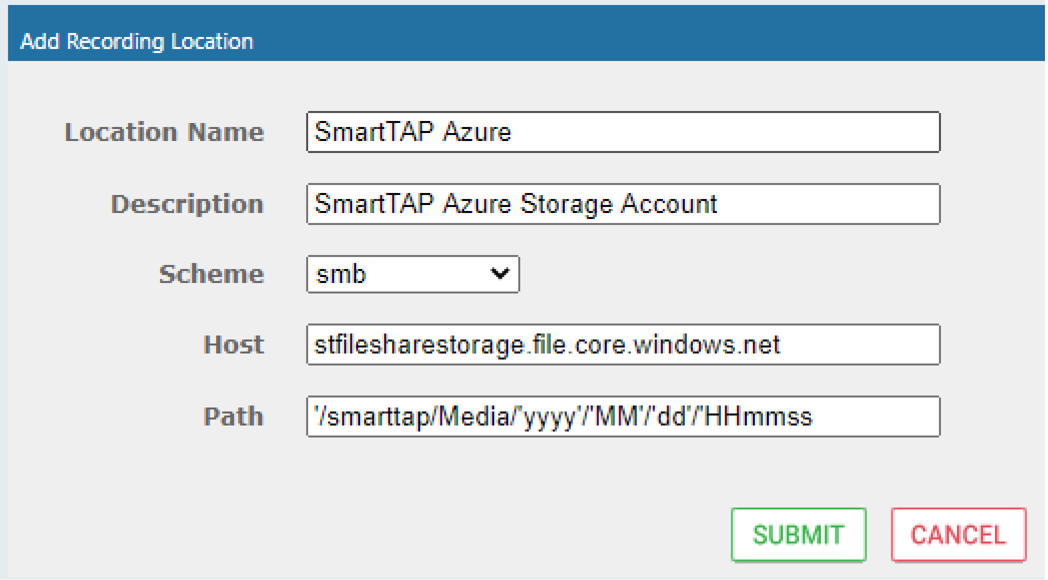
2. Use the tables below as references for configuring the Microsoft Azure recording location according to the deployment scenarios described above.

Table 6-19: Microsoft Azure Fileshare Recording Location

Parameter	Description
Location Name	Defines the name of the location of the Microsoft Azure Fileshare storage account.
Description	Description of the Microsoft Azure Fileshare storage account
Scheme	**smb**
Host	The FQDN of the SMB Scheme host machine (either **local** or **remote** host depending on the deployment scenarios described above). For example: stfilesharestorage.file.core.windows.net
Path	Defines the media path pattern. For example, '/[fileshare]/[directory]/'yyyy'/'MM'/'dd'/'HHmmss

For extracting the above credentials, see Extracting User Credentials from Microsoft Azure Fileshare Account on page 67

Figure 6-44: Microsoft Azure Fileshare Recording Location


Add Recording Location

Location Name: SmartTAP Azure

Description: SmartTAP Azure Storage Account

Scheme: smb

Host: stfilesharestorage.file.core.windows.net

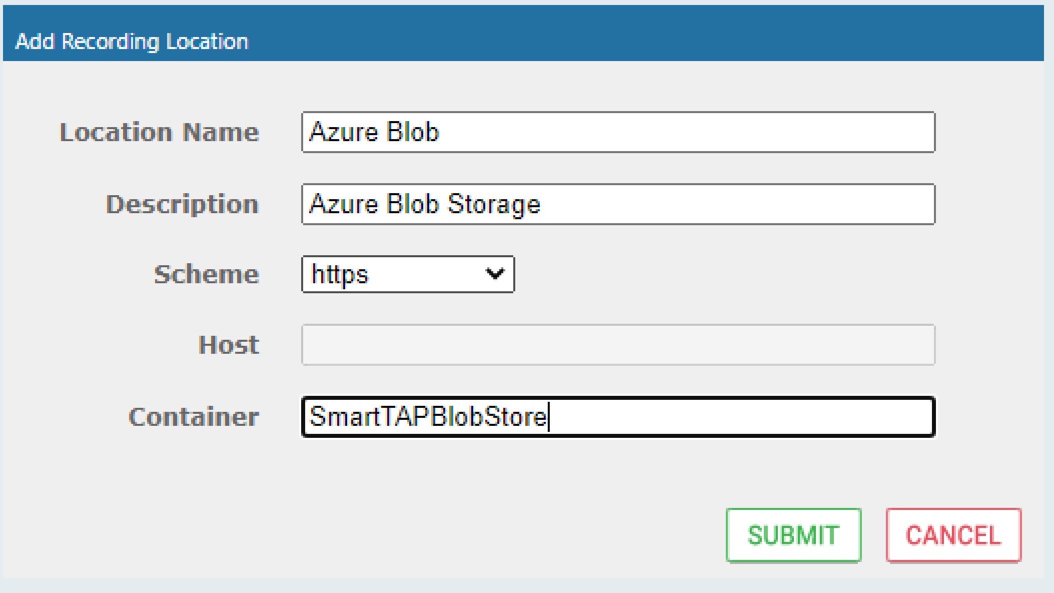
Path: '/smarttap/Media/'yyyy'/'MM'/'dd'/'HHmmss

Table 6-20: Microsoft Azure Blob Recording Location

Parameter	Description
Location Name	Defines the name of the Microsoft Blob storage account.
Description	Description of the Microsoft Blob storage account
Scheme	**https**
Container Name	The name of the container of the Microsoft Blob storage account.

For extracting the above credentials, see Setting up Microsoft Azure Blob Storage Account on page 69

Figure 6-45: Microsoft Blob Recording Location



Add Recording Location

Location Name	Azure Blob
Description	Azure Blob Storage
Scheme	https
Host	
Container	SmartTAPBlobStore

3. Click SUBMIT.

> ⚠
> - If you define the media location in a different domain to the SmartTAP 360° AS, ensure that write permissions are set for the directory to which you wish to save the media files.
> - For configuration of Azure Fileshare storage account, refer to https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-create-file-share?tabs=azure-portal

Viewing and Modifying a Recording Location

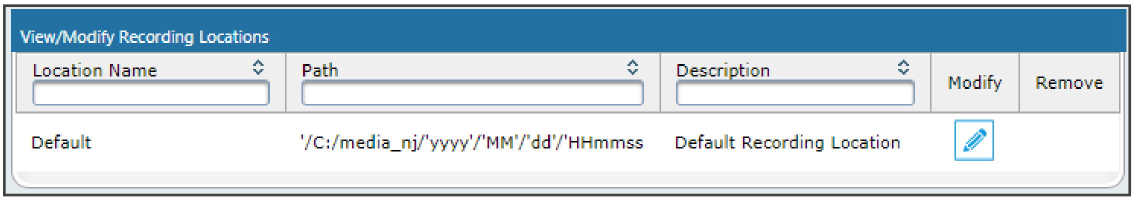
This section shows how to view or modify a location for saving recorded media.

➢ To modify a recording location:

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

> ⚠ The default location cannot be modified.

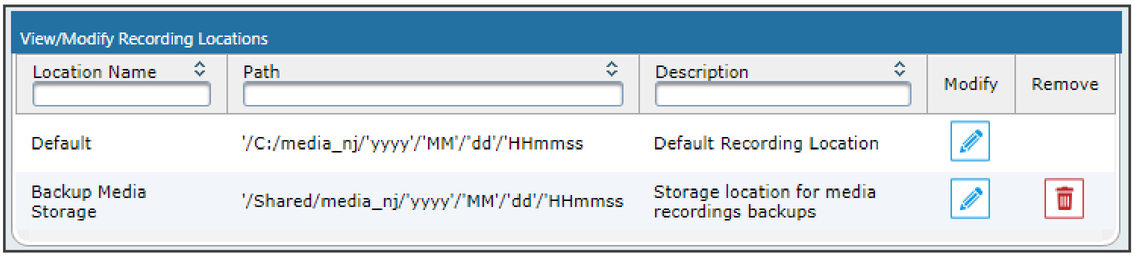
Figure 6-46: View/Modify Recording Locations - with Default Location Only



View/Modify Recording Locations

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

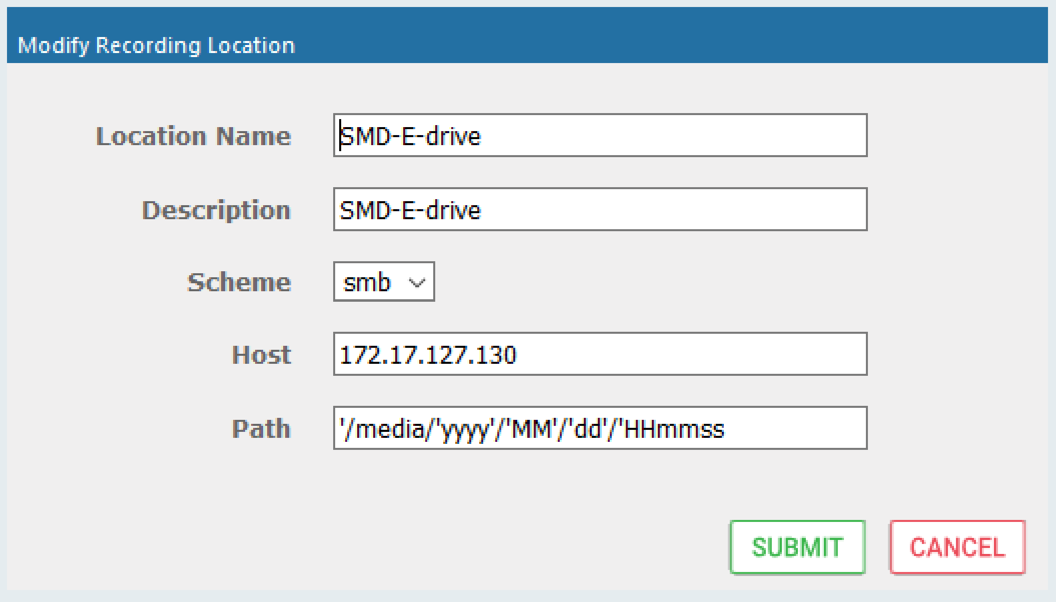
Figure 6-47: View/Modify Recording Locations - with Additional Recording Locations



View/Modify Recording Locations

Location Name	Path	Description	Modify	Remove
Default	'/C:/media_nj/'yyyy'/'MM'/'dd'/'HHmmss	Default Recording Location	✎	
Backup Media Storage	'/Shared/media_nj/'yyyy'/'MM'/'dd'/'HHmmss	Storage location for media recordings backups	✎	🗑

2. Click ✎ to open the Modify Recording Location screen.



Modify Recording Location

Location Name	SMD-E-drive
Description	SMD-E-drive
Scheme	smb
Host	172.17.127.130
Path	'/media/'yyyy'/'MM'/'dd'/'HHmmss

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

Table 6-21: Modify Recording Location

Parameter	Description
Location Name	Defines a name for the media location. The Location Name of Default cannot be modified.
Description	Description of the location name.
Scheme	Defines the type of database scheme (smb or file).
Host	The IP address or FQDN of the SMB Scheme host machine.
Path	Defines the media path pattern.

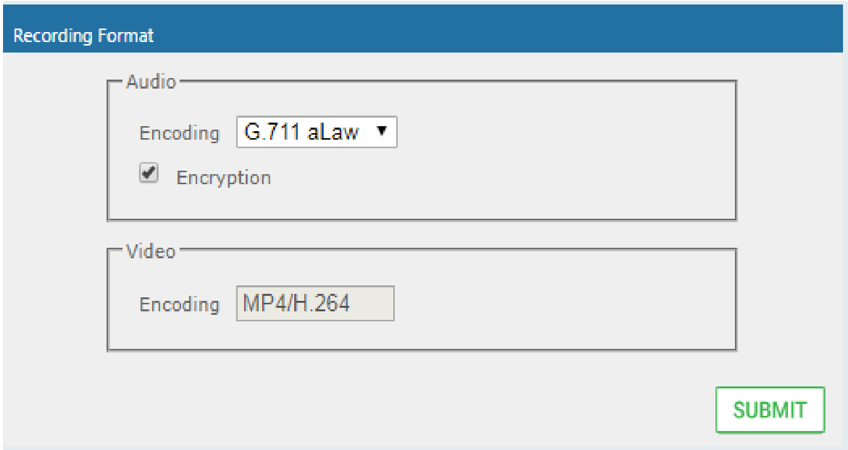
Defining a Recording Format

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 6-48: Recording Format



Recording Format

Audio

Encoding G.711 aLaw ▼

☑ Encryption

Video

Encoding MP4/H.264

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

Table 6-22: Recording Format

Parameter	Description
Audio Encoding	From the drop-down list, choose one of the following: ■ **g711Ulaw** (uncompressed storage) ■ **g711Alaw** (uncompressed storage) ■ **g729** (compressed storage)
	'Encryption' check box: 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 SUBMIT to submit changes.

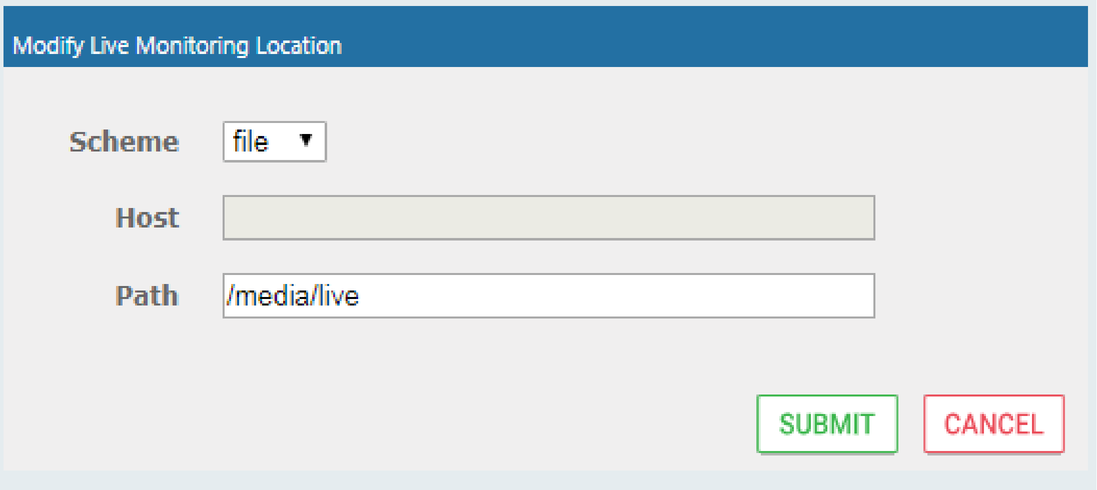
Configure Live Monitoring Location

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 360° client and can be played back by the user by clicking the Live Monitor microphone button (see Determining User/Device Status on page 18).

➢ To configure Live Monitoring file location:

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

Figure 6-49: Modify Live Monitoring Location



Modify Live Monitoring Location

Scheme: file

Host:

Path: /media/live

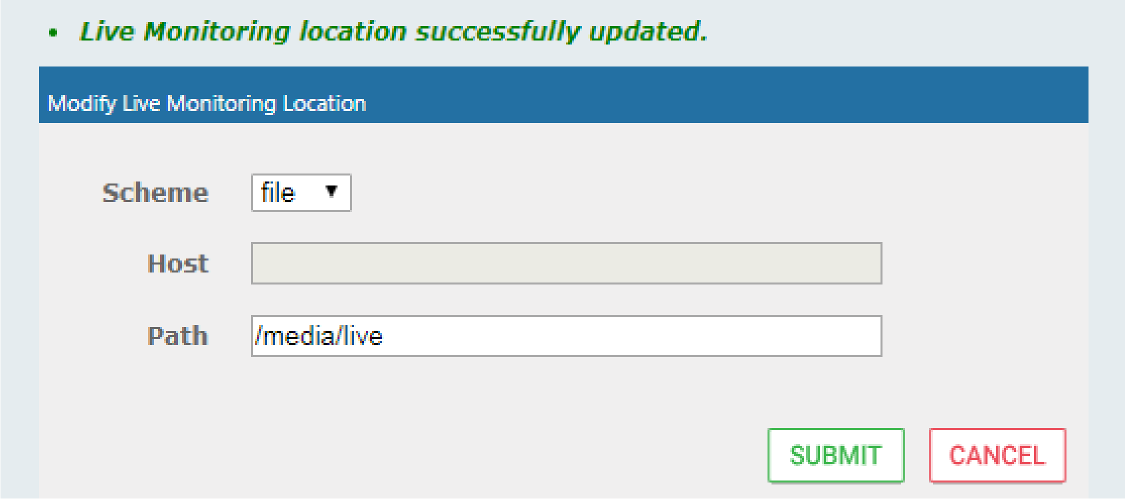
In this page, the following can be configured:

- **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).

> ⚠ 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 Configuring User Credentials on page 65Configuring User Credentials on page 65).

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

Figure 6-50: Modify Live Monitoring Location-Successfully Update



- *Live Monitoring location successfully updated.*

Modify Live Monitoring Location

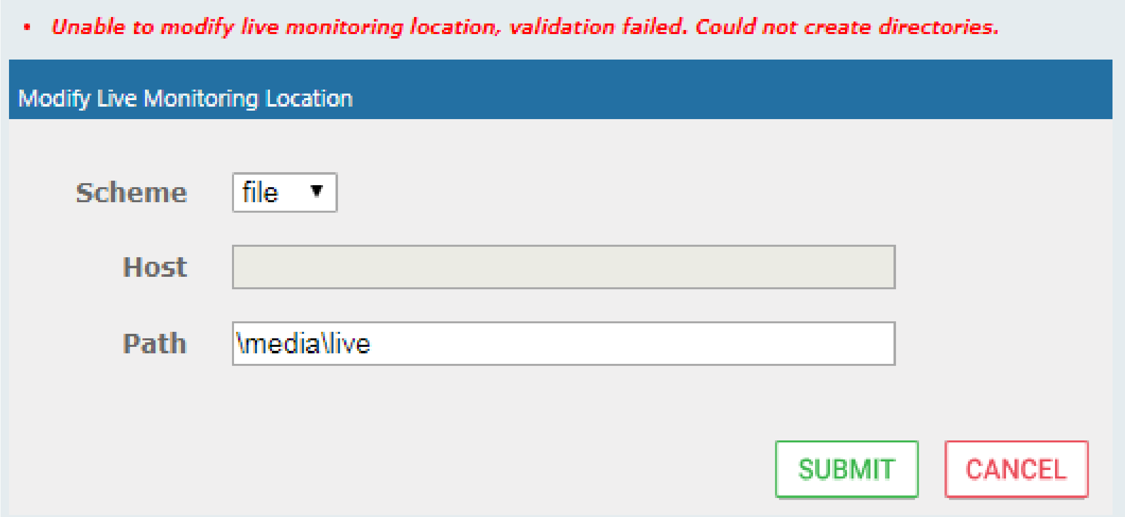
Scheme: file

Host:

Path: /media/live

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

Figure 6-51: Modify Live Monitoring Location-Update Error



- *Unable to modify live monitoring location, validation failed. Could not create directories.*

Modify Live Monitoring Location

Scheme: file

Host:

Path: \media\live

Configuring Single Sign-On

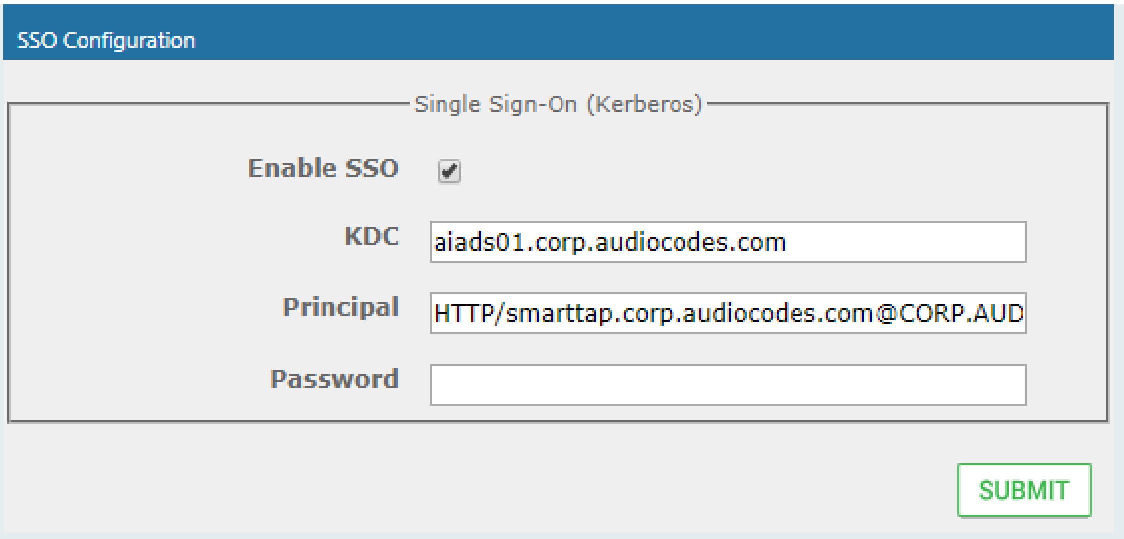
Single Sign-on (SSO) simplifies the login process for domain administrators. The administrator logs into their machine using domain credentials. The user then attempts to access the Application Server's Web service via a Web browser such as IE, Chrome or Firefox. Without SSO, the administrator is directed to a login form where Username and Password are entered and authenticated with the SmartTAP 360° server. When SSO is 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. 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 360°.

⚠ The SmartTAP 360° 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**).

Figure 6-52: Single Sign-On



SSO Configuration

Single Sign-On (Kerberos)

Enable SSO ☑

KDC aiads01.corp.audiocodes.com

Principal HTTP/smarttap.corp.audiocodes.com@CORP.AUD

Password

2. Configure the parameters described in the table below.

Table 6-23: 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 360°.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.

3. When you have completed the configuration click SUBMIT.

4. A status notification indicates that the entries were validated and applied; a popup advises to restart the Application Server for the changes to take effect.

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.

See Searching for Messages on page 188 for other necessary steps to configure SSO.

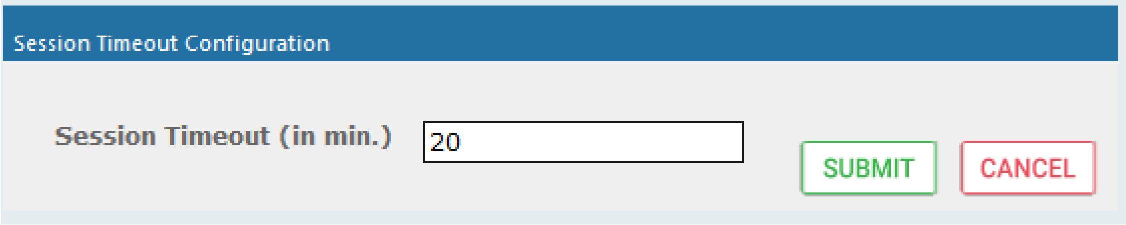
Configuring Web Session Timeout

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 logging in after the configuration 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 > **WEB** folder > **Session Timeout**).

Figure 6-53: Session Timeout



Session Timeout Configuration

Session Timeout (in min.) 20

2. Specify the appropriate Session Timeout.
3. Click SUBMIT to accept changes.

Configuring an LDAP Connection

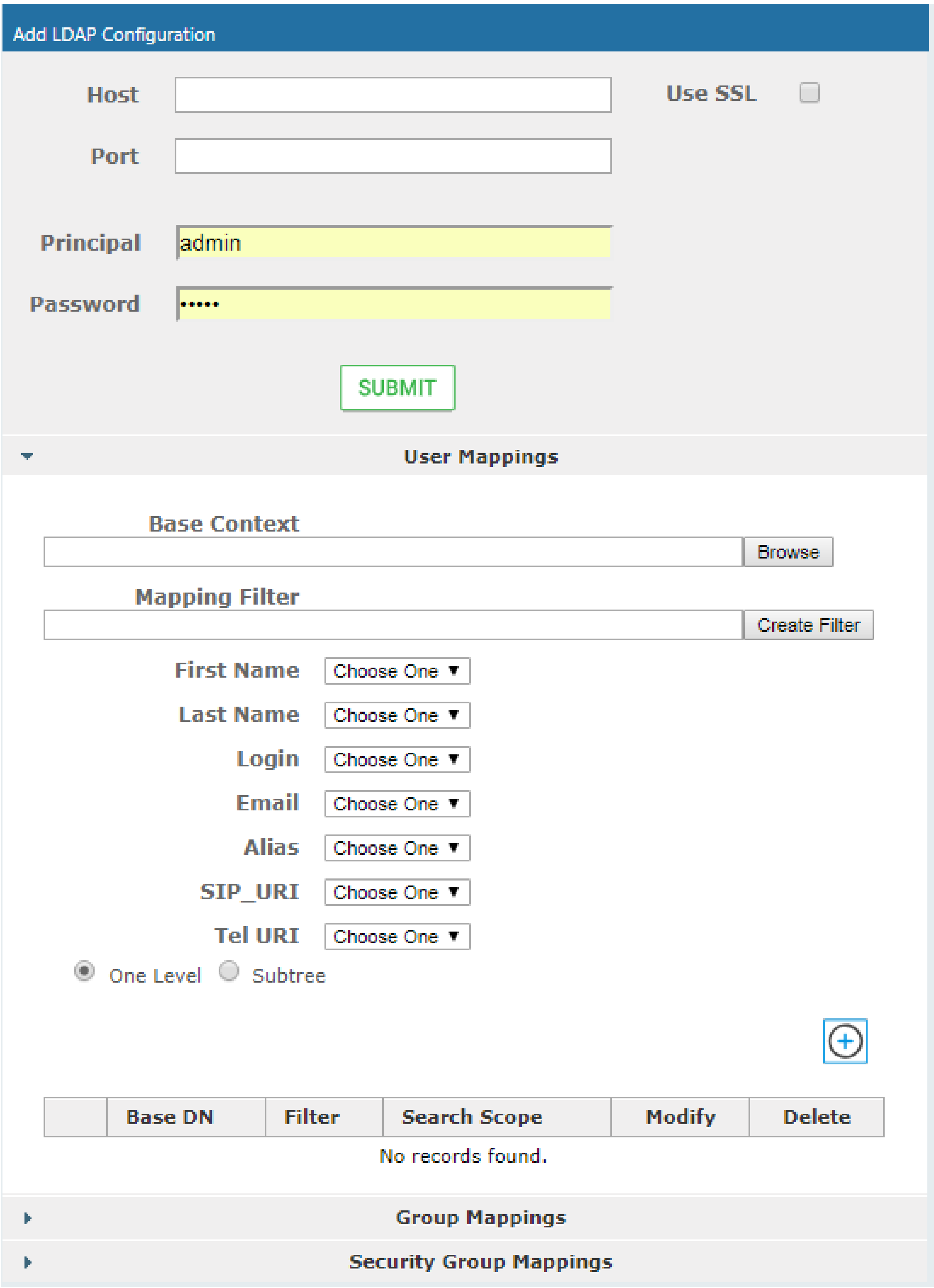
The LDAP Configuration page shown below allows configuration of an LDAP Provider. The information required to connect to the LDAP server, along with the user, group, and security group attribute mappings, are all configured from this page. Once the connection information is correctly entered and submitted,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

⚠ SmartTAP 360° existing local users that match LDAP-obtained users are treated as the same unique user.

➢ To add an LDAP connection:

1. Open the Add LDAP Connection screen (**System** > **LDAP** > **Add LDAP Connection**).

Figure 6-54: LDAP Connection Configuration



Add LDAP Configuration

Host		Use SSL	□
Port			
Principal	admin		
Password	•••••		

First Name	Choose One ▼
Last Name	Choose One ▼
Login	Choose One ▼
Email	Choose One ▼
Alias	Choose One ▼
SIP_URI	Choose One ▼
Tel URI	Choose One ▼

● One Level ○ Subtree

	Base DN	Filter	Search Scope	Modify	Delete

No records found.

2. Use the table as reference to the screen parameters.

Table 6-24: 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	Select this option to secure an SSL connection with the LDAP host. If you select this option, see Configuring SSL below.

➢ 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=A-Administrator,CN=Users,DC=qalabEE,DC=local)

➢ To configure an LDAP connection from SmartTAP 360°:

1. Enter the IP or Name of the domain controller in the 'Host' field.
2. Enter distinguishedName in the 'Principal' field.
3. Enter the Port number in the 'Port' field.
4. Provide the password for the distinguishedName account used.
5. Check 'Use SSL' if required (see Configuring SSL below).
6. Click SUBMIT to apply changes; 'LDAP Provider Configuration successfully saved.' is displayed above the LDAP Configuration screen title bar.

Configuring SSL

This section shows how to enable SSL encryption between SmartTAP 360° and AD for all LDAP transactions.

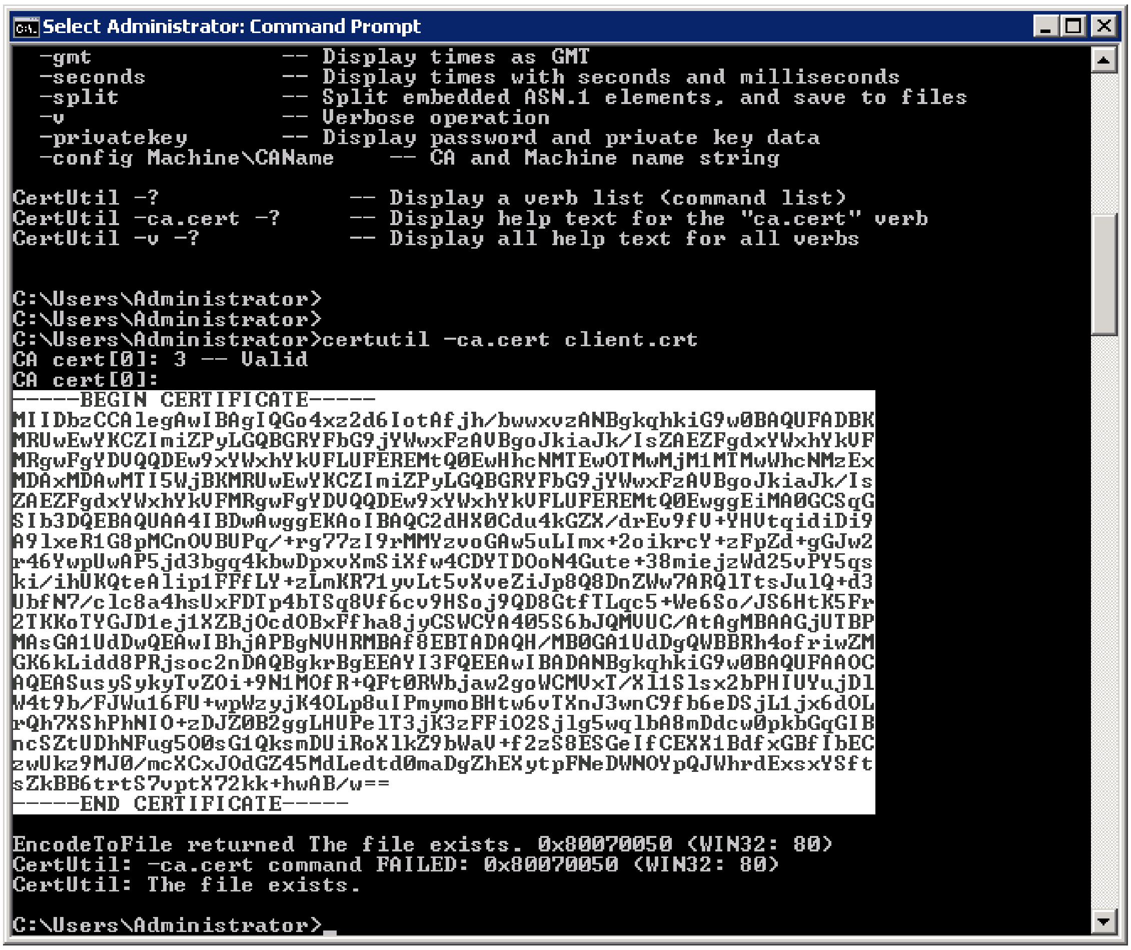
➢ To enable encryption between SmartTAP 360° and AD for all LDAP transactions:

1. On the server that stores 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 360° server, copy from -----BEGIN CERTIFICATE----- to -----END CERTIFICATE----.

Figure 6-55: Copy Client Certificate From Active Directory

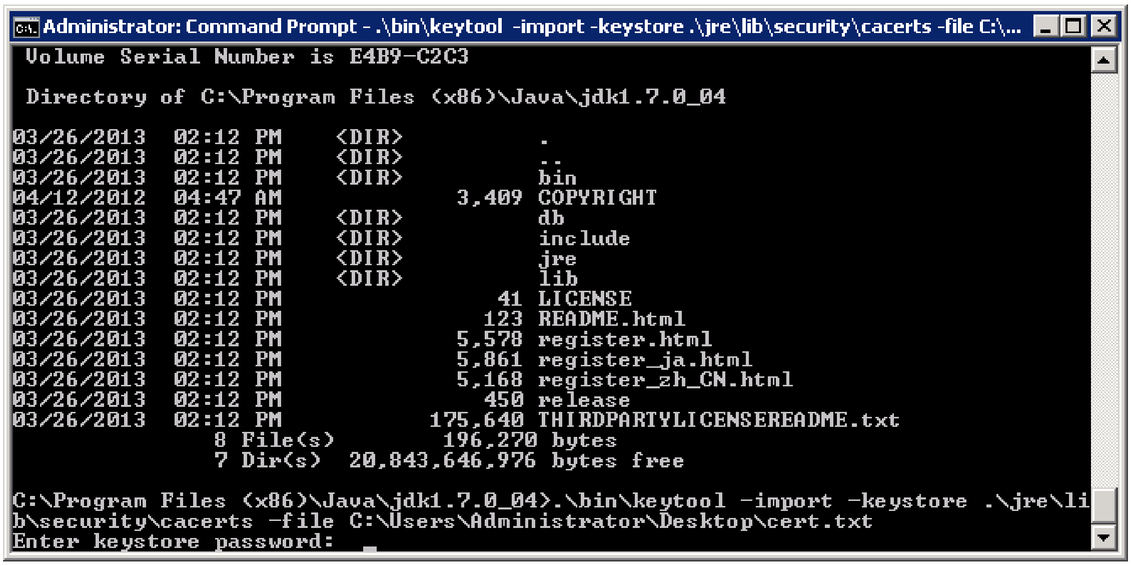


```
  -gmt                  -- Display times as GMT
  -seconds              -- Display times with seconds and milliseconds
  -split                -- Split embedded ASN.1 elements, and save to files
  -v                    -- Verbose operation
  -privatekey           -- Display password and private key data
  -config Machine\CAName     -- CA and Machine name string

CertUtil -?              -- Display a verb list (command list)
CertUtil -ca.cert -?     -- Display help text for the "ca.cert" verb
CertUtil -v -?           -- Display all help text for all verbs


C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>certutil -ca.cert client.crt
CA cert[0]: 3 -- Valid
CA cert[0]:
-----BEGIN CERTIFICATE-----
MIIDbzCCAlegAwIBAgIQGo4xz2d6IotAfjh/bwwxvzANBgkqhkiG9w0BAQUFADBK
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFzAVBgoJkiaJk/IsZAEZFgdxYWxhYkVF
MRgwFgYDVQQDEw9xYWxhYkVFLUFEREMtQ0EwHhcNMTEwOTMwMjM1MTMwWhcNMzEx
MDAxMDAwMTI5WjBKMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFzAVBgoJkiaJk/Is
ZAEZFgdxYWxhYkVFMRgwFgYDVQQDEw9xYWxhYkVFLUFEREMtQ0EwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQC2dHX0Cdu4kGZX/drEv9fV+YHVtqidiDi9
A9lxeR1G8pMCnOVBUPq/+rg77zI9rMMYzvoGAw5uLImx+2oikrcY+zFpZd+gGJw2
r46YwpUwAP5jd3bgq4kbwDpxvXmSiXfw4CDYTDOoN4Gute+38miejzWd25vPY5qs
ki/ihUKQteAlip1FFfLY+zLmKR71yvLt5vXveZiJp8Q8DnZWw7ARQlTtsJulQ+d3
UbfN7/clc8a4hsUxFDTp4bTSq8Vf6cv9HSoj9QD8GtfTLqc5+We6So/JS6HtK5Fr
2TKKoTYGJD1ej1XZBjOcdOBxFfha8jyCSWCYA405S6bJQMVUC/AtAgMBAAGjUTBP
MAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBRh4ofriwZM
GK6kLidd8PRjsoc2nDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQUFAAOC
AQEASusySykyTvZOi+9N1MOfR+QFt0RWbjaw2goWCMVxT/Xl1Slsx2bPHIUYujDl
W4t9b/FJWu16FU+wpWzyjK4OLp8uIPmymoBHtw6vTXnJ3wnC9fb6eDSjL1jx6dOL
rQh7XShPhNIO+zDJZ0B2ggLHUPelT3jK3zFFiO2Sjlg5wqlbA8mDdcw0pkbGqGIB
ncSZtUDhNFug5O0sG1QksmDUiRoXlkZ9bWaV+f2zS8ESGeIfCEXX1BdfxGBfIbEC
zwUkz9MJ0/mcXCxJOdGZ45MdLedtd0maDgZhEXytpFNeDWNOYpQJWhrdExsxYSft
sZkBB6trtS7vptX72kk+hwAB/w==
-----END CERTIFICATE-----

EncodeToFile returned The file exists. 0x80070050 (WIN32: 80)
CertUtil: -ca.cert command FAILED: 0x80070050 (WIN32: 80)
CertUtil: The file exists.

C:\Users\Administrator>_
```

3. Copy client.crt to the SmartTAP 360° machine. From the Java directory (C:\Program Files\Java\<jre_version>\ on SmartTAP 360°) run the following:

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

Figure 6-56: Copy Client Certificate to SmartTAP 360° Machine



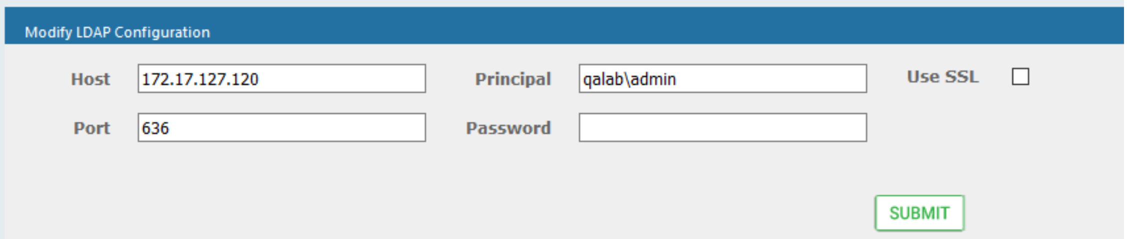
Administrator: Command Prompt - .\bin\keytool -import -keystore .\jre\lib\security\cacerts -file C:\...

```
 Volume Serial Number is E4B9-C2C3

 Directory of C:\Program Files (x86)\Java\jdk1.7.0_04

03/26/2013  02:12 PM    <DIR>          .
03/26/2013  02:12 PM    <DIR>          ..
03/26/2013  02:12 PM    <DIR>          bin
04/12/2012  04:47 AM             3,409 COPYRIGHT
03/26/2013  02:12 PM    <DIR>          db
03/26/2013  02:12 PM    <DIR>          include
03/26/2013  02:12 PM    <DIR>          jre
03/26/2013  02:12 PM    <DIR>          lib
03/26/2013  02:12 PM                41 LICENSE
03/26/2013  02:12 PM               123 README.html
03/26/2013  02:12 PM             5,578 register.html
03/26/2013  02:12 PM             5,861 register_ja.html
03/26/2013  02:12 PM             5,168 register_zh_CN.html
03/26/2013  02:12 PM               450 release
03/26/2013  02:12 PM           175,640 THIRDPARTYLICENSEREADME.txt
               8 File(s)        196,270 bytes
               7 Dir(s)  20,843,646,976 bytes free

C:\Program Files (x86)\Java\jdk1.7.0_04>.\bin\keytool -import -keystore .\jre\li
b\security\cacerts -file C:\Users\Administrator\Desktop\cert.txt
Enter keystore password: _
```

- 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. Restart the SmartTAP 360° Application server for the new certificate to be loaded.
5. The default port for LDAPS (LDAP with SSL support) is 636 (see the figure below).
6. Check the 'Use SSL' checkbox (see the figure below).
7. Click SUBMIT to continue (see the figure below).

Figure 6-57: LDAP SSL Configuration



Modify LDAP Configuration

Host 172.17.127.120 Principal qalab\admin Use SSL □

Port 636 Password

Configuring an LDAP User

This section describes how to map an Active Directory/LDAP user to Microsoft Active Directory. The following entities must be configured:

- User Mappings (Configuring User Mappings on the next page
- Group Mappings (Configuring Group Mappings on page 93
- Security Group Mappings (Configuring Security Group Mappings on page 96

Active Directory/LDAP user mapping is not supported for Microsoft Teams deployments.

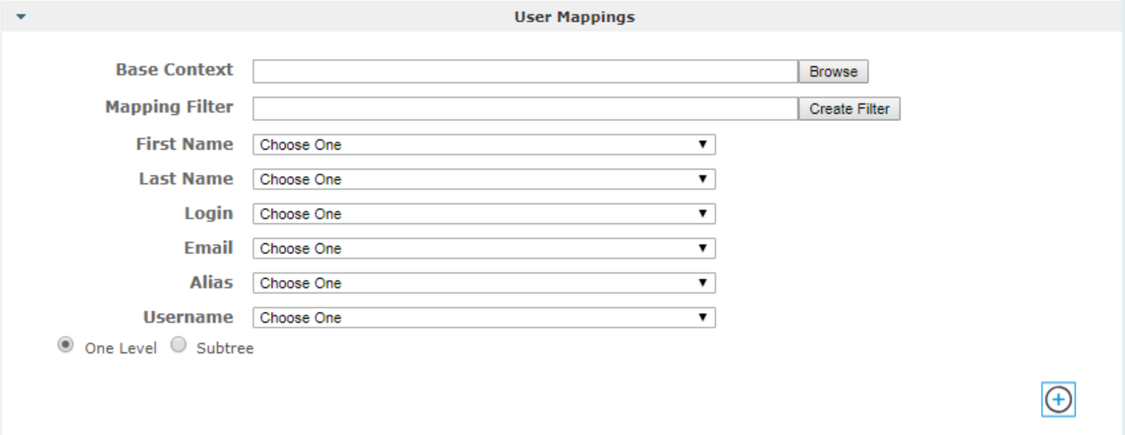
Configuring User Mappings

The procedure below describes how to configure User Mappings.

➢ To configure User Mappings:

1. Open the User Mappings screen shown below.

Figure 6-58: User Mappings



User Mappings

Base Context: [ ] Browse

Mapping Filter: [ ] Create Filter

First Name: Choose One

Last Name: Choose One

Login: Choose One

Email: Choose One

Alias: Choose One

Username: Choose One

● One Level ○ Subtree

2. Use the table below as reference.

Table 6-25: 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

Field	Description
	🟦 ▼ = shrink screen

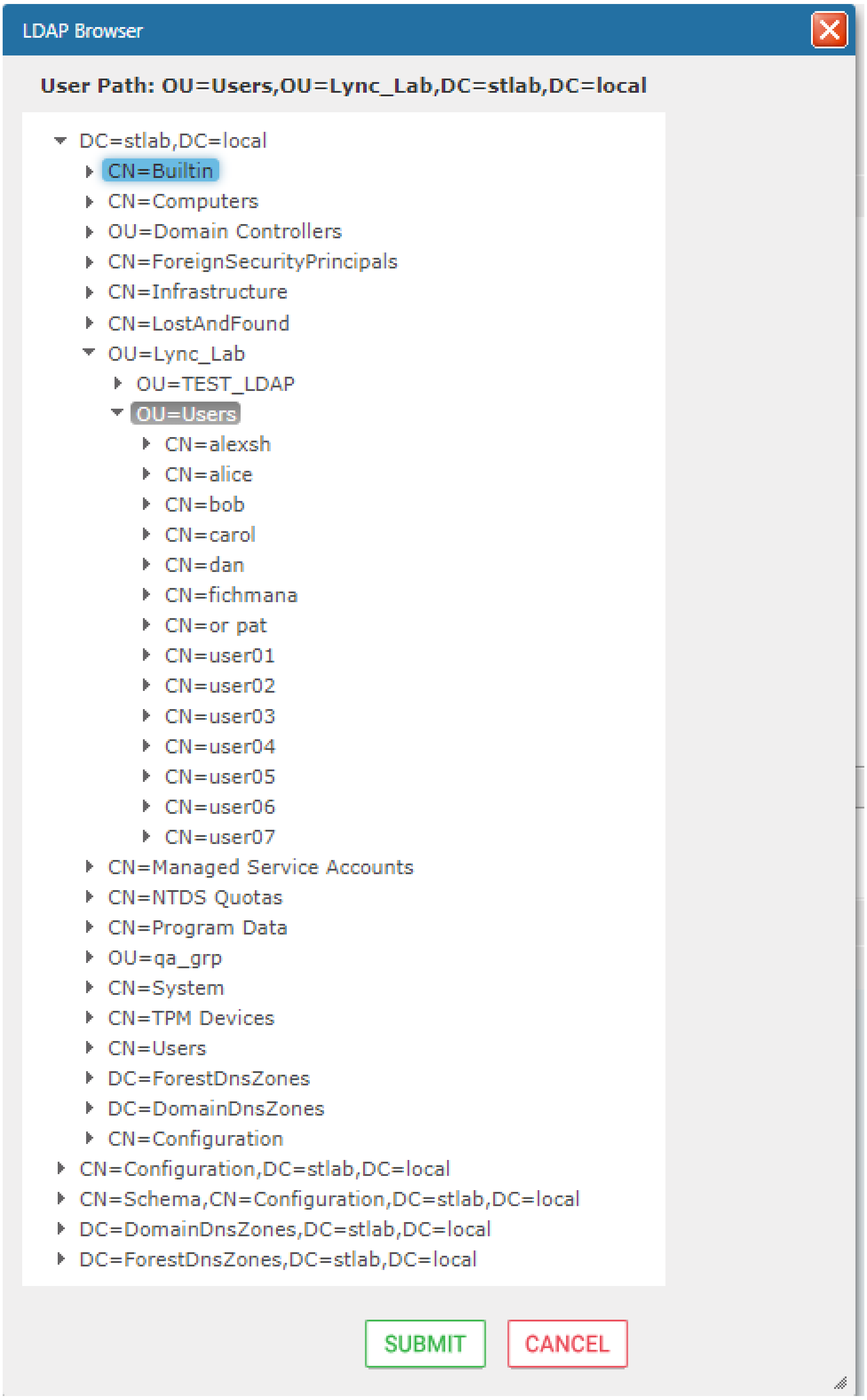
3. Enter the User Mappings Information in the 'User Mappings' screen (click ► if necessary to expand the screen).

4. The default user location in Windows is displayed as follows:

   OU=Ai-Logix,OU=USA,OU=AudioCodes,DC=corp,DC=audiocodes,DC=com

5. Click **Browse** and navigate to the appropriate OU.

Figure 6-59: LDAP Browser



User Path: OU=Users,OU=Lync_Lab,DC=stlab,DC=local

- DC=stlab,DC=local
    - CN=Builtin
    - CN=Computers
    - OU=Domain Controllers
    - CN=ForeignSecurityPrincipals
    - CN=Infrastructure
    - CN=LostAndFound
    - OU=Lync_Lab
        - OU=TEST_LDAP
        - OU=Users
            - CN=alexsh
            - CN=alice
            - CN=bob
            - CN=carol
            - CN=dan
            - CN=fichmana
            - CN=or pat
            - CN=user01
            - CN=user02
            - CN=user03
            - CN=user04
            - CN=user05
            - CN=user06
            - CN=user07
    - CN=Managed Service Accounts
    - CN=NTDS Quotas
    - CN=Program Data
    - OU=qa_grp
    - CN=System
    - CN=TPM Devices
    - CN=Users
    - DC=ForestDnsZones
    - DC=DomainDnsZones
    - CN=Configuration
- CN=Configuration,DC=stlab,DC=local
- CN=Schema,CN=Configuration,DC=stlab,DC=local
- DC=DomainDnsZones,DC=stlab,DC=local
- DC=ForestDnsZones,DC=stlab,DC=local

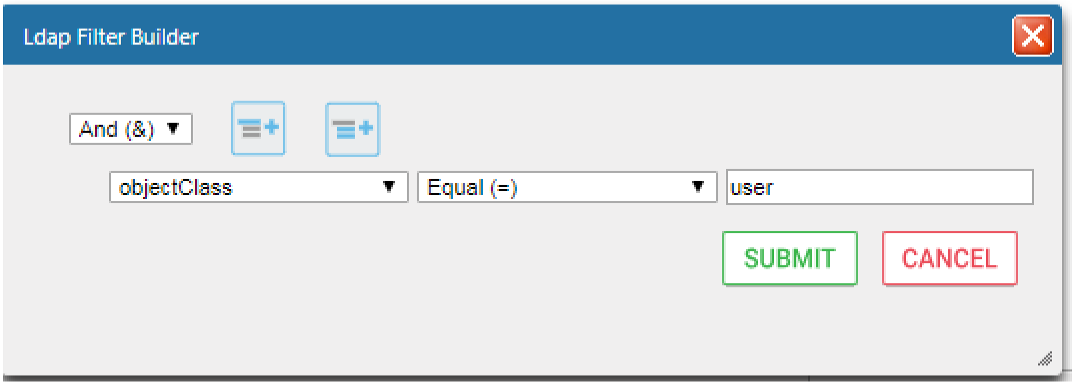
6. Navigate to the appropriate 'User Path' and then click SUBMIT.

7. Use filtering if you prefer not to add all users.

➢ To add a filter:

1. Select the **Create Filter** button.
2. Select the appropriate Conditional Operator (And, Or, Not)
3. Select the appropriate Attribute
4. Select the appropriate Equality Operator (>=, =, ~=, <=)
5. Specify value = (objectClass = user) recommended
6. Click SUBMIT to apply changes.
7. Click the ≡+ icon to add an additional filter condition and repeat above filter steps.
8. Click the ≡+ icon to add a new Sub filter and repeat above filter steps.

Figure 6-60: LDAP Filter Builder Example



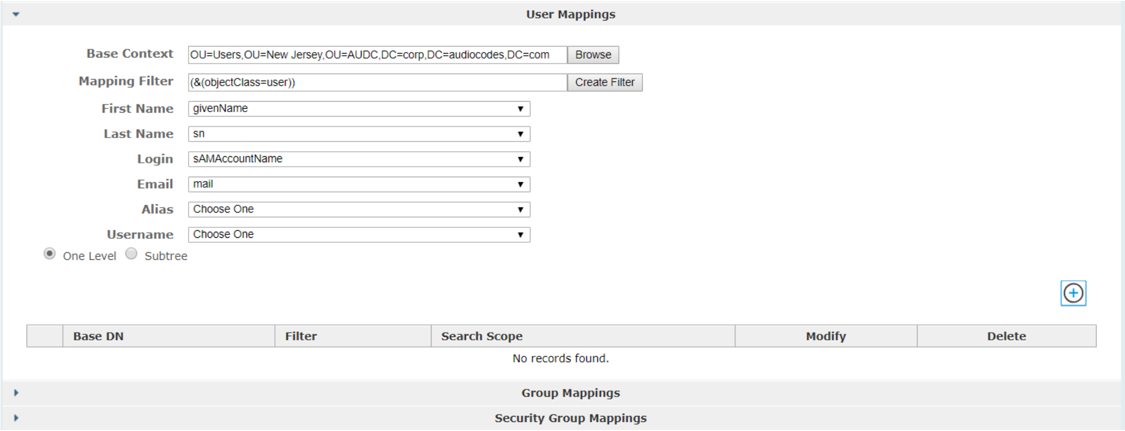
Ldap Filter Builder

And (&) ▼

objectClass ▼ | Equal (=) ▼ | user

9. Scroll through the list and select the First Name, Last Name, Login, Email and Alias user attributes:
   - If you created any SmartTAP 360° 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 360° User attributes added for recording purposes.
10. Map SmartTAP 360° attributes to appropriate AD user attributes.

Figure 6-61: User Filtering Screen



User Mappings

Base Context: OU=Users,OU=New Jersey,OU=AUDC,DC=corp,DC=audiocodes,DC=com [Browse]

Mapping Filter: (&(objectClass=user)) [Create Filter]

First Name: givenName

Last Name: sn

Login: sAMAccountName

Email: mail

Alias: Choose One

Username: Choose One

● One Level ○ Subtree

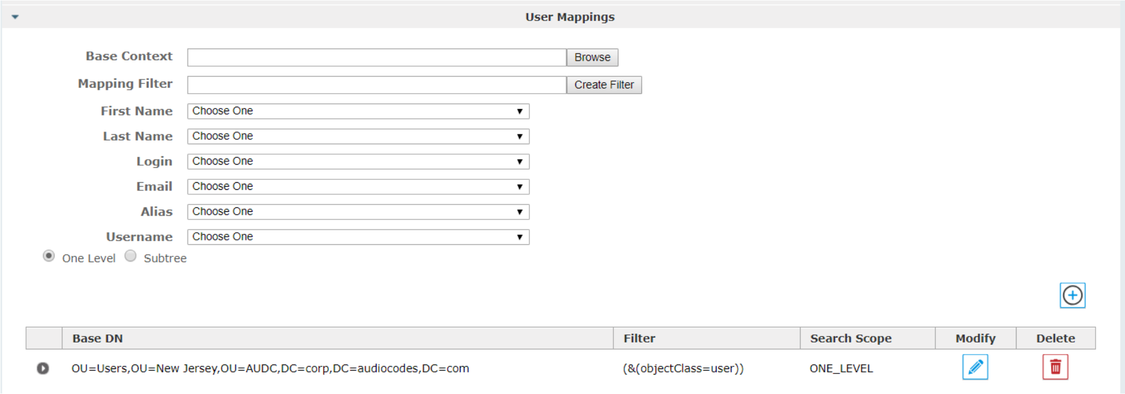
	Base DN	Filter	Search Scope	Modify	Delete
	No records found.				

Group Mappings

Security Group Mappings

11. Click ⊕ to apply changes.

Figure 6-62: User Mapping Configured



User Mappings

Base Context: [Browse]

Mapping Filter: [Create Filter]

First Name: Choose One

Last Name: Choose One

Login: Choose One

Email: Choose One

Alias: Choose One

Username: Choose One

● One Level ○ Subtree

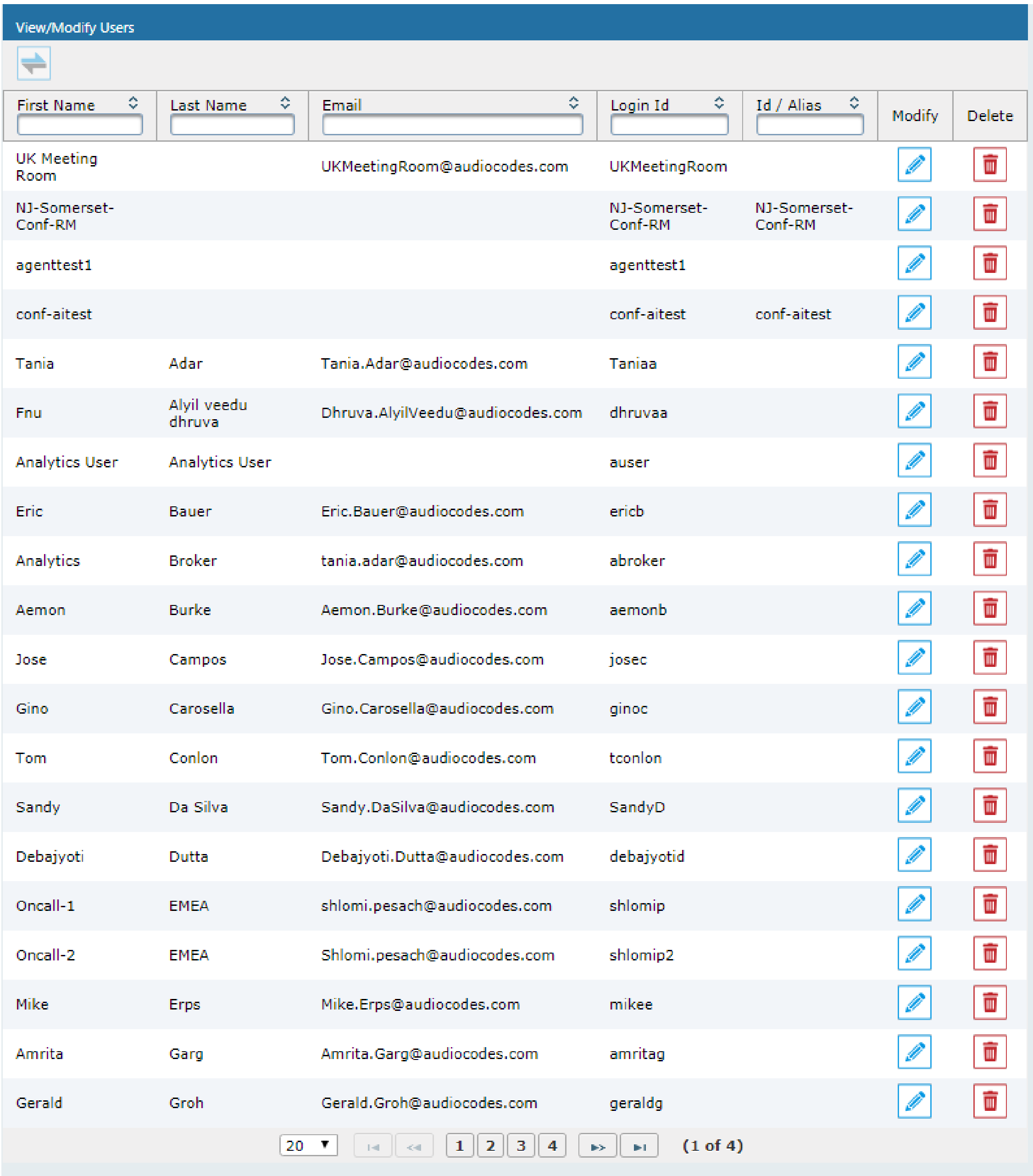
	Base DN	Filter	Search Scope	Modify	Delete
●	OU=Users,OU=New Jersey,OU=AUDC,DC=corp,DC=audiocodes,DC=com	(&(objectClass=user))	ONE_LEVEL	✎	🗑

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

13. Add additional User Mappings as needed.

14. Go to the User tab (**Users** > **User Management** > **View/Modify Users**) to see the list of users added from the Active Directory.

Figure 6-63: View/Modify Users



View/Modify Users

First Name	Last Name	Email	Login Id	Id / Alias	Modify	Delete
UK Meeting Room		UKMeetingRoom@audiocodes.com	UKMeetingRoom		✎	🗑
NJ-Somerset-Conf-RM			NJ-Somerset-Conf-RM	NJ-Somerset-Conf-RM	✎	🗑
agenttest1			agenttest1		✎	🗑
conf-aitest			conf-aitest	conf-aitest	✎	🗑
Tania	Adar	Tania.Adar@audiocodes.com	Taniaa		✎	🗑
Fnu	Alyil veedu dhruva	Dhruva.AlyilVeedu@audiocodes.com	dhruvaa		✎	🗑
Analytics User	Analytics User		auser		✎	🗑
Eric	Bauer	Eric.Bauer@audiocodes.com	ericb		✎	🗑
Analytics	Broker	tania.adar@audiocodes.com	abroker		✎	🗑
Aemon	Burke	Aemon.Burke@audiocodes.com	aemonb		✎	🗑
Jose	Campos	Jose.Campos@audiocodes.com	josec		✎	🗑
Gino	Carosella	Gino.Carosella@audiocodes.com	ginoc		✎	🗑
Tom	Conlon	Tom.Conlon@audiocodes.com	tconlon		✎	🗑
Sandy	Da Silva	Sandy.DaSilva@audiocodes.com	SandyD		✎	🗑
Debajyoti	Dutta	Debajyoti.Dutta@audiocodes.com	debajyotid		✎	🗑
Oncall-1	EMEA	shlomi.pesach@audiocodes.com	shlomip		✎	🗑
Oncall-2	EMEA	Shlomi.pesach@audiocodes.com	shlomip2		✎	🗑
Mike	Erps	Mike.Erps@audiocodes.com	mikee		✎	🗑
Amrita	Garg	Amrita.Garg@audiocodes.com	amritag		✎	🗑
Gerald	Groh	Gerald.Groh@audiocodes.com	geraldg		✎	🗑

20 ▼ 1 2 3 4 (1 of 4)

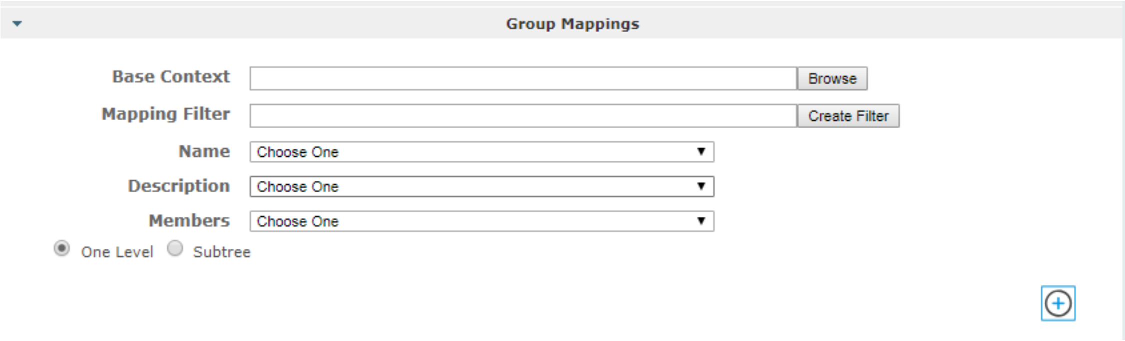
Configuring Group Mappings

The procedure below describes how to configure Group Mappings.

➢ To configure Group Mappings:

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

Figure 6-64: Group Mappings



▼ Group Mappings

Base Context [ ] Browse

Mapping Filter [ ] Create Filter

Name: Choose One ▼

Description: Choose One ▼

Members: Choose One ▼

● One Level ○ Subtree

⊕

3. Use the table below as reference.

Table 6-26: 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.

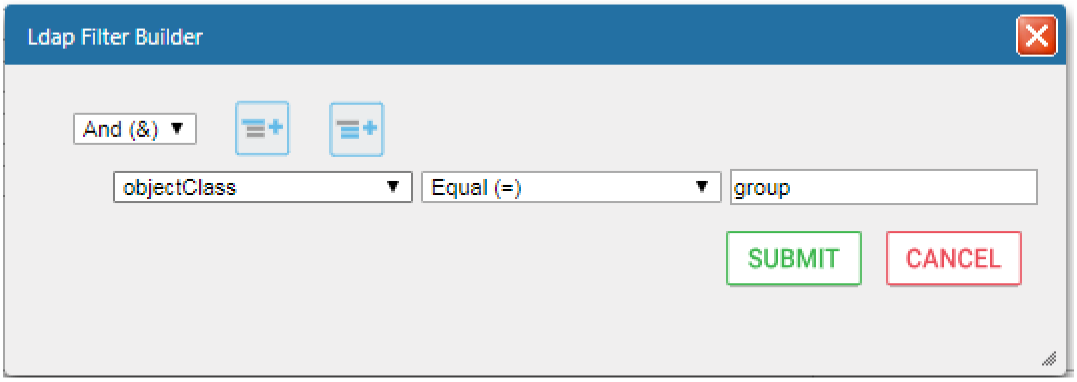
6. Use filtering if you prefer not to add all groups.

➢ To add a Group Filter:

1. Select the appropriate Conditional Operator (And, Or, Not).
2. Select the appropriate Attribute.
3. Select the appropriate Equality Operator (>=, =, ~=, <=).
4. Specify a value.

5. Click SUBMIT to apply changes.

Figure 6-65: Group Filter



Ldap Filter Builder

And (&) ▼ ≡+ ≡+

objectClass ▼ | Equal (=) ▼ | group

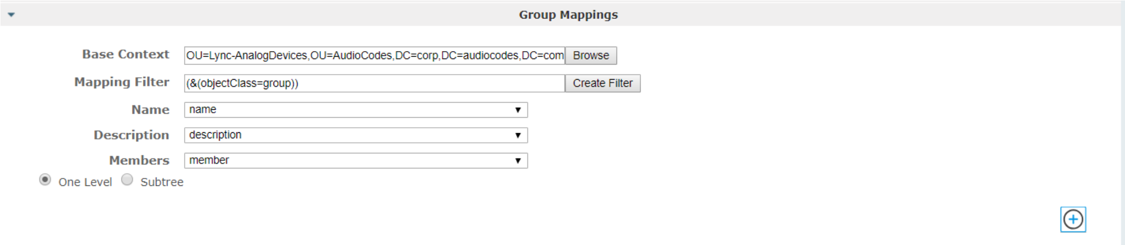
6. Click the ≡+ icon to add an additional filter condition and repeat above filter steps.

7. Click the ≡+ icon to add a new Sub filter and repeat above filter steps.

8. Click SUBMIT to apply changes.

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

Figure 6-66: Group Filtering Screen



Group Mappings

Base Context: OU=Lync-AnalogDevices,OU=AudioCodes,DC=corp,DC=audiocodes,DC=com Browse

Mapping Filter: (&(objectClass=group)) Create Filter

Name: name ▼

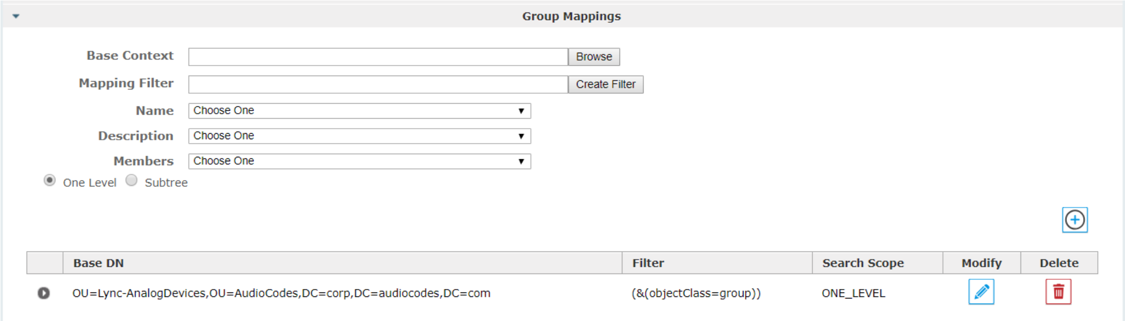
Description: description ▼

Members: member ▼

● One Level ○ Subtree

10. Click ⊕ to apply changes; view the listed group in the table .

Figure 6-67: Group Mapping Configured



Group Mappings

Base Context: Browse

Mapping Filter: Create Filter

Name: Choose One ▼

Description: Choose One ▼

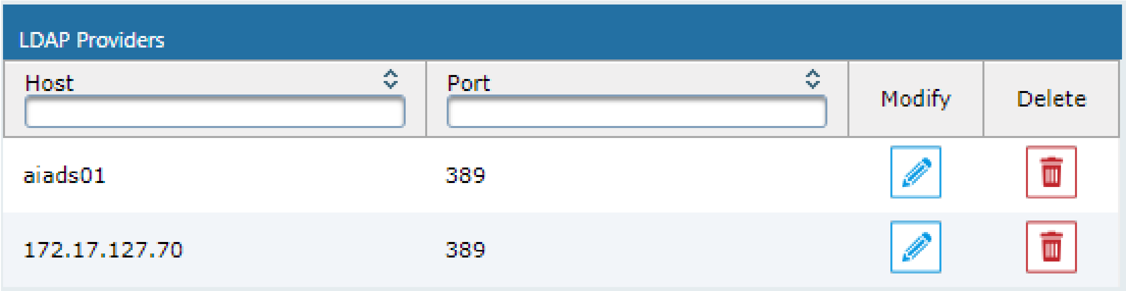
Members: Choose One ▼

● One Level ○ Subtree

	Base DN	Filter	Search Scope	Modify	Delete
●	OU=Lync-AnalogDevices,OU=AudioCodes,DC=corp,DC=audiocodes,DC=com	(&(objectClass=group))	ONE_LEVEL	✎	🗑

11. Select the **Group Mapping** tab page 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 6-68: View/Modify Groups



LDAP Providers

Host	Port	Modify	Delete
aiads01	389		
172.17.127.70	389		

Configuring Security Group Mappings

This section shows how to configure Security Group Mappings. All mapped Active Directory security groups automatically become SmartTAP 360° Security Profiles.

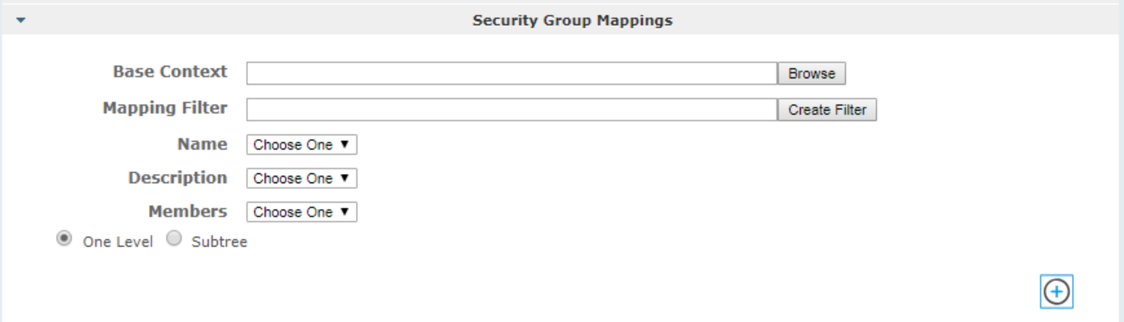
By default, new security profiles are granted no SmartTAP 360° permissions.

➢ To configure Security Group Mappings:

1. Open the Add LDAP Config screen (**System** tab > **LDAP** folder > **Add LDAP Config**).

2. Open the Security Group Mappings screen (click ► if necessary to expand the screen).

Figure 6-69: Security Group Mappings



Security Group Mappings

Base Context [ ] Browse

Mapping Filter [ ] Create Filter

Name Choose One ▼

Description Choose One ▼

Members Choose One ▼

● One Level ○ Subtree

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

Table 6-27: 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

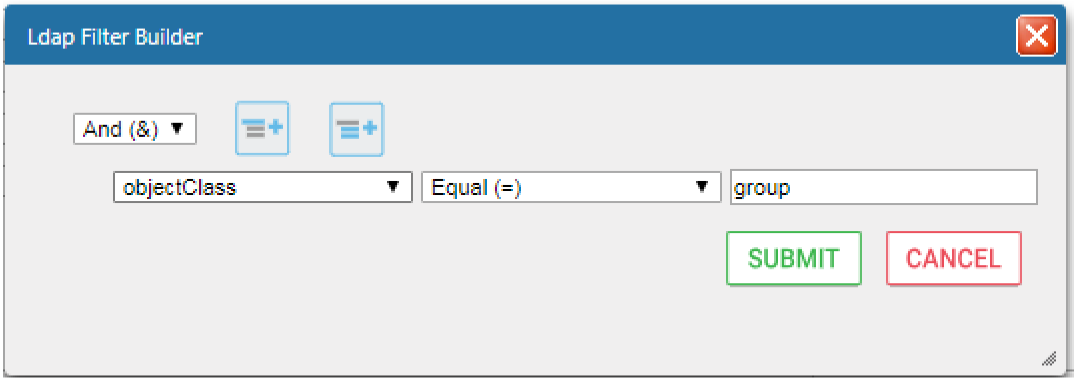
Field	Description
	users that belong to the group.) ■ One Level -Retrieves LDAP attributes for the selected node. ■ Subtree – Retrieves LDAP attributes for the selected node and all its child nodes in the LDAP directory tree. ■ Expand or Shrink screen

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

➢ To add a Security Group Filter:

1. Select the appropriate Conditional Operator (And, Or, Not).
2. Select the appropriate Attribute.
3. Select the appropriate Equality Operator (>=, =, ~=, <=).
4. Specify a value.
5. Click SUBMIT to apply changes.

Figure 6-70: Security Group Filter



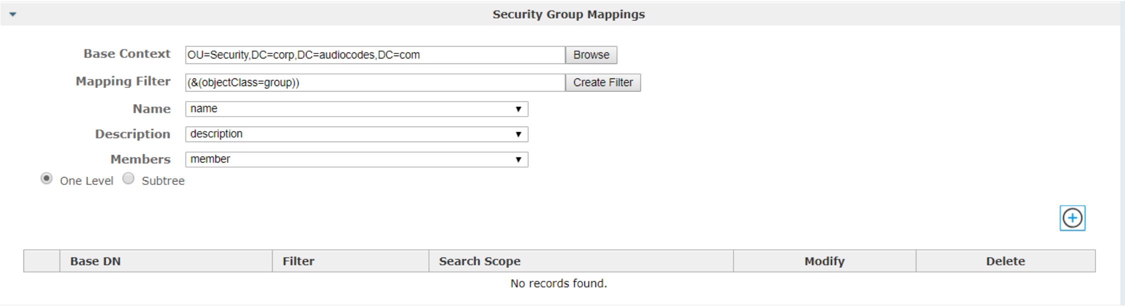
Ldap Filter Builder

And (&) ▼

objectClass ▼ Equal (=) ▼ group

6. Click the ≡+ icon to add an additional filter condition and repeat above filter steps
7. Click the ≡+ icon to add a new Sub filter and repeat above filter steps
8. Click SUBMIT to apply changes.

Figure 6-71: Security Group Filtering Screen



Security Group Mappings

Base Context: OU=Security,DC=corp,DC=audiocodes,DC=com [Browse]

Mapping Filter: (&(objectClass=group)) [Create Filter]

Name: name

Description: description

Members: member

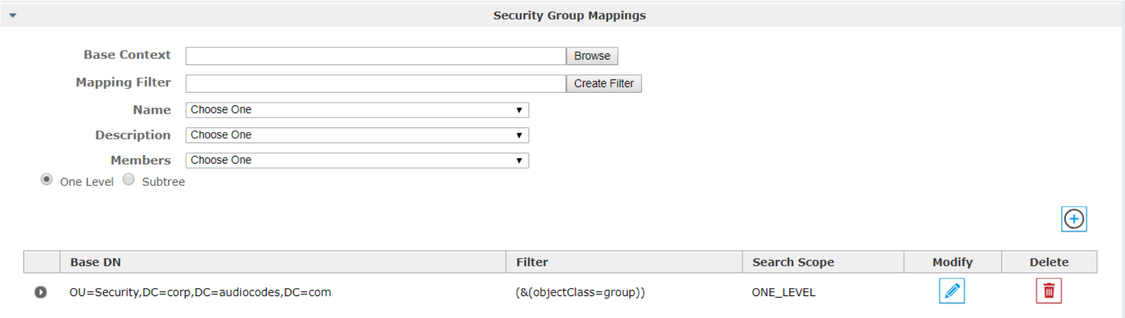
● One Level ○ Subtree

	Base DN	Filter	Search Scope	Modify	Delete

No records found.

9. Click ⊕ to apply changes.

Figure 6-72: Security Group Configured



Security Group Mappings

Base Context: [Browse]

Mapping Filter: [Create Filter]

Name: Choose One

Description: Choose One

Members: Choose One

● One Level ○ Subtree

	Base DN	Filter	Search Scope	Modify	Delete
●	OU=Security,DC=corp,DC=audiocodes,DC=com	(&(objectClass=group))	ONE_LEVEL	✎	🗑

10. Click ⊕ to easily add additional Security Group Mappings.

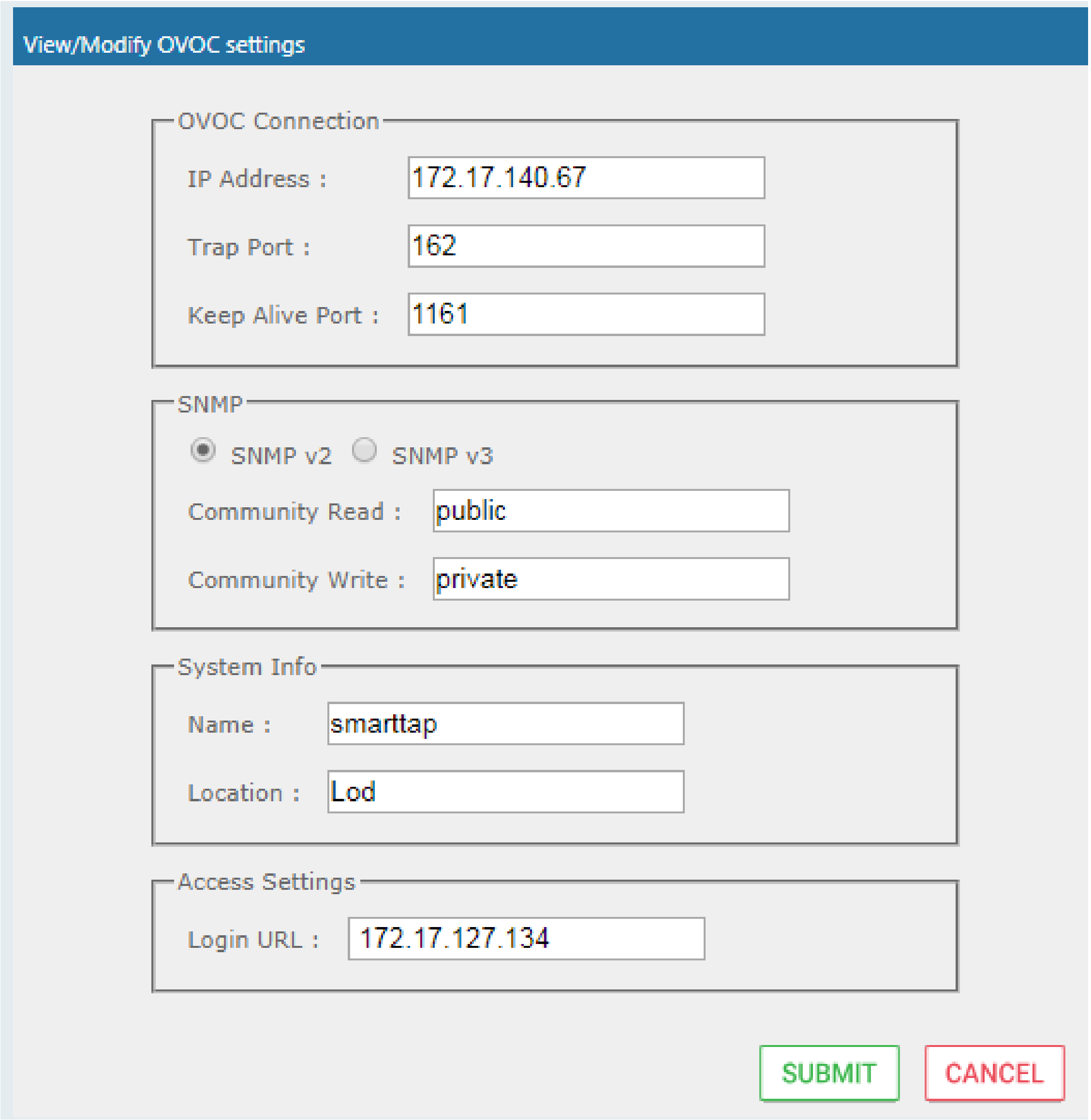
Configuring OVOC Connection

This section describes how to setup the connection to the OVOC server. SmartTAP 360° is managed under AudioCodes One Voice Operations Center in a similar way to other entities that are managed by OVOC (e.g. devices, endpoints and links). This includes the aggregation of alarms and statuses that are raised by the SmartTAP 360° components and forwarded to OVOC from the SmartTAP 360° Application server. OVOC Agents are installed on the SmartTAP 360° Application server for this purpose (for details, refer to the *SmartTAP 360° Installation Guide*).

➢ To configure the connection with the OVOC server:

1. Open the OVOC Settings screen (**System** tab > **Monitoring** > **OVOC**).

Figure 6-73: OVOC Settings



View/Modify OVOC settings

OVOC Connection

IP Address : 172.17.140.67

Trap Port : 162

Keep Alive Port : 1161

SNMP

● SNMP v2 ○ SNMP v3

Community Read : public

Community Write : private

System Info

Name : smarttap

Location : Lod

Access Settings

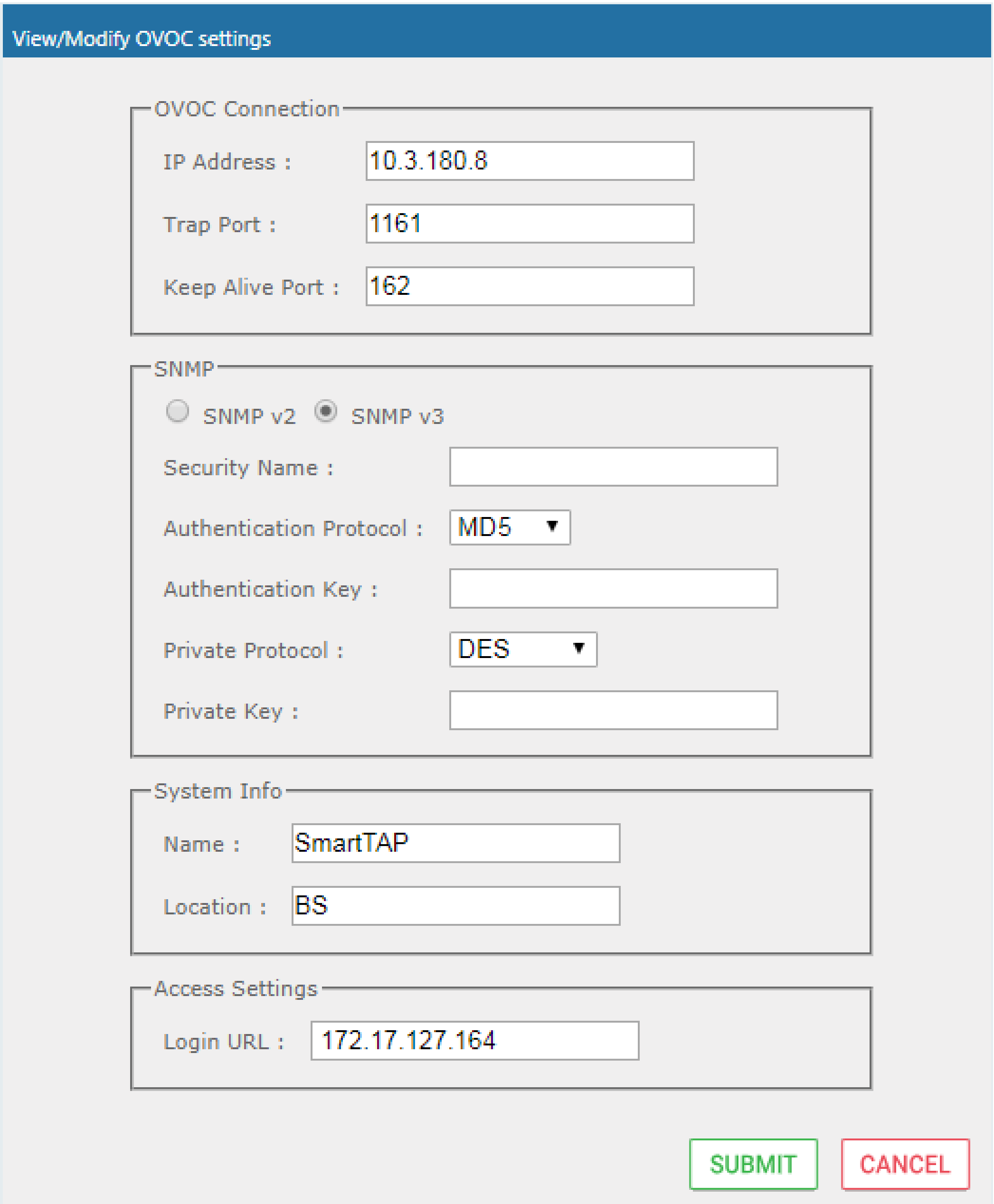
Login URL : 172.17.127.134

2. Configure the following settings:
   - OVOC IP Address
   - Trap Port
   - Keep-alive Port
3. Configure the SNMPv2 community strings:
   - SNMPv2 Community Read string
   - SNMPv2 Community Write string
4. Configure SNMPv3 settings:
   - Security Name-Security Name of the SNMPv3 operator
   - Authentication Protocol-the SNMPv3 authentication protocol (SHA or MD5)
   - Authentication Key- the authentication password.

- Private Protocol-the SNMPv3 privacy protocol (AES 128 or DES)
- Private Key-the private key

The SNMPv2 and SNMPv3 settings should be identically configured on both SmartTAP 360° and the OVOC server.

Figure 6-74: SNMPv3 Settings



View/Modify OVOC settings

OVOC Connection

IP Address : 10.3.180.8

Trap Port : 1161

Keep Alive Port : 162

SNMP

○ SNMP v2 ● SNMP v3

Security Name :

Authentication Protocol : MD5

Authentication Key :

Private Protocol : DES

Private Key :

System Info

Name : SmartTAP

Location : BS

Access Settings

Login URL : 172.17.127.164

5. Configure System Information:
    - Name
    - Location

- Login URL- this login is used for logging into the SmartTAP 360° Web interface from OVOC (Device Information Page)

Managing Users

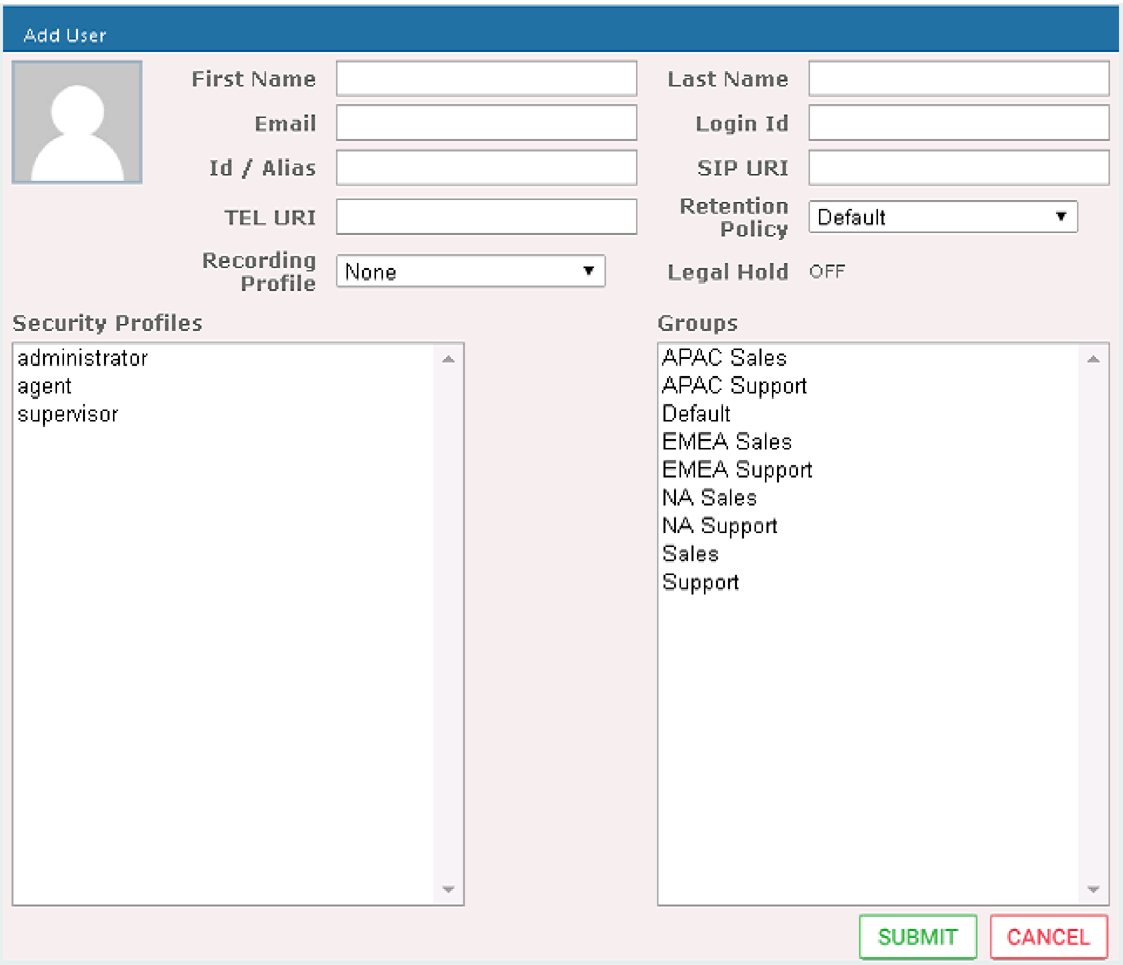
This section shows how to perform user management. This section describes the following:

- Adding a user (see below)
- View and Modify Users on page 130
- Update an Admin User on page 131
- Reset User Password on page 132
- Modify a User Password on page 132
- Uploading an Image on page 133

➢ To add a user:

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

Figure 6-75: Adding a User



Retention Policy: Default

Recording Profile: None

Legal Hold: OFF

Security Profiles:
administrator
agent
supervisor

Groups:
APAC Sales
APAC Support
Default
EMEA Sales
EMEA Support
NA Sales
NA Support
Sales
Support

2. Enter the user's First Name.

3. Enter the user's Last Name.
4. Optionally enter the user's email (SmartTAP 360° 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.

    If SmartTAP 360° is configured for LDAP, any SmartTAP 360° attributes mapped to AD attributes will be auto populated.

11. 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 360° sends an email to the user with their login and initial password, assuming that an email was provided.
12. Use the table below as reference.

Table 6-28: 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.
Recording Profile	Select an appropriate recording profile for the user.
Security	Lists the Security Profiles that can be assigned to the user. Highlighted items

Field	Description
Profiles	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 or messages when the user is placed on legal hold. This feature is only available when modifying a user.
SUBMIT	Apply the changes.
CANCEL	Cancel the changes.

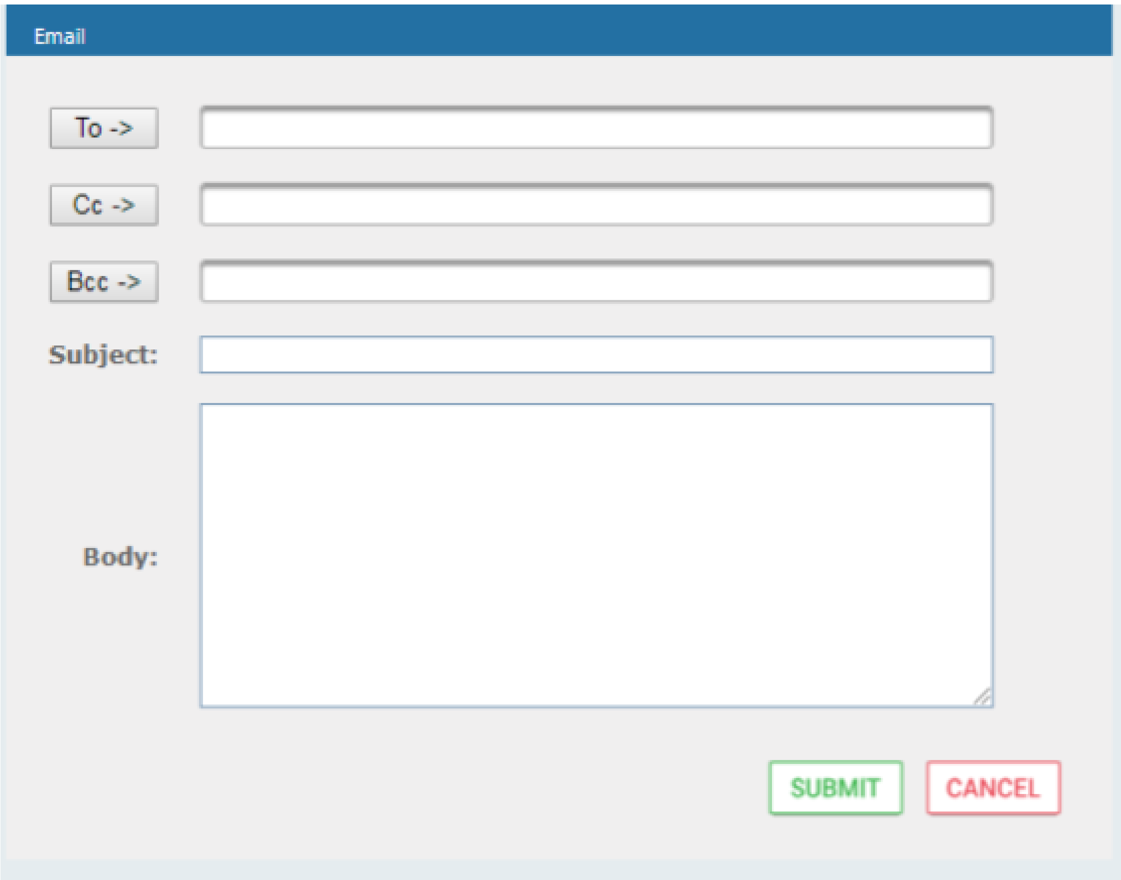
Sending Email

The Email screen allows the network administrator to send emails directly from the SmartTAP 360° Web interface.

➢ To send an Email:

1. Open the Email screen.

Figure 6-76: Email



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

Table 6-29: 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.

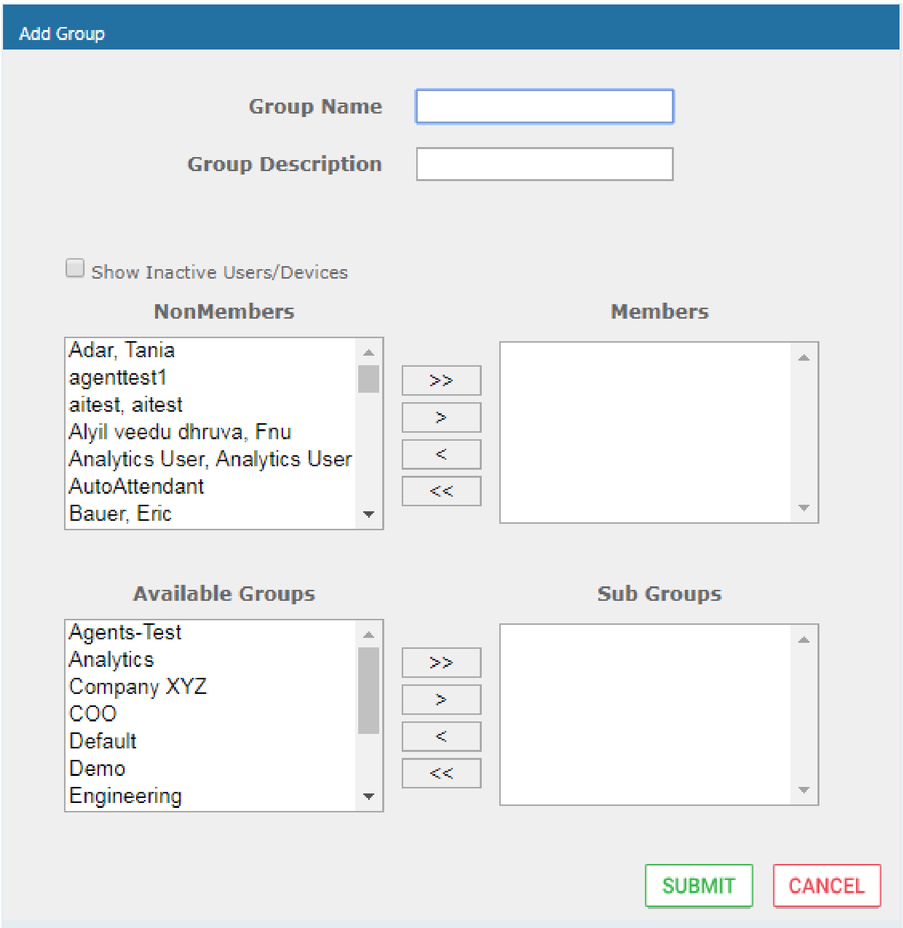
Managing Groups

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 (**Users** tab > **Group Management** folder > **Add Group**).

Figure 6-77: Add Group



Use the table below as reference.

Table 6-30: Group Screen Settings

Field	Description
Group Name	Name of group to add.
Group	Description of the group to add.

Field	Description
Description	
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.
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 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.

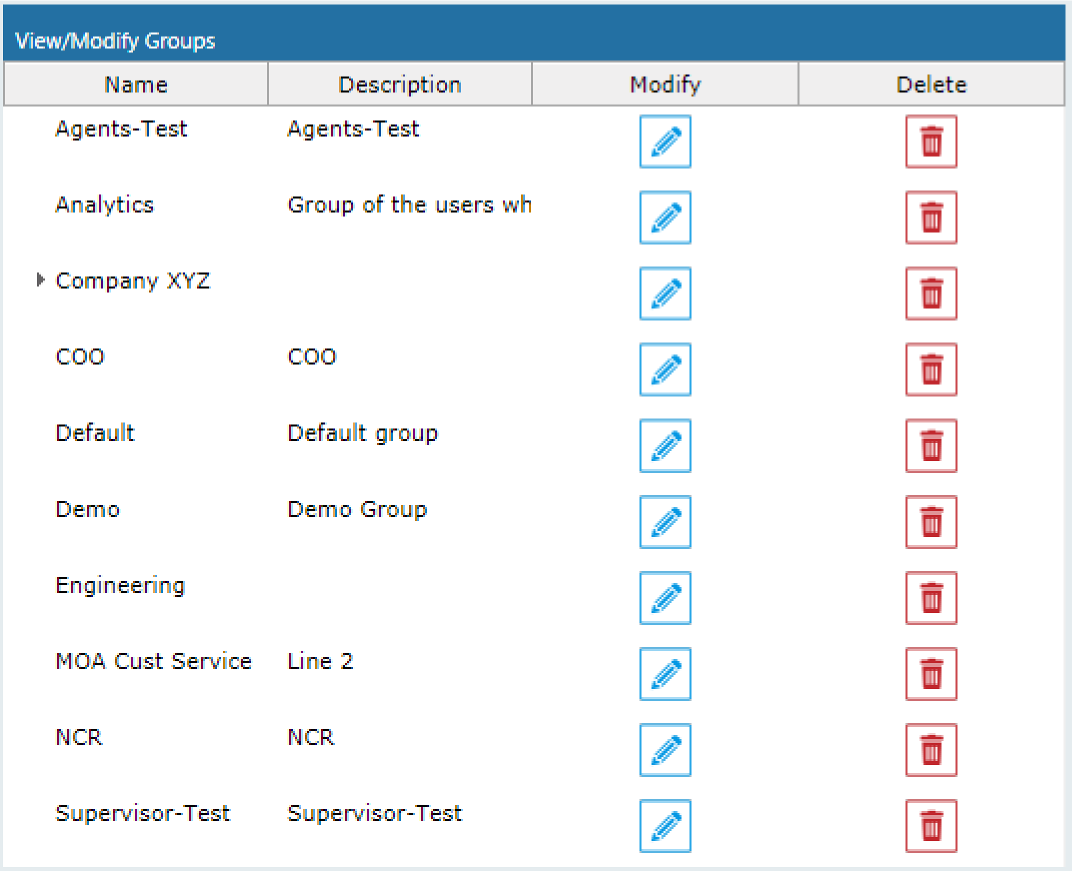
5. (Optionally, Sub Groups for the Group just being added can be entered from the Add Group screen).

6. Click SUBMIT.

➢ To view/modify a Group:

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

Figure 6-78: View/Modify Group



View/Modify Groups

Name	Description	Modify	Delete
Agents-Test	Agents-Test	✎	🗑
Analytics	Group of the users wh	✎	🗑
▸ Company XYZ		✎	🗑
COO	COO	✎	🗑
Default	Default group	✎	🗑
Demo	Demo Group	✎	🗑
Engineering		✎	🗑
MOA Cust Service	Line 2	✎	🗑
NCR	NCR	✎	🗑
Supervisor-Test	Supervisor-Test	✎	🗑

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

Figure 6-79: 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
✎	Click to modify the group.
🗑	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 SUBMIT to apply changes, or click the 🗑 button to delete the group.

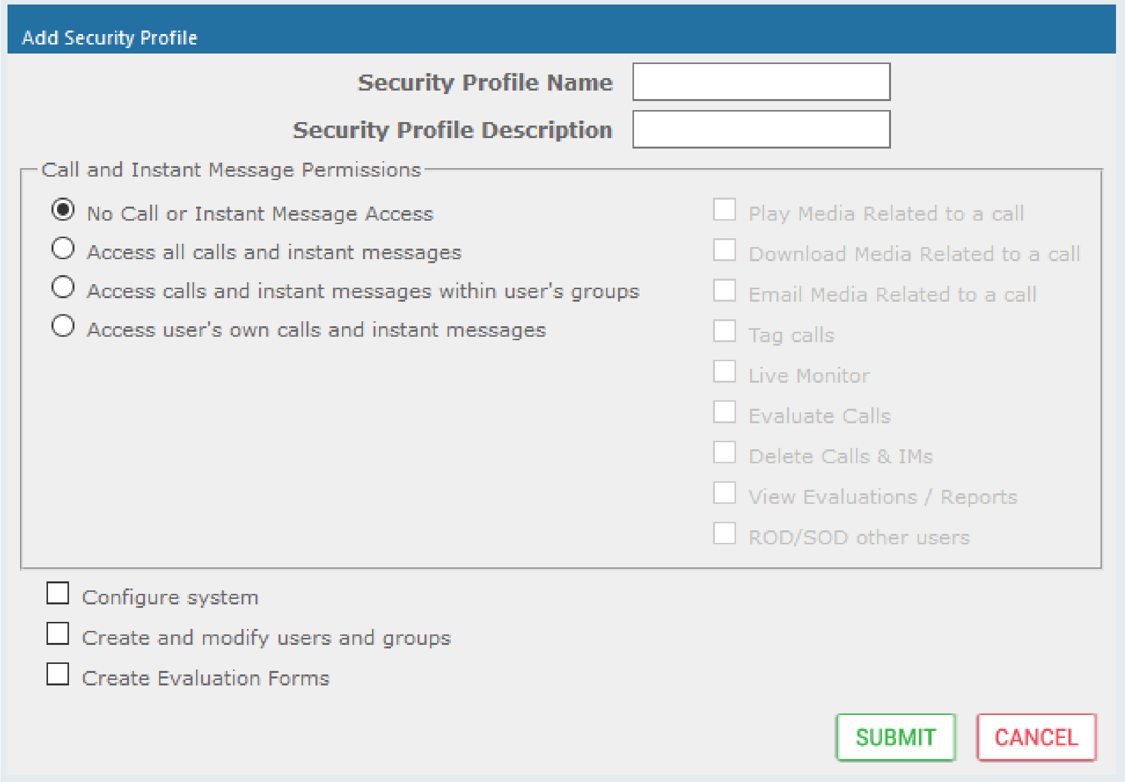
Managing Security Profiles

This section describes how to create, view, modify and delete security profiles and to delete calls and messages. The screen allows the administrator to control system access and permissions. The security profiles assigned to users provides a flexible way to access SmartTAP 360° resources.

➢ To add a Security Profile:

1. Open the Add Security Profile screen (**Users** > **Security Profile** > .**Add Security Profile**).

Figure 6-80: Add Security Profile



Add Security Profile

Security Profile Name

Security Profile Description

Call and Instant Message Permissions

● No Call or Instant Message Access
○ Access all calls and instant messages
○ Access calls and instant messages within user's groups
○ Access user's own calls and instant messages

□ Play Media Related to a call
□ Download Media Related to a call
□ Email Media Related to a call
□ Tag calls
□ Live Monitor
□ Evaluate Calls
□ Delete Calls & IMs
□ View Evaluations / Reports
□ ROD/SOD other users

□ Configure system
□ Create and modify users and groups
□ Create Evaluation Forms

2. Use the table below as reference.

Table 6-31: Security Profile Settings

Field	Description
Security Profile Name	The name of the new security profile.
Security Profile Description	Description of the new security profile.

Field	Description
Call and Instant Message Permissions	
No Call or Instant Message Access	Select this option to prevent users with this security profile from accessing call and instant message data. These users cannot delete calls and instant messages.
Access all calls	Select this option to allow users with this security profile to access calls for all users and devices. These users can delete any calls and instant messages.
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. These users can delete calls and instant messages that belong to the user's groups.
Access user’s own calls	Select this option to allow users with this security profile to access their calls. These users can only delete their own calls and instant messages.
Play Media Related to a call	Select this option to allow users with this security profile to play calls to which they have access.
Download Media Related to a call	Select 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	Select this option to allow users with this security profile to email media for calls to which they have access.
Tag Calls	Select this option to allow users with this security profile to add Call Tags to calls to which they have access.
Live Monitor	Select this option to allow users with this security profile to live monitor calls to which they have access.
Evaluate Calls	Select 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
Delete Calls	Select this option to delete calls and instant message conversations

Field	Description
and IMs	according to the different user privileges described above. For more information, see Deleting Calls and Instant Messages on page 146.
View Evaluations / Reports	Select 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	Select 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	Select this option to allow users with this security profile to view and modify system configuration settings.
Create and modify users and groups	Select this option to allow users with this security profile to create and modify users, groups, and security profiles.
Create Evaluation Forms	Select this option to allow users with this security profile access to the SmartTAP 360° Web interface.
SUBMIT	Apply changes.
CANCEL	Cancel changes.
🗑	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.

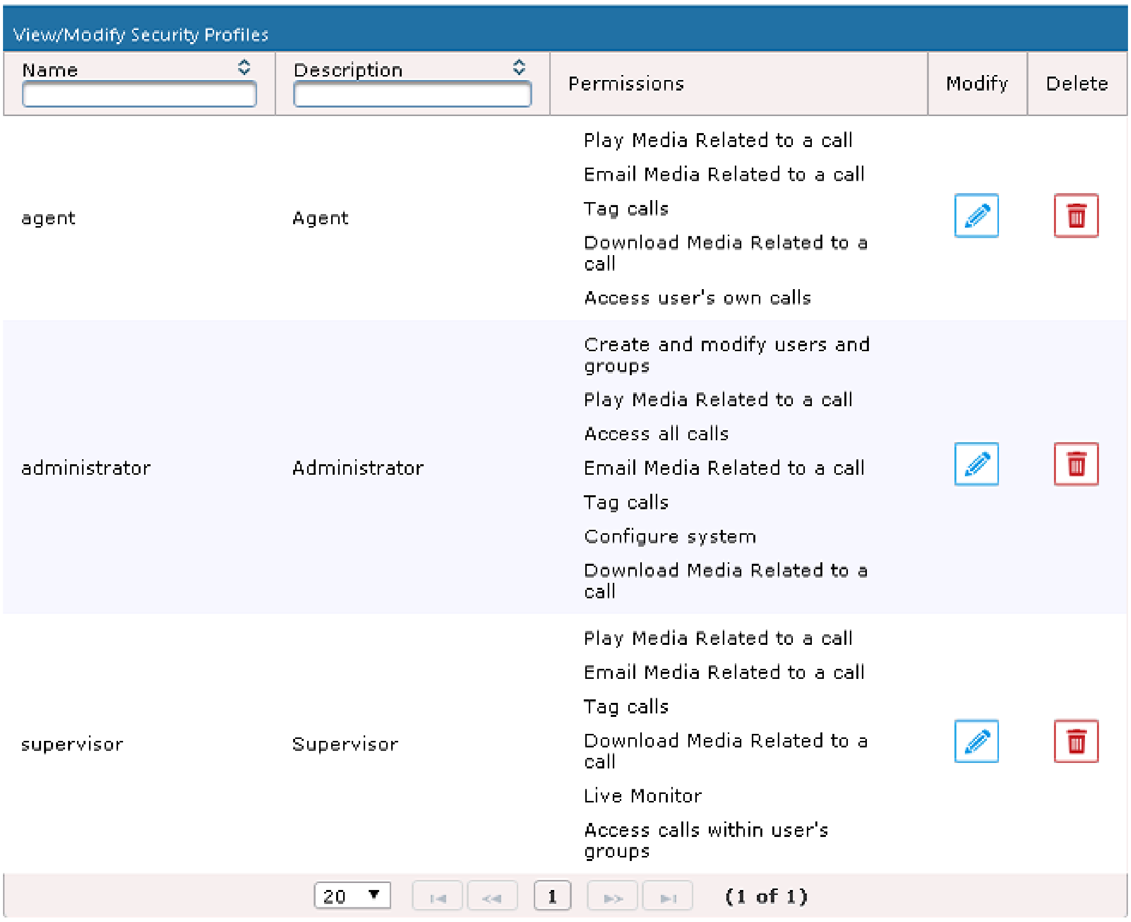
7. Select the configuration permissions at the bottom of the form.

8. Click SUBMIT.

➢ To view/modify Security Profiles:

1. Open the View/Modify Security Profiles screen.

Figure 6-81: View/Modify Security Profiles



View/Modify Security Profiles

Name	Description	Permissions	Modify	Delete
agent	Agent	Play Media Related to a call Email Media Related to a call Tag calls Download Media Related to a call Access user's own calls	✎	🗑
administrator	Administrator	Create and modify users and groups Play Media Related to a call Access all calls Email Media Related to a call Tag calls Configure system Download Media Related to a call	✎	🗑
supervisor	Supervisor	Play Media Related to a call Email Media Related to a call Tag calls Download Media Related to a call Live Monitor Access calls within user's groups	✎	🗑

20 ▼ |◂ ◂◂ 1 ▸▸ ▸| (1 of 1)

2. Use the table below as reference.

Table 6-32: 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.
✎	Click to modify the Security Profile.
🗑	Click to delete the Security Profile.

Managing Recording Profiles

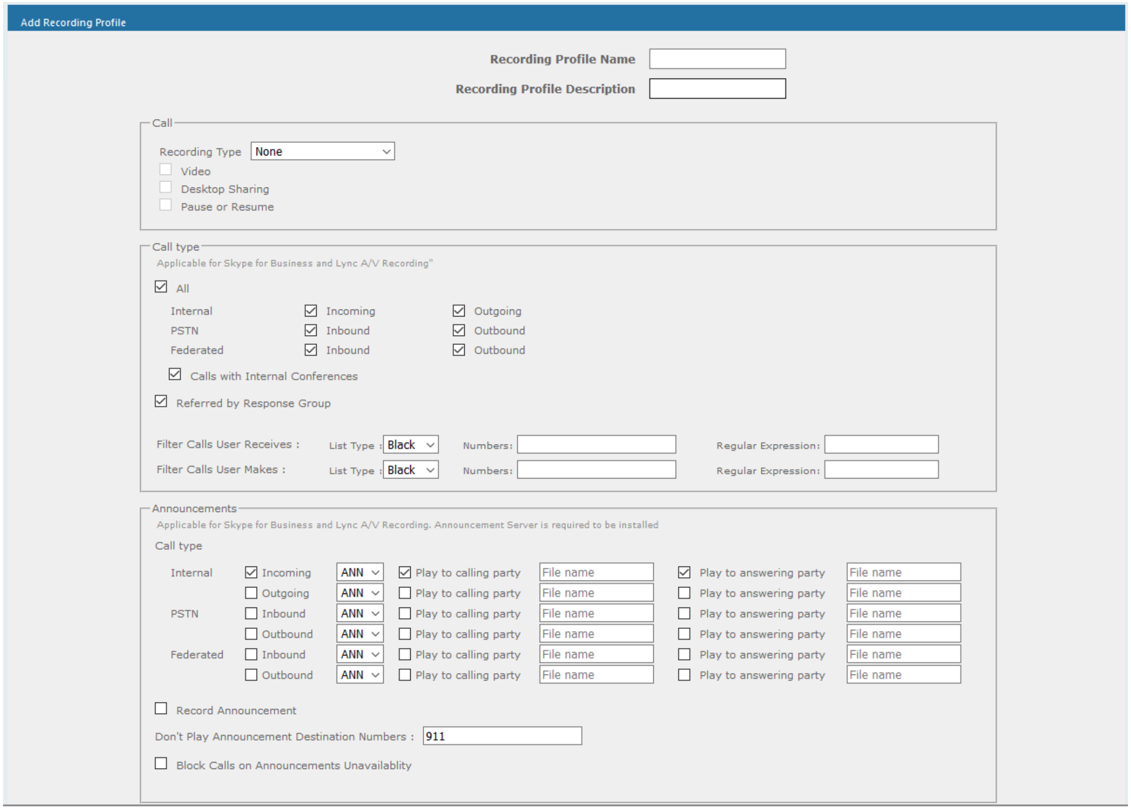
Recording profiles determine the method by which a user or device is recorded. A profile may be assigned to one or more users or devices. The Recording profile includes the following settings:

- **Call:**
  - Recording Type – Full Time, Record on Demand, Save on Demand or none.
  - Video – enable if video call recording is desired
  - Desktop sharing – enable if desktop sharing recording is desired
  - Pause or Resume – enable if the assign with profile user should be able to pause and resume call recordings
- **Call Type:** All, Internal (incoming, outgoing); PSTN (inbound, outbound); Federated (inbound, outbound); Calls with Internal Conference; Referred by Response Group
- **Annoucements:** Enable annoucements for one or more of the above call types.
- **Recording Beep tone:** Play a beep tone in the background during the recording.
- **Instant Messages:** Enable if Instant Messaging recording is desired

➢ To add a Recording Profile:

1. Open the Add Recording Profile screen (**Users** tab > **Recording Profiles** folder > **Add Recording Profile**).

Figure 6-82: Add Recording Profile



Add Recording Profile

Recording Profile Name

Recording Profile Description

Call

Recording Type None

□ Video

□ Desktop Sharing

□ Pause or Resume

Call type

Applicable for Skype for Business and Lync A/V Recording"

☑ All

Internal	☑ Incoming	☑ Outgoing
PSTN	☑ Inbound	☑ Outbound
Federated	☑ Inbound	☑ Outbound

☑ Calls with Internal Conferences

☑ Referred by Response Group

Filter Calls User Receives : List Type : Black Numbers: Regular Expression:

Filter Calls User Makes : List Type : Black Numbers: Regular Expression:

Announcements

Applicable for Skype for Business and Lync A/V Recording. Announcement Server is required to be installed

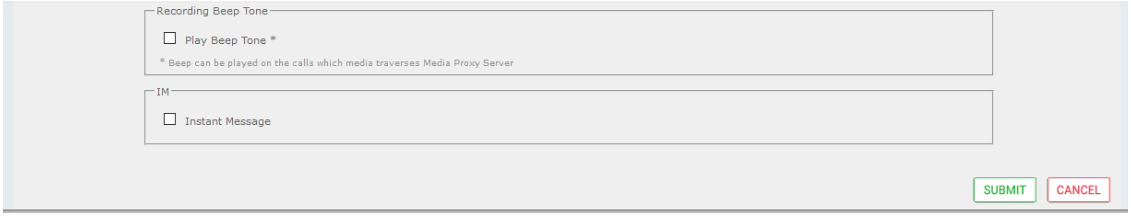
Call type

Internal	☑ Incoming	ANN	☑ Play to calling party	File name	☑ Play to answering party	File name
	□ Outgoing	ANN	□ Play to calling party	File name	□ Play to answering party	File name
PSTN	□ Inbound	ANN	□ Play to calling party	File name	□ Play to answering party	File name
	□ Outbound	ANN	□ Play to calling party	File name	□ Play to answering party	File name
Federated	□ Inbound	ANN	□ Play to calling party	File name	□ Play to answering party	File name
	□ Outbound	ANN	□ Play to calling party	File name	□ Play to answering party	File name

□ Record Announcement

Don't Play Announcement Destination Numbers : 911

□ Block Calls on Announcements Unavailablity



Recording Beep Tone

☐ Play Beep Tone *

* Beep can be played on the calls which media traverses Media Proxy Server

IM

☐ Instant Message

2. In the Call pane ,from the Drop-down list, select a Recording Type and select the appropriate check box For more information, use table below as a reference.

3. In the Call type pane, select a Call type. Note that the corresponding announcement profile is activated in the Annoucements pane. For more information, use table below as a reference.

4. In the Annoucements pane, assign audio files to play to the Calling party, the Answering party or both according to your selection in the Call type pane. For example, if you selected "Federated Inbound" calls in the Call type pane, then you can assign audio files to play to the calling party and to the answering party. For more information, see example figures and table below as references.

5. Assign Announcement WMA media files or IVR JSON script files to play to the Calling party, to the Answering party or to both for incoming and outgoing calls for Internal, PSTN and Federated Call Types. You can assign a different media file to play to the Calling party and to the Answering party.

> Ensure that you have setup the Announcement server to support this functionality (see Announcement Server (Skype for Business) on page 232
>
> - See example configurations in Example Annoucement Server Scenarios on page 237

6. Fill in the required fields using the tables below as a reference.

7. Click SUBMIT.

Table 6-33: Recording Profile

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 one of the following: ■ **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.

Field	Description
	■ **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. Audio recording can be triggered from the GUI Status page or from the Skype for Business CWE toolbar. ■ **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. Audio and/or Video recording can be triggered from the GUI Status page or from the Skype for Business CWE toolbar. ■ For more information, see SmartTAP 360° Skype for Business Toolbar on page 214
Video	Record a video call (Full Time or Save on Demand).
Pause / Resume	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. Pause/Resume of a recording can be triggered from the SmartTAP 360° Web interface status page or from the Skype for Business CWE toolbar.
Instant Message	Automatic Instant Message recording.
Desktop Sharing Recording	Recording of Desktop Sharing sessions is currently supported with Full time or Save on Demand recording type.
SUBMIT	Apply the changes.
CANCEL	Cancel the changes.

- **Call Type**

The Recording profile contains call types that can be selected and recorded. The call types described in the following table are supported. The options below relate to SmartTAP 360°

users and devices regardless of the users or devices location (intranet, internet, mobile device).

These call types are relevant for Skype For Business; Audio; Video and Desktop Sharing recording.

Table 6-34: Call Type

Field	Description
All	Record all calls that the recording profile user participates in as calling party. This option is enabled by default or when a new recording profile is created.
Internal (incoming, outgoing)	Internal calls are calls made between the recording profile user or device and other users belonging to the same domain as the recording profile user. To record Internal calls that the user receives, select the “Incoming” option. To record Internal calls that the user makes, select the “Outgoing” option. *Select the “Calls with Internal Conference” to record Internal calls that are elevated to a conference.
PSTN (inbound, outbound)	PSTN calls are those calls made between the recording profile user and PSTN parties. To record PSTN calls that the user receives, select the “Inbound” option. To record internal calls that the user makes, select the “Outbound” option. *Select the “Calls with Internal Conference” to record PSTN calls that are elevated to a conference.
Federated (inbound, outbound)	Federated calls are those calls made between the recording profile user and federated domain users. To record Federated calls that the user receives, select the “Inbound” option. To record Federated calls that the user makes, select the “Outbound” option. This option covers calls between the user and the federated conference bridges according to the selected directions.
Calls with Internal Conference	Record user calls with an Internal conference bridge in the company domain.
Referred by Response Group	Record user calls that are referred by a response group. To record calls referred by a response group to any user, select this option and create a user or device with the network mapping attributes that are associated with the response group (the Response Group URI). To record all calls that a response group is involved, select this option and the “All” option and create a user or device with the network mapping attributes that are associated with the response group (the Response Group URI).
Filter Calls User Receives	To filter calls that the user receives or makes, choose the type of the filter. To record the user calls with specific numbers, choose “White” in the List Type.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Filter Calls User Makes</td><td>To record calls of the user except with specific numbers, choose “Black: in the List Type. The Filter is applied on the calls with the comma-separated phone numbers defined in the Numbers field. For example: “17326524689, 17326524690”, a regular expression can be entered when the phone number ranges need to be filtered. For example, to filter calls with phone numbers that starts with area code 732 or 609, enter the following in the regular expression field: ^(1{1}|\+1{1})?(732|609)\d*$. When both the numbers and regular expressions are provided, the system first checks against the regular expression and if a match is not found, continues with the numbers. The maximum length of the numbers and the regular expression field is 2048 characters.</td></tr>
</table>

- **Annoucements**

Recording profile contains announcements configuration that can be selected and applied on the recorded user calls according to the options in the following table.

- The configuration options below are supported for Skype For Business calls.
- The Announcement server must be installed.
- The configuration options below relate to SmartTAP 360° users and devices, regardless of the user or device location (intranet/internet, mobile device).

Table 6-35: Announcements

Field	Description
Internal (incoming, outgoing)	Play announcement on the Internal calls of the recorded user. To play announcement on the calls the user receives, select the “Incoming” option. To play announcement on the calls the user makes, select the “Outgoing” option. *Playing the announcement on the calls with conference server is currently not supported
PSTN (inbound, outbound)	Play announcement on the PSTN calls of the recorded user. To play announcement on the PSTN calls that the user receives, select the “Inbound” option. To play announcement on the PSTN calls that the user makes, select “Outbound” option.
Federated (inbound, outbound)	Play announcement on the Federated calls of the recorded user. To play announcement on the Federated calls that the user receives, select the “Inbound” option. To play announcement on the Federated calls that the user makes, select the “Outbound” option.
Record Announcement	To record played announcement, select this option. When the option is enabled and the announcement is played to both the incoming and

Field	Description
	outgoing legs of the call, both call legs are recorded and two recording licenses are consumed for the announcement part of the call recording. .
Don’t Play Announcement Destination Number	Don’t play announcements on the calls to the numbers defined in this field. The numbers should be comma separated. Enter the numbers when playing announcement on calls to a specific destination is not desired. For example, calls to 911, enter 911
Block Calls on Announcement Unavailability	The calls with the recorded user will be blocked when the calls can’t be routed to the announcement server(s).
Configure Media Files to Play on Announcements	● ANN files must be of file type WMA ● IVR files must be of file type JSON ● You must specify the file extension type in the file name. For example, PSTN_Inbound.wma ● ANN and IVR files must be pre-saved to the StateMachineConfig folder on the ANN server: see Section Step 3-Configuring Announcement Server (Skype for Business) in the *SmartTAP 360° Installation Guide.*

- **Beep Tone:** Beep tones can be played on the calls which media traverses the Media Proxy Server only.

> - The Announcement Server does not require to be installed to play beep tones.
> - Beep tone can be played on calls which media traverse the Media Proxy Server only
> - The playing of beep tones on the calls between targeted users and Skype For Business Conference Server is not supported.
> - Contact AudioCodes sales or support for information on the supported scenarios.
>
> For configuration of beep tone parameters, refer to the *SmartTAP 360° Installation Guide*.

Field	Description
Play Beep Tone	The beep tone is played in the background during the call recording (disabled by default). Beep tone can be played on the calls which media traverses the Media Proxy Server.

- **Instant Messages**

  Enables Automatic Instant Message recording.

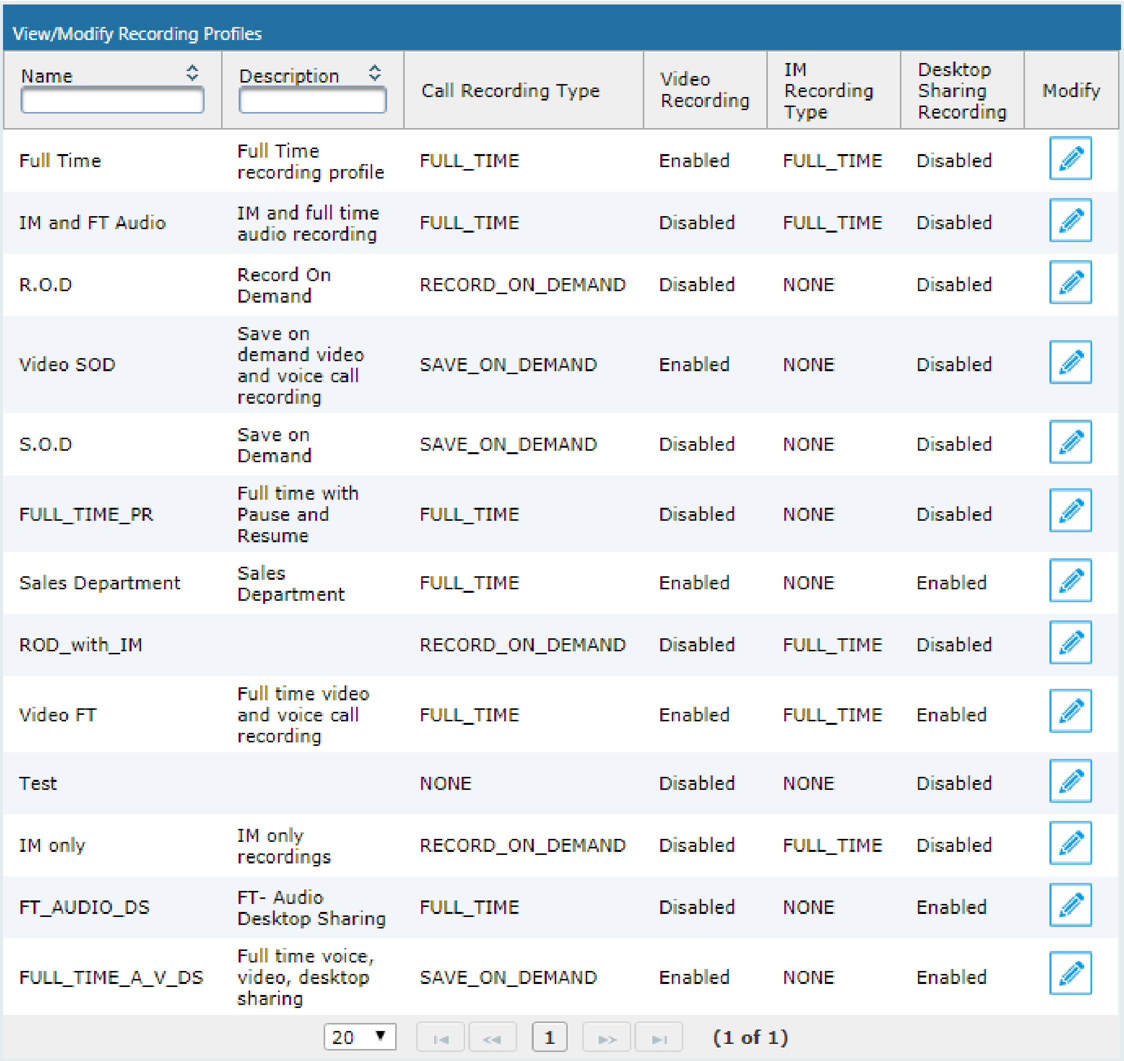
Viewing or Modifying Recording Profiles

This section describes how to view or modify recording profiles.

➢ To view/modify Recording Profiles:

1. Open the View/Modify Recording Profiles screen (**Users** tab > **Recording Profiles** folder > **View/Modify Recording Profiles**).

Figure 6-83: View/Modify Recording Profiles



View/Modify Recording Profiles

Name	Description	Call Recording Type	Video Recording	IM Recording Type	Desktop Sharing Recording	Modify
Full Time	Full Time recording profile	FULL_TIME	Enabled	FULL_TIME	Disabled	
IM and FT Audio	IM and full time audio recording	FULL_TIME	Disabled	FULL_TIME	Disabled	
R.O.D	Record On Demand	RECORD_ON_DEMAND	Disabled	NONE	Disabled	
Video SOD	Save on demand video and voice call recording	SAVE_ON_DEMAND	Enabled	NONE	Disabled	
S.O.D	Save on Demand	SAVE_ON_DEMAND	Disabled	NONE	Disabled	
FULL_TIME_PR	Full time with Pause and Resume	FULL_TIME	Disabled	NONE	Disabled	
Sales Department	Sales Department	FULL_TIME	Enabled	NONE	Enabled	
ROD_with_IM		RECORD_ON_DEMAND	Disabled	FULL_TIME	Disabled	
Video FT	Full time video and voice call recording	FULL_TIME	Enabled	FULL_TIME	Enabled	
Test		NONE	Disabled	NONE	Disabled	
IM only	IM only recordings	RECORD_ON_DEMAND	Disabled	FULL_TIME	Disabled	
FT_AUDIO_DS	FT- Audio Desktop Sharing	FULL_TIME	Disabled	NONE	Enabled	
FULL_TIME_A_V_DS	Full time voice, video, desktop sharing	SAVE_ON_DEMAND	Enabled	NONE	Enabled	

2. Use the table below as reference.

Table 6-36: 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

Field	Description
	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
✎	Click to modify the Recording Profile.

Assigning Recording Profile to User or Device

This section describes how to assign a recording profile to a user or device.

➢ 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 360°. To create a new user account and assign a Recording Profile:

  a. Under the User tab, select **View/Modify Users**.

  b. Click ✎.

  c. From the 'Recording Profile' dropdown, select the required profile (i.e., R.O.D).

  d. 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:

  a. Under the User tab, select Recording Profile | User / Devices.

  b. Using the arrows, move single or bulk list of user / devices from the left screen to one of the recording profiles available.

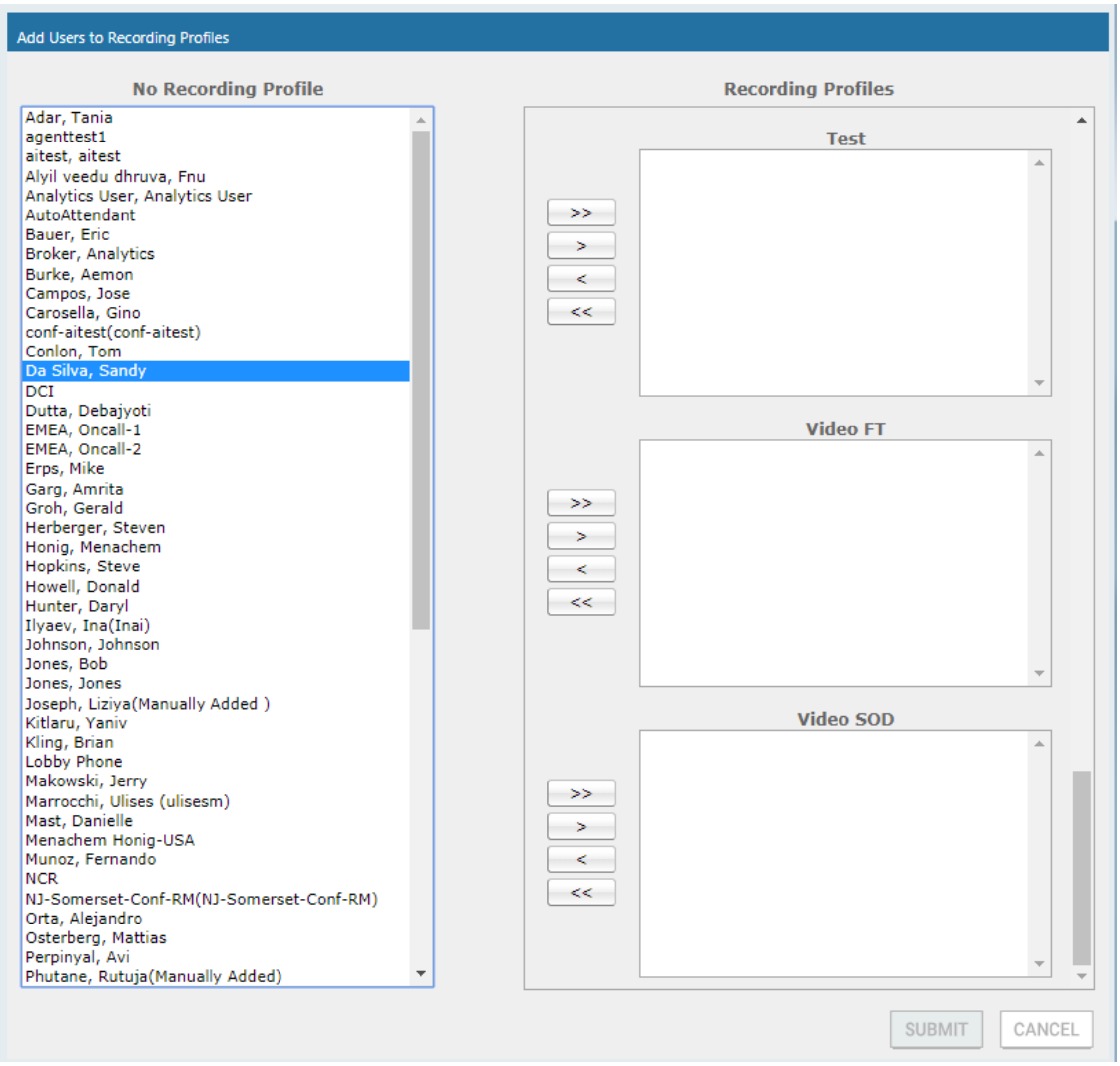
  c. Click Submit to apply changes.

- By default, SmartTAP 360° 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 6-84: Add Users to Recording Profiles


Add Users to Recording Profiles

No Recording Profile

Adar, Tania
agenttest1
aitest, aitest
Alyil veedu dhruva, Fnu
Analytics User, Analytics User
AutoAttendant
Bauer, Eric
Broker, Analytics
Burke, Aemon
Campos, Jose
Carosella, Gino
conf-aitest(conf-aitest)
Conlon, Tom
Da Silva, Sandy
DCI
Dutta, Debajyoti
EMEA, Oncall-1
EMEA, Oncall-2
Erps, Mike
Garg, Amrita
Groh, Gerald
Herberger, Steven
Honig, Menachem
Hopkins, Steve
Howell, Donald
Hunter, Daryl
Ilyaev, Ina(Inai)
Johnson, Johnson
Jones, Bob
Jones, Jones
Joseph, Liziya(Manually Added)
Kitlaru, Yaniv
Kling, Brian
Lobby Phone
Makowski, Jerry
Marrocchi, Ulises (ulisesm)
Mast, Danielle
Menachem Honig-USA
Munoz, Fernando
NCR
NJ-Somerset-Conf-RM(NJ-Somerset-Conf-RM)
Orta, Alejandro
Osterberg, Mattias
Perpinyal, Avi
Phutane, Rutuja(Manually Added)

Recording Profiles

Test

Video FT

Video SOD

2. Use the table below as reference.

Table 6-37: Add Users to Recording Profiles Screen

Field	Description
No Recording Profile	List of available Users / Devices in SmartTAP 360° unassigned to a specific recording profile.

Field	Description
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.

⚠

- In addition to assigning a user / device with a recording profile, you must add a recording attribute and a targeting value.
- SmartTAP 360° will use the added targeting value to trigger recording once detected in the call signaling.

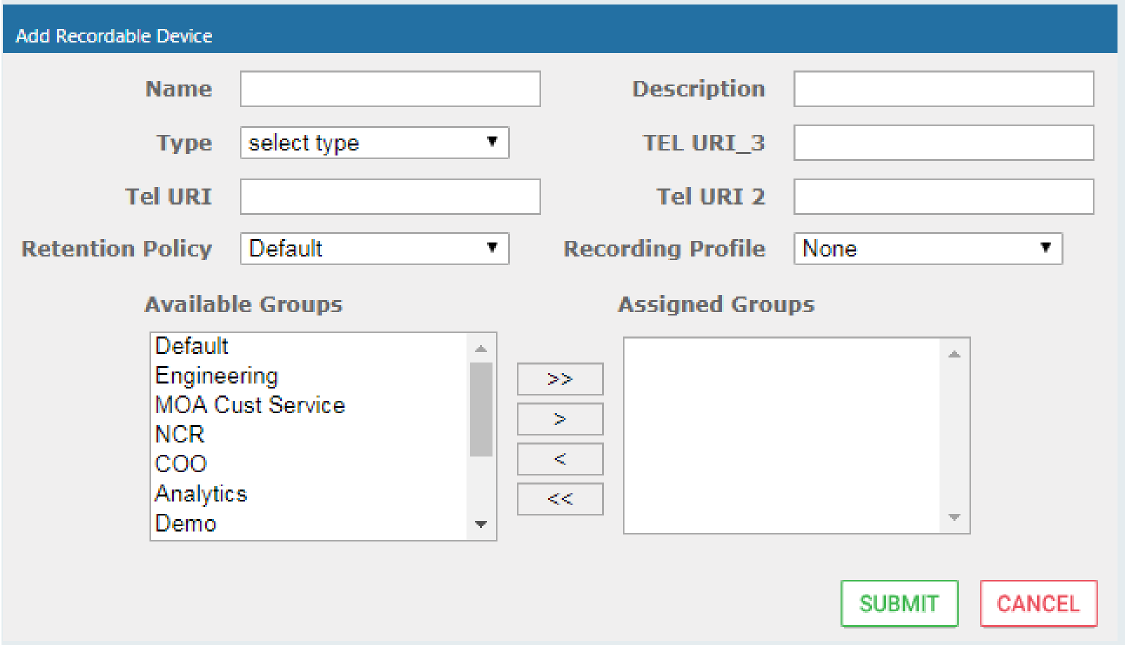
Managing Recordable Devices

This section shows how to manage recordable devices.

➢ To add a Recordable Device:

1. Open the Add Recordable Device screen (**Users** tab > **Recording Profile** > **Add Recordable Device**).

Figure 6-85: Add Recordable Device



Add Recordable Device

Name		Description	
Type	select type	TEL URI_3	
Tel URI		Tel URI 2	
Retention Policy	Default	Recording Profile	None

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 6-38: Recordable Device – Settings Descriptions

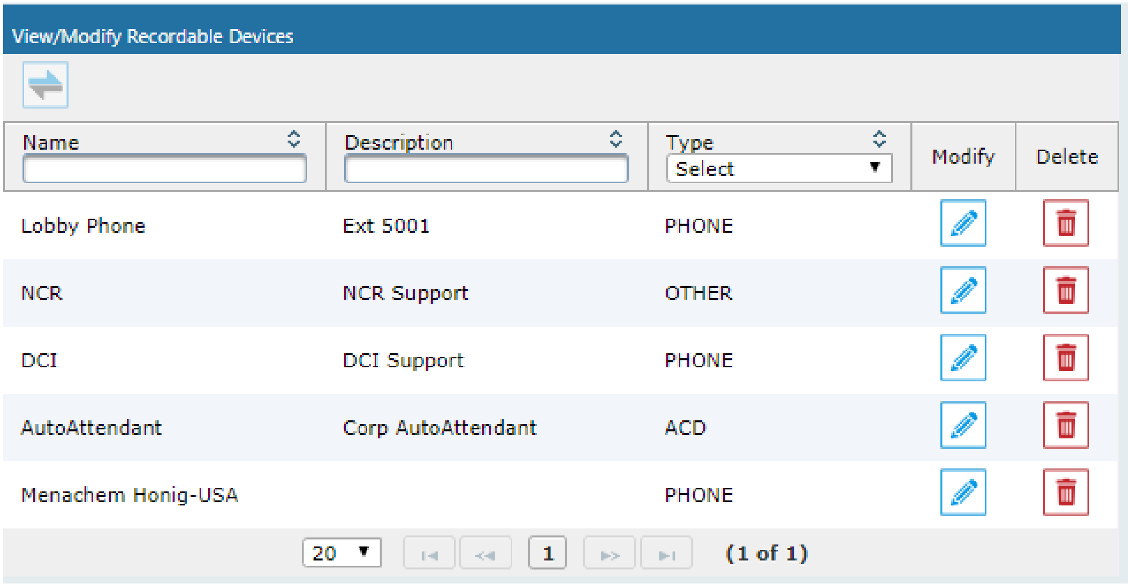
Field	Description
Name	Name of the new recordable device.
Description	Description of the new recordable device.
Type	Type of recordable device. Dropdown menu shows valid entries.
Retention Policy	Select an appropriate retention policy for the device.
Recording Profile	Select an appropriate recording 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	User groups assigned to this device. Select group by clicking the group

Field	Description
Groups	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.
SUBMIT	Apply the changes.
CANCEL	Cancel the changes.
🗑	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 6-86: View/Modify Recordable Devices



View/Modify Recordable Devices

Name	Description	Type Select	Modify	Delete
Lobby Phone	Ext 5001	PHONE	✎	🗑
NCR	NCR Support	OTHER	✎	🗑
DCI	DCI Support	PHONE	✎	🗑
AutoAttendant	Corp AutoAttendant	ACD	✎	🗑
Menachem Honig-USA		PHONE	✎	🗑

2. Use the table below as reference.

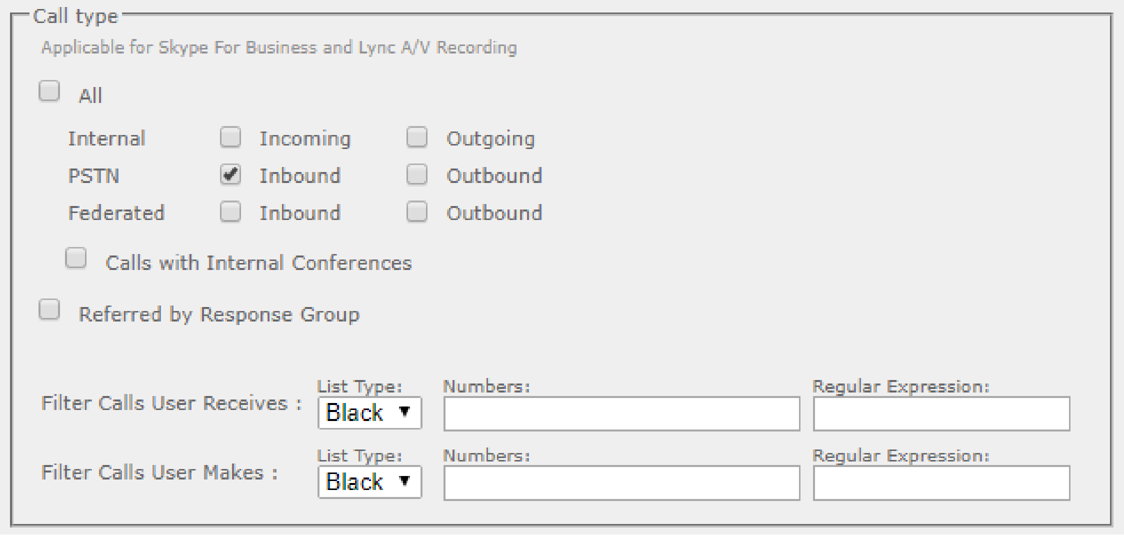
Figure 6-87: View/Modify Recordable Devices – Field Descriptions

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.
✎	Click to modify the Security Profile.
🗑	Click to delete the Security Profile.

Recording Profile-Call Type Configuration Examples

This section describes configuration examples for different call type settings.

- Record inbound PSTN calls:



Call type

Applicable for Skype For Business and Lync A/V Recording

□ All

Internal □ Incoming □ Outgoing

PSTN ☑ Inbound □ Outbound

Federated □ Inbound □ Outbound

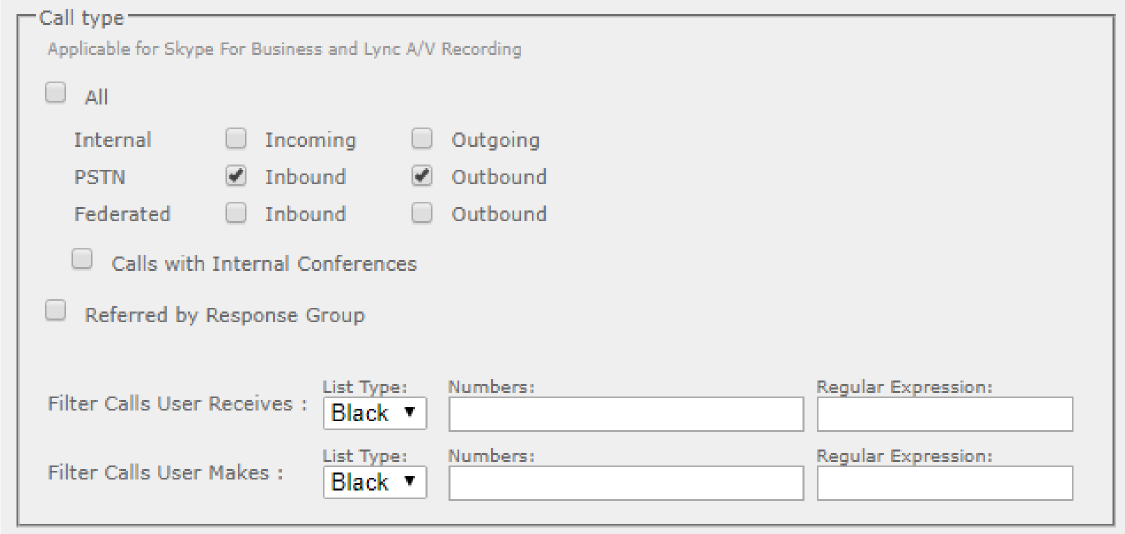
□ Calls with Internal Conferences

□ Referred by Response Group

Filter Calls User Receives : List Type: Black ▾ Numbers: Regular Expression:

Filter Calls User Makes : List Type: Black ▾ Numbers: Regular Expression:

- Record all PSTN Calls:



Call type

Applicable for Skype For Business and Lync A/V Recording

☐ All

Internal	☐ Incoming	☐ Outgoing
PSTN	☑ Inbound	☑ Outbound
Federated	☐ Inbound	☐ Outbound

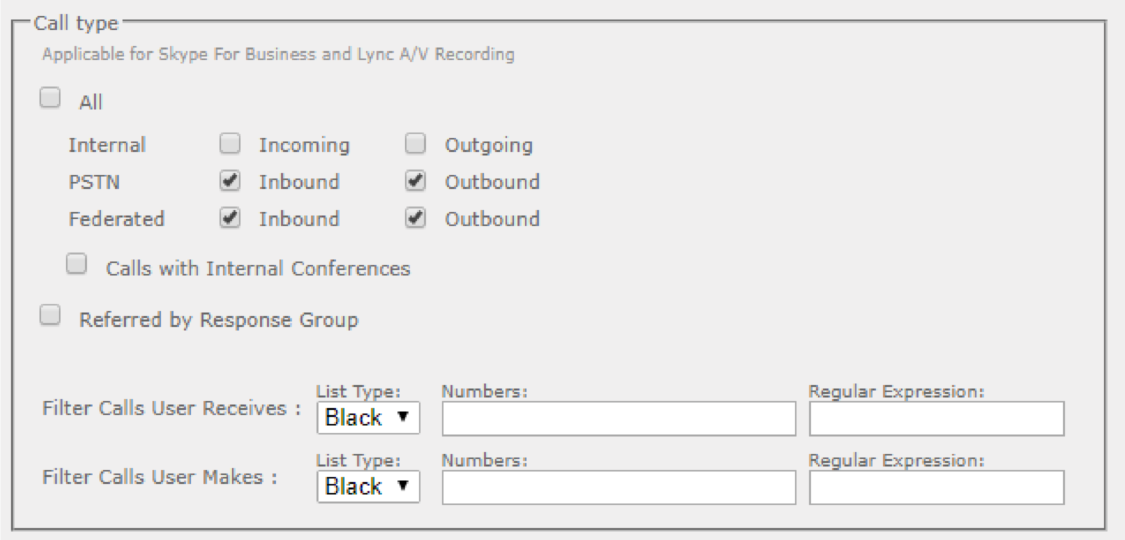
☐ Calls with Internal Conferences

☐ Referred by Response Group

Filter Calls User Receives : List Type: Black ▼ Numbers: Regular Expression:

Filter Calls User Makes : List Type: Black ▼ Numbers: Regular Expression:

- Record External calls (PSTN and Federation):



Call type

Applicable for Skype For Business and Lync A/V Recording

☐ All

Internal	☐ Incoming	☐ Outgoing
PSTN	☑ Inbound	☑ Outbound
Federated	☑ Inbound	☑ Outbound

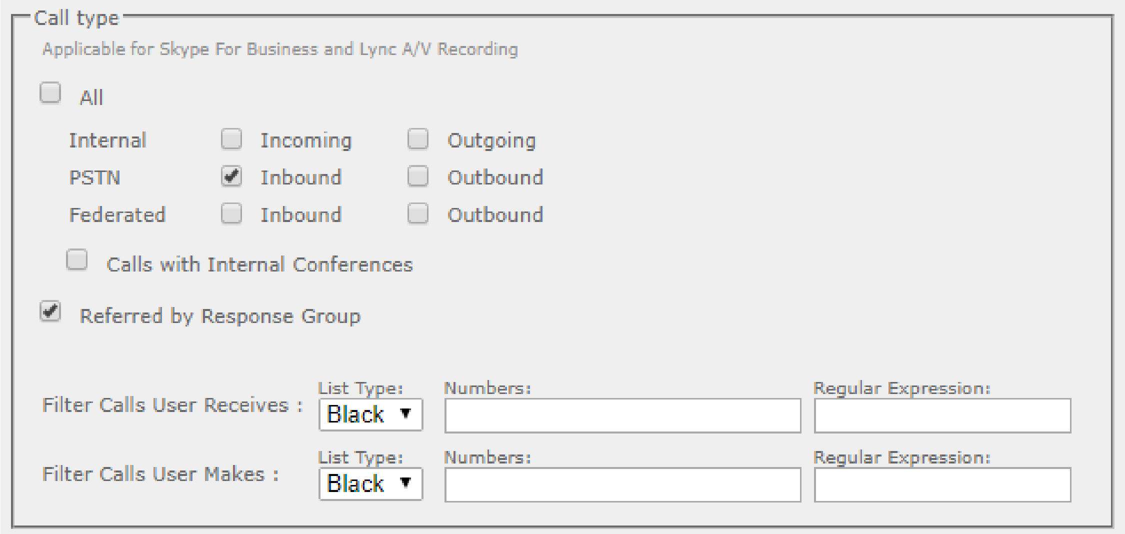
☐ Calls with Internal Conferences

☐ Referred by Response Group

Filter Calls User Receives : List Type: Black ▼ Numbers: Regular Expression:

Filter Calls User Makes : List Type: Black ▼ Numbers: Regular Expression:

- Record PSTN inbound calls and calls from Response Group



Call type

Applicable for Skype For Business and Lync A/V Recording

☐ All

Internal	☐ Incoming	☐ Outgoing
PSTN	☑ Inbound	☐ Outbound
Federated	☐ Inbound	☐ Outbound

☐ Calls with Internal Conferences

☑ Referred by Response Group

Filter Calls User Receives : List Type: Black ▼ Numbers: Regular Expression:

Filter Calls User Makes : List Type: Black ▼ Numbers: Regular Expression:

Adding a Device Attribute

This section describes how to add a SmartTAP 360° device attribute. The table below describes the purposes of these attributes.

Table 6-39: SmartTAP 360° Device Attributes

Attribute Purpose	Priority	Description
Trigger Recording	Critical	To designate to SmartTAP 360° 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 360° 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 360°, for example, Ext, Tel URI, Mobile, etc. for information purposes only. See also Adding a General Device Attribute on the next page.

Enhance the integration by mapping SmartTAP 360° attributes to Active Directory attributes to auto populate device information within SmartTAP 360°. To map a device attribute to an Active Directory device attribute, see Configuring an LDAP Connection on page 82

Table 6-40: User Attributes

User Attribute	Description
Name	Unique easily identifiable name to the attribute.
Description	Brief Description of the attribute.
Network Mapping	Indicates whether attribute mapping is required. When selected, the 'Network Mapping Type' drop-down list is available.
Network Mapping Type	Indicates the type of network mapping that is required for the user. Choose from one of the following values: ■ TEL_URI ■ SIP_URI ■ IP_ADDRESS ■ TERMINAL_ADDRESS ■ USERNAME ■ EXTENSION ■ TRUNK_ID

User Attribute	Description
	■ OBJECT_ID

You can add the following types of attributes:

- Adding a General Device Attribute below
- Adding a Device Attribute for Recording on the next page
- Adding a Microsoft Teams User Attribute on page 129

Figure 6-88:

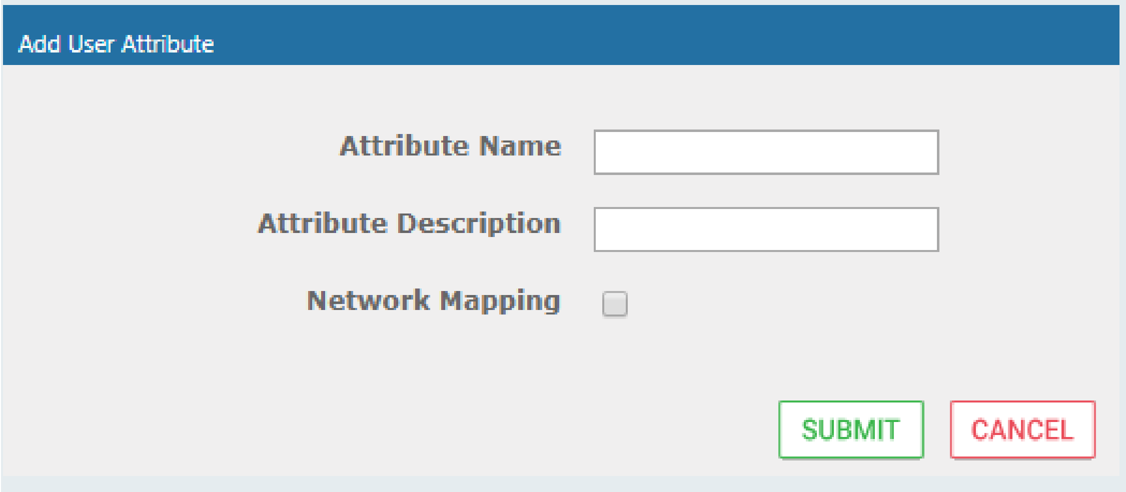
Adding a General Device Attribute

This section describes how to add a general device attribute. A general device attribute is not used for recording purposes.

➢ To add a general device attribute:

1. Open the Add Device Attribute screen (**Users** > **User Management** > **Add Device Attribute**).

Figure 6-89: Add General 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.

Adding a Device Attribute for Recording

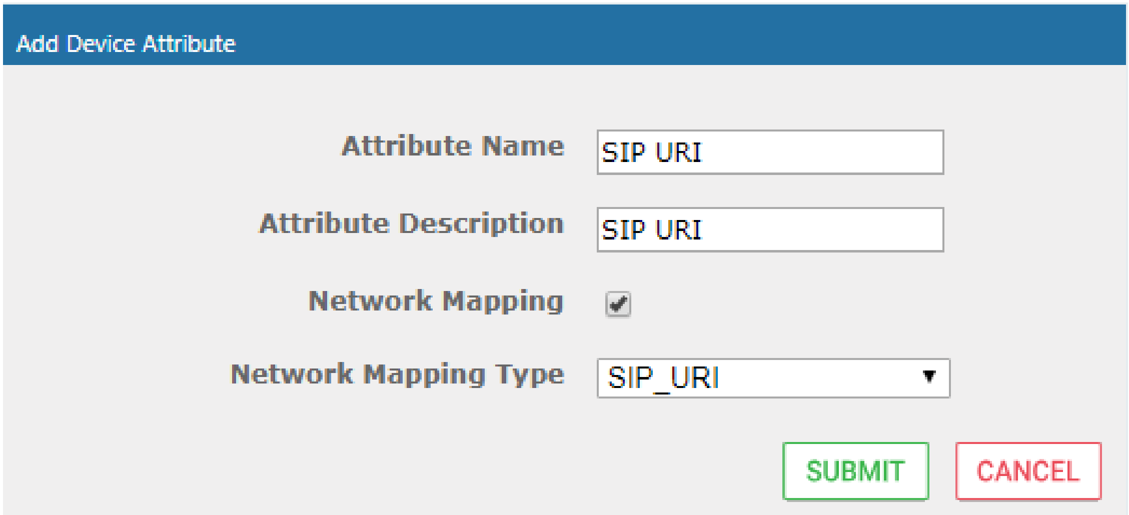
This section describes how to add a recording device attribute.

➢ To add a device attribute for recording purposes:

1. Open the Add Device Attribute screen (**Users** > **User Management** > **Add Device Attribute**).
2. Enter the Attribute Name.
3. Enter the Attribute Description.
4. Select the **Network Mapping** option.
5. From the Network Mapping drop-down list, select the appropriate Network Mapping type e.g. 'SIP_URI'
6. Click SUBMIT to apply new device attribute or CANCEL to exit.

Following are examples of device attributes created for recording purposes:

Figure 6-90: Add Device Attribute - Example 1



Add Device Attribute

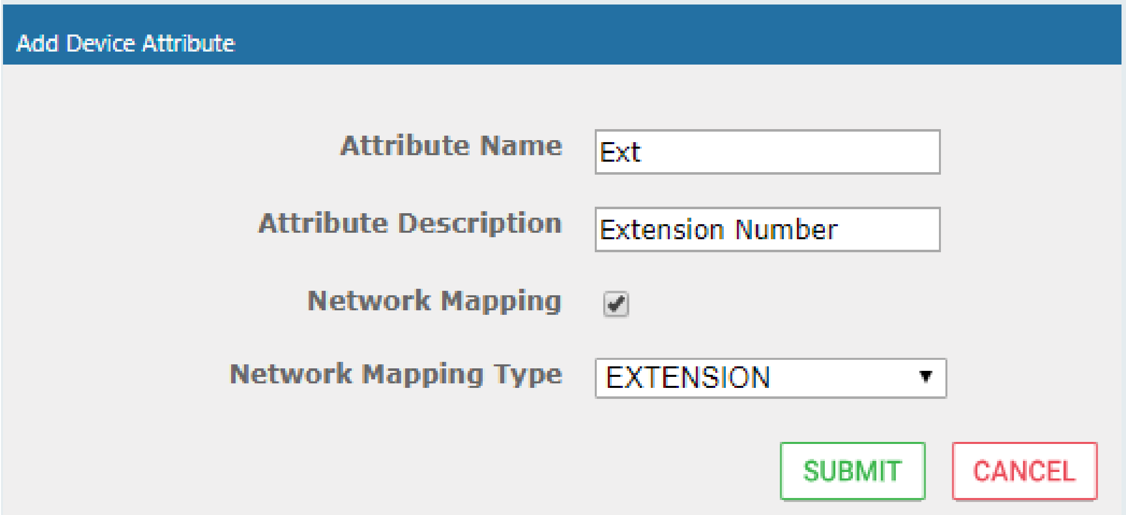
Attribute Name: SIP URI

Attribute Description: SIP URI

Network Mapping: ☑

Network Mapping Type: SIP_URI ▾

Figure 6-91: Add Device Attribute - Example 2



Add Device Attribute

Attribute Name: Ext

Attribute Description: Extension Number

Network Mapping: ☑

Network Mapping Type: EXTENSION

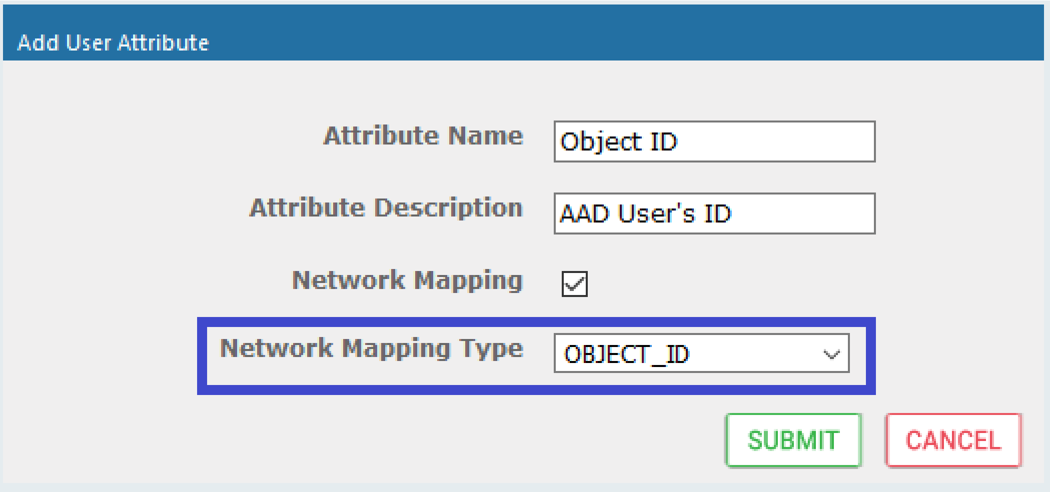
Adding a Microsoft Teams User Attribute

This section describes how to add a custom user attribute for mapping the Object ID of the Microsoft Teams user Active Directory attribute. When the Object_ID is assigned its mapped to the value 'id' which can then be configured in the mapping profile in the Active Directory Configuration (see Step 5 Add Azure Active Directory Mapping in SmartTAP 360° on page 256).

➢ **To map SmartTAP 360° user to Object ID attribute:**

1. Open the Add Device Attribute screen (**Users** > **User Management** > **Add Device Attribute**).
2. Enter the Attribute Name.
3. Enter the Attribute Description.
4. Select the **Network Mapping** option.
5. Select the Network Mapping type 'OBJECT_ID'

Figure 6-92: Add User Attribute



Add User Attribute

Attribute Name: Object ID

Attribute Description: AAD User's ID

Network Mapping: ☑

Network Mapping Type: OBJECT_ID

6. Click SUBMIT to apply new device attribute or CANCEL to exit.

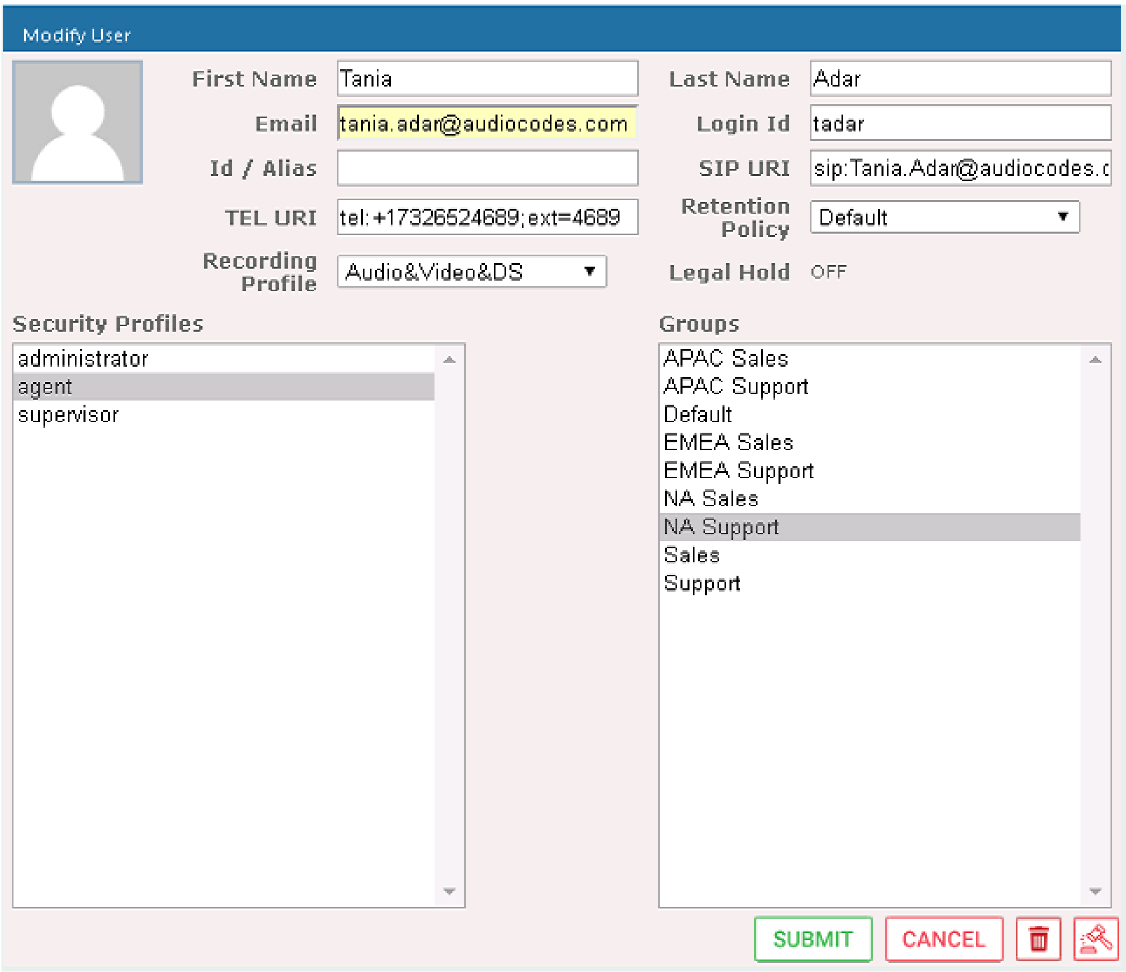
View and Modify Users

This section describes how to view and modify users.

➢ **To view/modify users:**

1. Open the View/Modify Users screen (**Users** tab > **User Management** folder> **View/Modify User**).
2. Use the table below as reference to search for a specific user to modify.

Figure 6-93: View/Modify Users



Modify User

First Name: Tania
Last Name: Adar
Email: tania.adar@audiocodes.com
Login Id: tadar
Id / Alias:
SIP URI: sip:Tania.Adar@audiocodes.c
TEL URI: tel:+17326524689;ext=4689
Retention Policy: Default
Recording Profile: Audio&Video&DS
Legal Hold: OFF

Security Profiles: administrator, agent, supervisor

Groups: APAC Sales, APAC Support, Default, EMEA Sales, EMEA Support, NA Sales, NA Support, Sales, Support

Table 6-41: 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

Field	Description
	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.
✎	Click to modify the user.
🗑	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.

3. Click ✎ adjacent to the user that you wish to change.
4. Modify the fields to change.
5. Click SUBMIT to apply changes.

Update an Admin User

This section describes how to update an Admin user.

➢ To update an Admin User (optional):

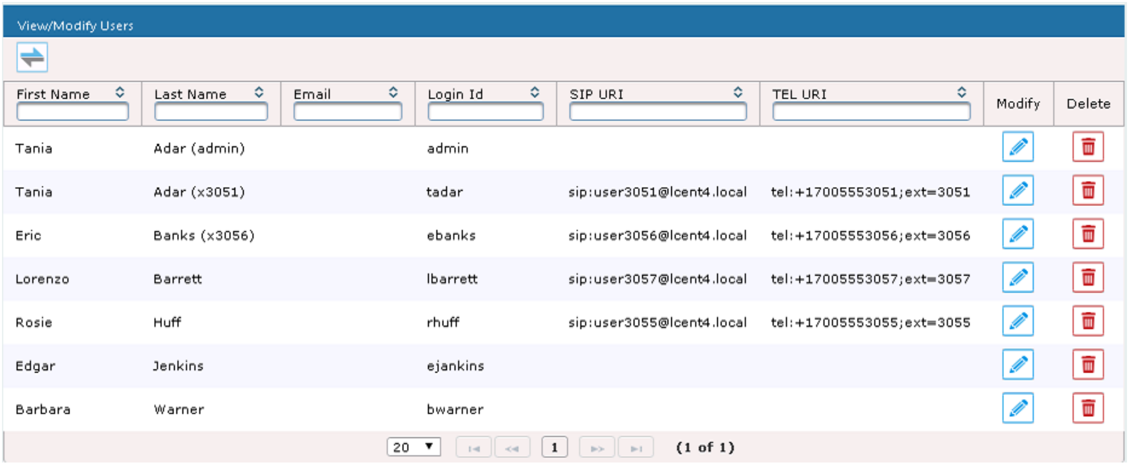
- After logging in, the 'admin' user can create a new administrator account or just edit the information and modify the password for this account.

⚠ Ensure that you configure SMTP settings (see .Configuring Email Server Settings on page 62).

➢ To modify / update an Admin User:

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

Figure 6-94: Modify User



View/Modify Users

First Name	Last Name	Email	Login Id	SIP URI	TEL URI	Modify	Delete
Tania	Adar (admin)		admin			✎	🗑
Tania	Adar (x3051)		tadar	sip:user3051@lcent4.local	tel:+17005553051;ext=3051	✎	🗑
Eric	Banks (x3056)		ebanks	sip:user3056@lcent4.local	tel:+17005553056;ext=3056	✎	🗑
Lorenzo	Barrett		lbarrett	sip:user3057@lcent4.local	tel:+17005553057;ext=3057	✎	🗑
Rosie	Huff		rhuff	sip:user3055@lcent4.local	tel:+17005553055;ext=3055	✎	🗑
Edgar	Jenkins		ejankins			✎	🗑
Barbara	Warner		bwarner			✎	🗑

20 ▼ 1 (1 of 1)

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.

Reset User Password

This section describes how to reset user passwords.

➢ To reset a user password:

⚠ 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 ✎ in the View/Modify User main screen display for the user to reset password.

3. Click the **Reset Password** 🔒 button.

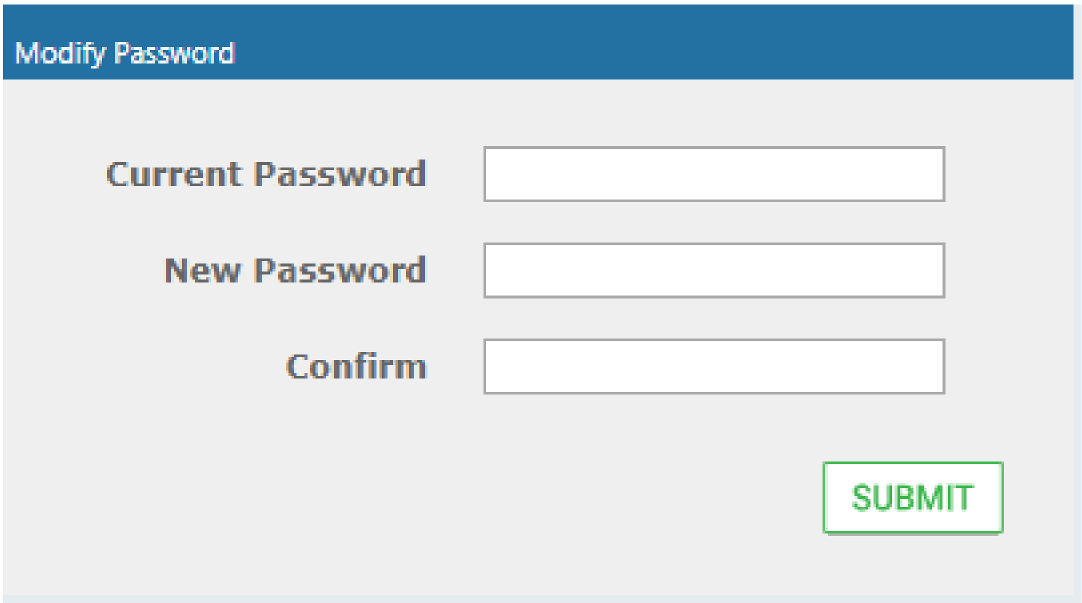
Modify a User Password

This section describes how to modify a user password.

➢ To modify a user password:

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

Figure 6-95: 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.

Figure 6-96: 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.

⚠ The only method to regain access to the SmartTAP 360° system after a password is lost is for a user with Add/Modify privileges to reset this user password.

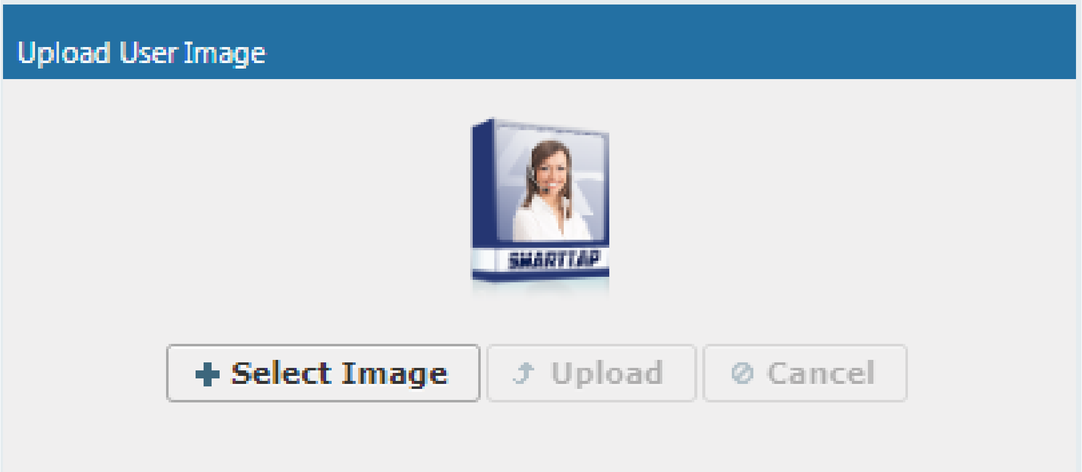
Uploading an Image

This section describe how to upload an image.

➢ To upload an image:

Select this option to upload your own image.

Figure 6-97: Upload User Image



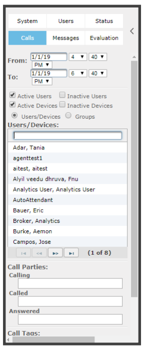
➢ **To upload an image**

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.

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.

Figure 6-98: Search Calls Navigation Screen - Calls Tab

Search Calls Navigation	Field	Description
 System Users Status Calls Messages Evaluation From: 1/1/19 4 40 PM To: 1/1/19 6 40 PM ☑ Active Users ☐ Inactive Users ☑ Active Devices ☐ Inactive Devices ● Users/Devices ○ Groups Users/Devices: Adar, Tania agenttest1 aitest, aitest Alyil veedu dhruva, Fnu Analytics User, Analytics User AutoAttendant Bauer, Eric Broker, Analytics Burke, Aemon Campos, Jose (1 of 8) Call Parties: Calling Called Answered Call Tags:	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 360° system.
	Inactive Users	Users whose accounts have been deleted from the SmartTAP 360° system.
	Active Devices	Devices that are not associated with users enabled in the

Search Calls Navigation	Field	Description
		SmartTAP 360° system and can be targeted for recording.
	Inactive Devices	Devices that have been deleted from the SmartTAP 360° 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.

Searching for Calls

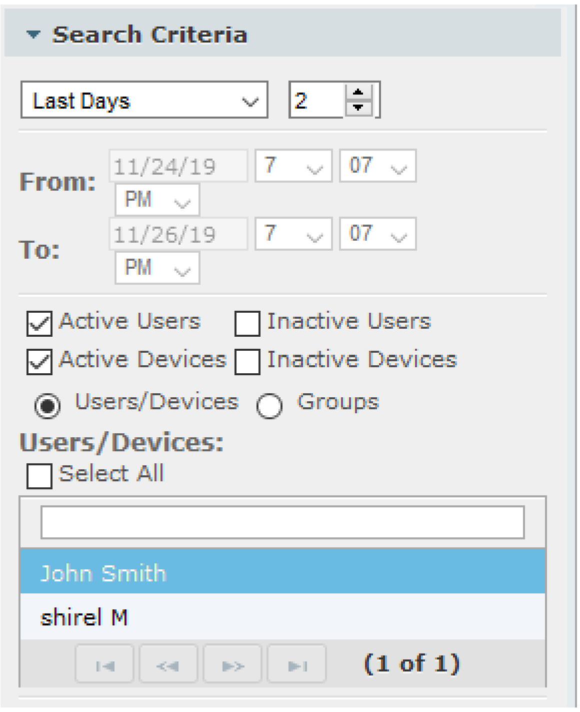
This section shows how to search for calls.

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 ORed and Call Tags (Call Tag1 … Call TagN) are logically ORed.

➢ To search for calls:

1. Open the Search Calls screen by clicking the **Calls** tab.
2. In the Search Critiera pane, from the Drop-down list, select one of the following search criteria:
    - Last Hours
    - Last Days
    - Last Weeks
    - Custom Dates (enables you to customize the day and time range using the calendar)

Figure 6-99: Search Criteria-Last Two Days



Search Criteria

Last Days 2

From: 11/24/19 7 07 PM

To: 11/26/19 7 07 PM

☑ Active Users ☐ Inactive Users
☑ Active Devices ☐ Inactive Devices

● Users/Devices ○ Groups

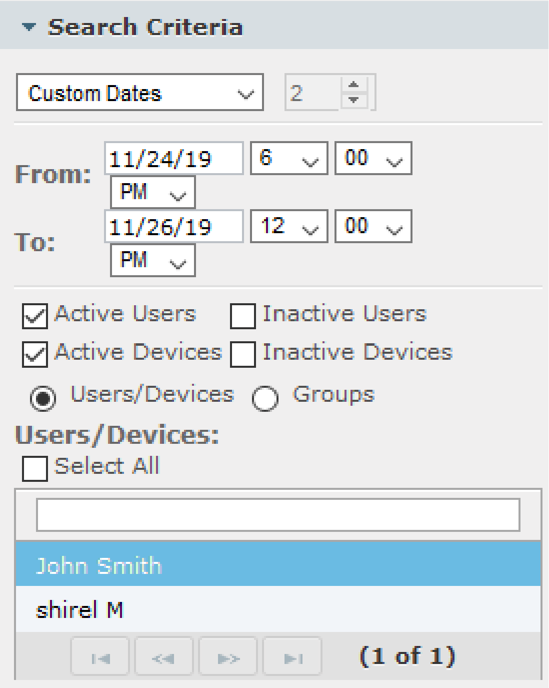
Users/Devices:
☐ Select All

John Smith
shirel M

(1 of 1)

3. If you selected Last Hours, Last Days or Last Weeks, use the arrow keys adjacent to the selected option to toggle to the desired value. If you selected Custom Dates, set the desired time and date range using the calendar. The figure below shows a calendar search from November 24 2019 at 06:00 am to November 26 at 12:00 am.

Figure 6-100: Calendar Search



▾ Search Criteria

Custom Dates 2

From: 11/24/19 6 00 PM

To: 11/26/19 12 00 PM

☑ Active Users ☐ Inactive Users

☑ Active Devices ☐ Inactive Devices

● Users/Devices ○ Groups

Users/Devices:

☐ Select All

John Smith

shirel M

(1 of 1)

4. Select the type of Users and Devices.

5. Select either the Users/Devices or Groups Radio button.

6. Selecting the User/Devices option changes the display below to show a list of Users/Devices.

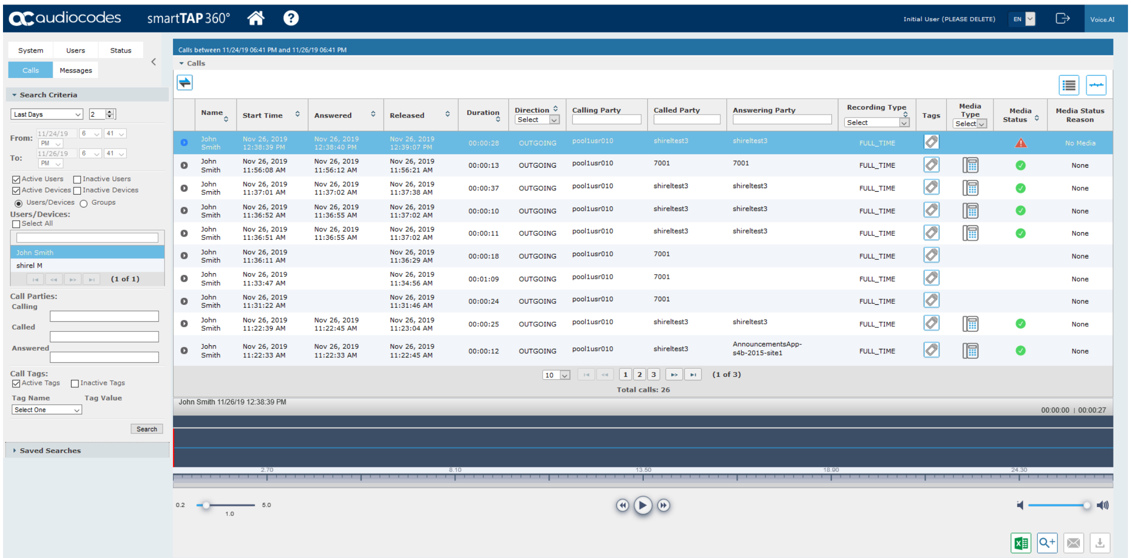
7. Selecting the Groups option changes the display below to show a list of Groups and Sub Groups (if the Search Sub Groups option is selected).

8. 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).

9. Optionally, specify a Calling, Called and/or Answered party.

10. 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 search for the last two days for user "John Smith"..

Figure 6-101: Retrieved Calls List for Specific User



Search Criteria

Last Days 2

From: 11/24/19 6 41 PM

To: 11/26/19 6 41 PM

☑ Active Users ☐ Inactive Users

☑ Active Devices ☐ Inactive Devices

● Users/Devices ○ Groups

Users/Devices:

☐ Select All

John Smith

shirel M

(1 of 1)

Call Parties:

Calling

Called

Answered

Call Tags:

☑ Active Tags ☐ Inactive Tags

Tag Name Tag Value

Select One

Calls between 11/24/19 06:41 PM and 11/26/19 06:41 PM

Calls

Name	Start Time	Answered	Released	Duration	Direction Select	Calling Party	Called Party	Answering Party	Recording Type Select	Tags	Media Type Select	Media Status	Media Status Reason
John Smith	Nov 26, 2019 12:38:39 PM	Nov 26, 2019 12:38:40 PM	Nov 26, 2019 12:39:07 PM	00:00:28	OUTGOING	pool1usr010	shireltest3	shireltest3	FULL_TIME			⚠	No Media
John Smith	Nov 26, 2019 11:56:08 AM	Nov 26, 2019 11:56:12 AM	Nov 26, 2019 11:56:21 AM	00:00:13	OUTGOING	pool1usr010	7001	7001	FULL_TIME			✓	None
John Smith	Nov 26, 2019 11:37:01 AM	Nov 26, 2019 11:37:02 AM	Nov 26, 2019 11:37:38 AM	00:00:37	OUTGOING	pool1usr010	shireltest3	shireltest3	FULL_TIME			✓	None
John Smith	Nov 26, 2019 11:36:52 AM	Nov 26, 2019 11:36:55 AM	Nov 26, 2019 11:37:02 AM	00:00:10	OUTGOING	pool1usr010	shireltest3	shireltest3	FULL_TIME			✓	None
John Smith	Nov 26, 2019 11:36:51 AM	Nov 26, 2019 11:36:55 AM	Nov 26, 2019 11:37:02 AM	00:00:11	OUTGOING	pool1usr010	shireltest3	shireltest3	FULL_TIME			✓	None
John Smith	Nov 26, 2019 11:36:11 AM		Nov 26, 2019 11:36:29 AM	00:00:18	OUTGOING	pool1usr010	7001		FULL_TIME				None
John Smith	Nov 26, 2019 11:33:47 AM		Nov 26, 2019 11:34:56 AM	00:01:09	OUTGOING	pool1usr010	7001		FULL_TIME				None
John Smith	Nov 26, 2019 11:31:22 AM		Nov 26, 2019 11:31:46 AM	00:00:24	OUTGOING	pool1usr010	7001		FULL_TIME				None
John Smith	Nov 26, 2019 11:22:39 AM	Nov 26, 2019 11:22:45 AM	Nov 26, 2019 11:23:04 AM	00:00:25	OUTGOING	pool1usr010	shireltest3	shireltest3	FULL_TIME			✓	None
John Smith	Nov 26, 2019 11:22:33 AM	Nov 26, 2019 11:22:33 AM	Nov 26, 2019 11:22:45 AM	00:00:12	OUTGOING	pool1usr010	shireltest3	AnnouncementsApp-s4b-2015-site1	FULL_TIME			✓	None

10 1 2 3 (1 of 3)

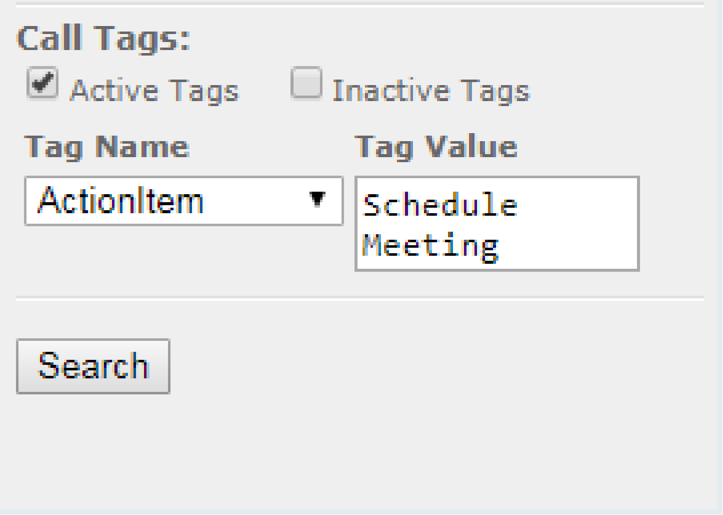
Total calls: 26

John Smith 11/26/19 12:38:39 PM

00:00:00 | 00:00:27

11. Optionally, specify a Call Tag & Value.

Figure 6-102: Call Tags



Call Tags:

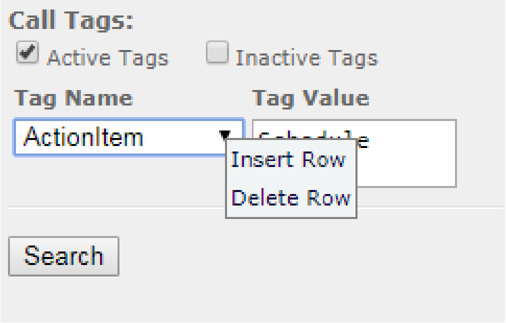
☑ Active Tags ☐ Inactive Tags

Tag Name Tag Value

ActionItem Schedule Meeting

12. 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 6-103: Call Tags

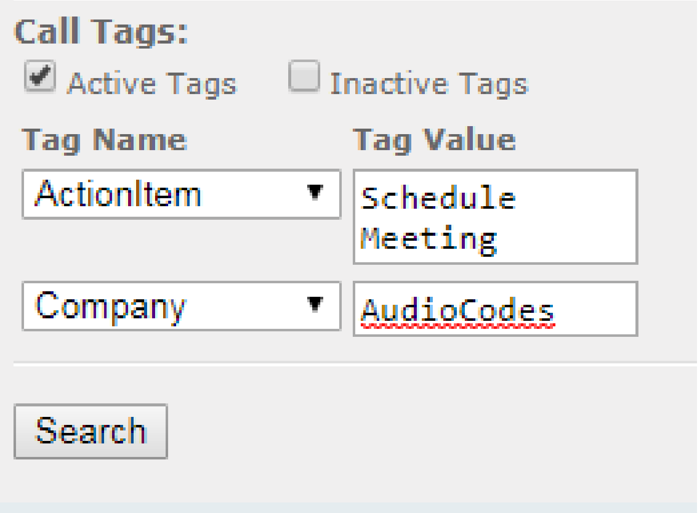


Call Tags:

☑ Active Tags ☐ Inactive Tags

Tag Name Tag Value

ActionItem Schedule



Call Tags:

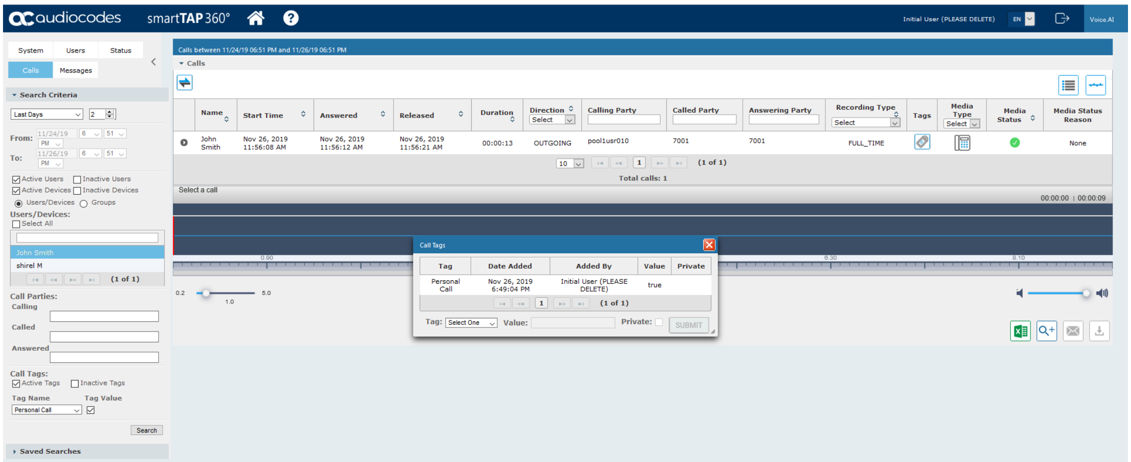
☑ Active Tags ☐ Inactive Tags

Tag Name	Tag Value
ActionItem ▼	Schedule Meeting
Company ▼	AudioCodes

Search

13. Ensure that the Active Tags check box is selected and then click Search to start the search for calls matching the search criteria; the Results are displayed in the Search Calls Results screen. The figure below shows an example of a retrieved call with an assigned Call Tag Action Item with value 'Personal Call' *. Calls with Call Tag Action Item with note value 'Personal Call' value are retrieved for the specified user and specified time frame. Note that this tag is of type "boolean"and therefore the "Tag Value" check box must be selected in order to retrieve results.

Figure 6-104: Search Calls Results



audiocodes smartTAP 360° Initial User (PLEASE DELETE) EN Voice.AI

System Users Status

Calls Messages

Search Criteria

Last Days 2

From: 11/24/19 6 51 PM

To: 11/26/19 6 51 PM

☑ Active Users ☐ Inactive Users

☑ Active Devices ☐ Inactive Devices

● Users/Devices ○ Groups

Users/Devices:

☐ Select All

John Smith

shirel M

(1 of 1)

Call Parties:

Calling

Called

Answered

Call Tags:

☑ Active Tags ☐ Inactive Tags

Tag Name Tag Value

Personal Call ☑

Search

Saved Searches

Calls between 11/24/19 06:51 PM and 11/26/19 06:51 PM

Calls

	Name	Start Time	Answered	Released	Duration	Direction	Calling Party	Called Party	Answering Party	Recording Type	Tags	Media Type	Media Status	Media Status Reason
						Select				Select		Select		
	John Smith	Nov 26, 2019 11:56:08 AM	Nov 26, 2019 11:56:12 AM	Nov 26, 2019 11:56:21 AM	00:00:13	OUTGOING	pool1usr010	7001	7001	FULL_TIME			✓	None

10 1 (1 of 1)

Total calls: 1

Select a call

00:00:00 | 00:00:09

Call Tags

Tag	Date Added	Added By	Value	Private
Personal Call	Nov 26, 2019 6:49:04 PM	Initial User (PLEASE DELETE)	true	

1 (1 of 1)

Tag: Select One Value: Private: ☐ SUBMIT

Notice the difference in the search results displayed in the above figure and how wild cards can affect the results.

14. To delete calls, select the button adjacent to each call that you wish to delete. The button becomes red. For more information, see Deleting Calls and Instant Messages on page 146.

Table 6-42: 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.
Release Calls Details	Release Cause of the Original Call. Applicable to Skype For Business. Example: "Call failed to establish due to a media connectivity...;22 "Action initiated by user";51004;.
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.

Field	Description
🖥	Indicates that the Desktop Sharing 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.
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.
Tags	Identifies whether tag have been defined for the call as follows
🏷	Indicates that no tags are associated with a recording
🏷	Indicates that a tag has been associated with a recording.
Media Status Reason	Corresponding Media Reason

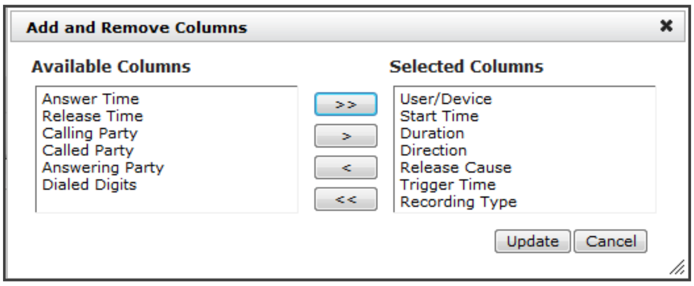
Field	Description
None	None - Indicated when there are no media files and the call was not answered i.e. Abandoned or Missed.
☑	None – There are no reasons.
⚠	Silent Media – Indicates when media files associated with the call are silent; the packets were received however didn't carry audio.
⚠	■ **No Media** – Indicates that there are no media files associated with the call; however, the call was answered. ■ **No License** - Indicates that the media cannot record as a result of no licenses being available. ■ **No Packets** - Indicates that no packets are received for media recording on one or both sides of the call.

➢ 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 6-105: Add/Remove Columns from the Search Call Results Screen



Add and Remove Columns

Available Columns

Answer Time
Release Time
Calling Party
Called Party
Answering Party
Dialed Digits

Selected Columns

User/Device
Start Time
Duration
Direction
Release Cause
Trigger Time
Recording Type

Table 6-43: Add and Remove Columns – Field Descriptions

Field	Description
Available Columns	List of columns that can be added to the search results table.

Field	Description
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.
<	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 the table below as reference.
3. Click Update to apply the changes and close the screen.

Table 6-44: Add and Remove Columns

Field	Description
User / Device	Targeted User or Device.
Start Time	Initial off-hook or offering of the call.
Answer Time	The time at which the call was answered.
Release Time	The time at which the call was disconnected.
Trigger Time	The time at which the user manually initiated Record or Save on Demand.
Duration	Total duration of the call, from the Start Time to the Release Time.
Calling Party	The call initiator.

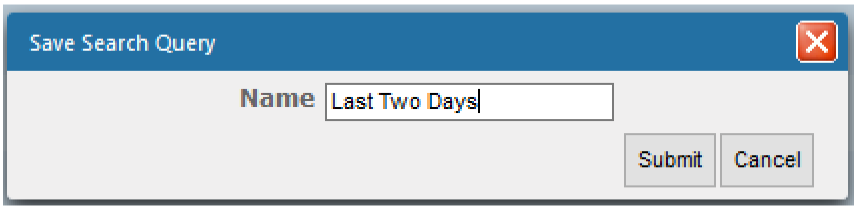
Field	Description	
Called Party	The intended recipient of the call.	
Answering Party	The party who ultimately answered the call.	
Dialed Digits	Any dialed digits to set up the call (only required for PSTN gateway calls).	
Direction	Inbound or Outbound.	
Release Cause	Normal	Answered call.
	Missed	Incoming call to targeted user that wasn’t answered.
	Abandoned	Outgoing call from targeted user that wasn’t completed.
	Conferenced *	Indicates the call leg was released as a result of the call being elevated to a conference call.
	Transferred *	Indicates the call leg was released as a result of being transferred.
Recording Type	**Full Time** **Record on Demand** **Save on Demand**	
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.	
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.	
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 Skype for Business client.	

Field	Description
Media Status Reason	Corresponding Media Reason
Tags	Identifies whether a tag has been assigned to the call record.
Release Calls Details	Release Cause of the Original Call. Applicable to Skype For Business. Example: ‘51004; reason=""“Action initiated by user";51004.

Saving Search Queries

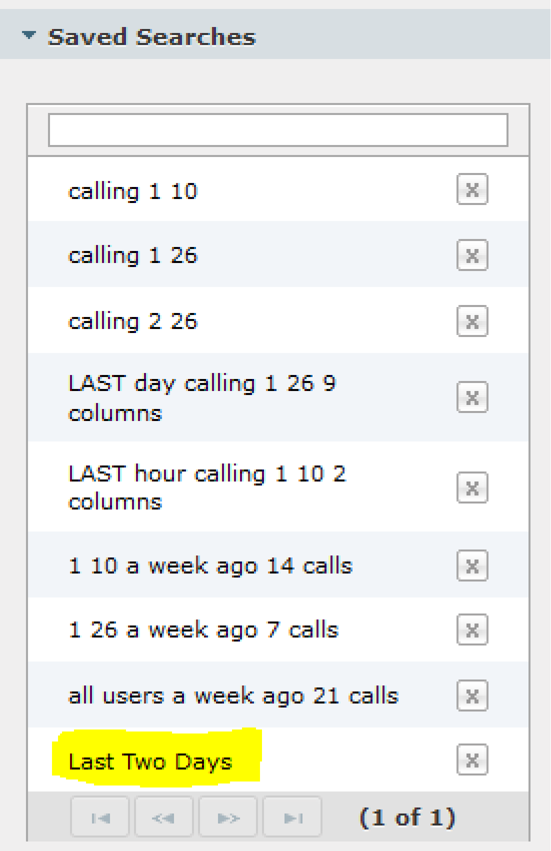
You can save search criteria as a query and then later retrieve it. Save the search criteria by selecting the 🔍+ in the bottom right-hand corner of the screen. The saved query is added to the Saved Searches pane in the bottom left-hand corner of the screen. In the figure below "Last Two Days" is added as the saved query.

Figure 6-106: Save Search Query



Save Search Query

Name: Last Two Days



Saved Searches

- calling 1 10
- calling 1 26
- calling 2 26
- LAST day calling 1 26 9 columns
- LAST hour calling 1 10 2 columns
- 1 10 a week ago 14 calls
- 1 26 a week ago 7 calls
- all users a week ago 21 calls
- Last Two Days

(1 of 1)

Deleting Calls and Instant Messages

SmartTAP 360° is deployed in several recording scenarios such as compliance, quality monitoring and for malicious call recordings. While regulatory compliance requires that recordings are deleted automatically after a regulated time frame, quality monitoring scenarios requires the ability to manually delete recordings. Consequently, calls and instant messages conversations can be deleted on demand by users with the appropriate permissions in security profiles (see .Managing Security Profiles on page 108).

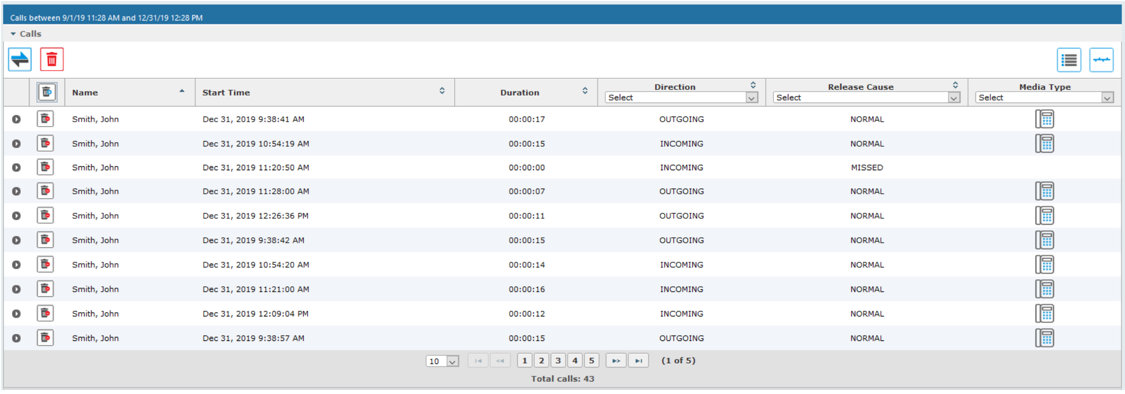
- This feature is enabled through the SmartTAP 360° Call Deletion license (SW/SMTP/CALLDEL)
- If a user in on Legal Hold, their Calls and Instant Messaging cannot be deleted (see Managing Users on page 101)
- When calls or messages are deleted, any associated evaluations are also deleted.

➢ To delete calls:

1. Search for calls according to desired search criteria (see Searching for Calls on page 135).
2. Select the button adjacent to each call that you wish to delete. The button becomes red .

Only the filtered and selected recordings are deleted.

Figure 6-107: Delete Calls



Calls between 9/1/19 11:28 AM and 12/31/19 12:28 PM

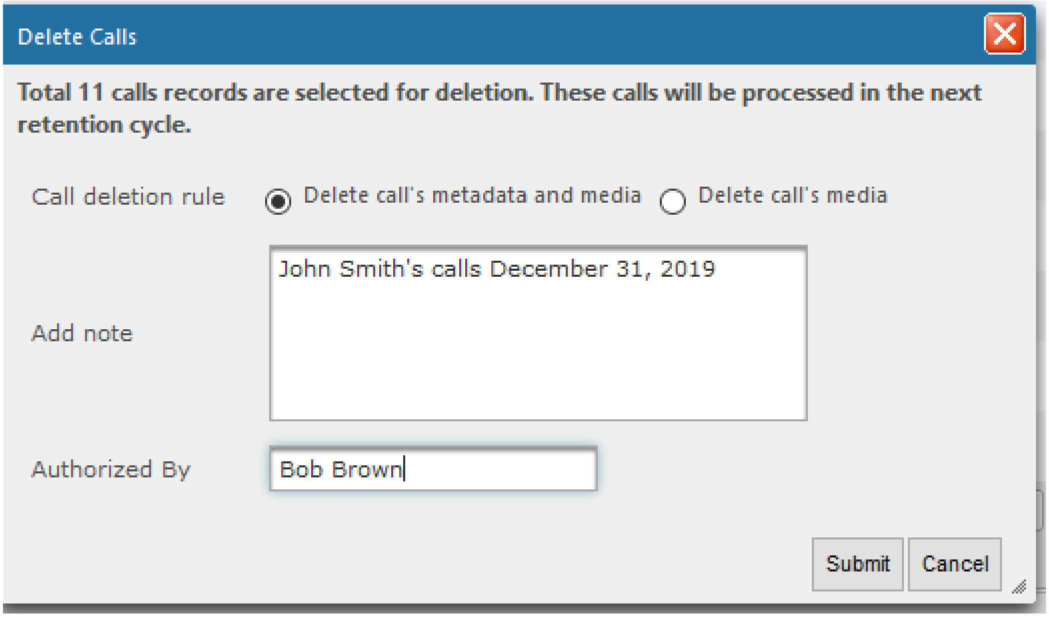
▾ Calls

		Name	Start Time	Duration	Direction Select	Release Cause Select	Media Type Select
		Smith, John	Dec 31, 2019 9:38:41 AM	00:00:17	OUTGOING	NORMAL	☎
		Smith, John	Dec 31, 2019 10:54:19 AM	00:00:15	INCOMING	NORMAL	☎
		Smith, John	Dec 31, 2019 11:20:50 AM	00:00:00	INCOMING	MISSED	
		Smith, John	Dec 31, 2019 11:28:00 AM	00:00:07	OUTGOING	NORMAL	☎
		Smith, John	Dec 31, 2019 12:26:36 PM	00:00:11	OUTGOING	NORMAL	☎
		Smith, John	Dec 31, 2019 9:38:42 AM	00:00:15	OUTGOING	NORMAL	☎
		Smith, John	Dec 31, 2019 10:54:20 AM	00:00:14	INCOMING	NORMAL	☎
		Smith, John	Dec 31, 2019 11:21:00 AM	00:00:16	INCOMING	NORMAL	☎
		Smith, John	Dec 31, 2019 12:09:04 PM	00:00:12	INCOMING	NORMAL	☎
		Smith, John	Dec 31, 2019 9:38:57 AM	00:00:15	OUTGOING	NORMAL	☎

Total calls: 43

3. Click , a confirmation dialog is displayed:

Figure 6-108: Delete Calls Confirmation



Total 11 calls records are selected for deletion. These calls will be processed in the next retention cycle.

Call deletion rule ● Delete call's metadata and media ○ Delete call's media

Add note: John Smith's calls December 31, 2019

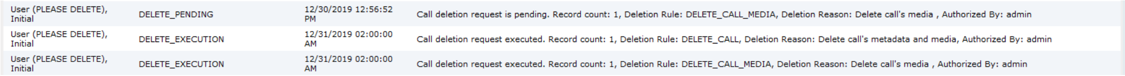
Authorized By: Bob Brown

You can add a note and also indicate who authorized the deletion.

4. Click **Submit**. You are prompted to confirm the deletion.

You can monitor the deletion process in the Audit Trails page:

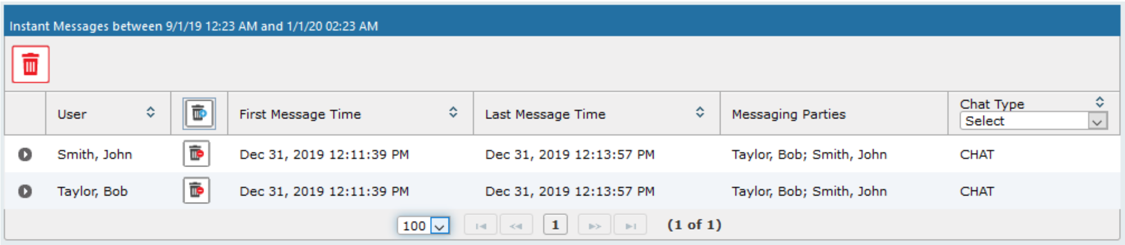
Figure 6-109: Audit Trail Page



User (PLEASE DELETE), Initial	DELETE_PENDING	12/30/2019 12:56:52 PM	Call deletion request is pending. Record count: 1, Deletion Rule: DELETE_CALL_MEDIA, Deletion Reason: Delete call's media , Authorized By: admin
User (PLEASE DELETE), Initial	DELETE_EXECUTION	12/31/2019 02:00:00 AM	Call deletion request executed. Record count: 1, Deletion Rule: DELETE_CALL, Deletion Reason: Delete call's metadata and media, Authorized By: admin
User (PLEASE DELETE), Initial	DELETE_EXECUTION	12/31/2019 02:00:00 AM	Call deletion request executed. Record count: 1, Deletion Rule: DELETE_CALL_MEDIA, Deletion Reason: Delete call's media , Authorized By: admin

Instant Messages can be deleted in a similar manner.

Figure 6-110: Deleting Instant Messages



Instant Messages between 9/1/19 12:23 AM and 1/1/20 02:23 AM

	User		First Message Time	Last Message Time	Messaging Parties	Chat Type Select
●	Smith, John		Dec 31, 2019 12:11:39 PM	Dec 31, 2019 12:13:57 PM	Taylor, Bob; Smith, John	CHAT
●	Taylor, Bob		Dec 31, 2019 12:11:39 PM	Dec 31, 2019 12:13:57 PM	Taylor, Bob; Smith, John	CHAT

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.

The Web browser support for the SmartTAP 360° 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 6-111: Audio Player Screen

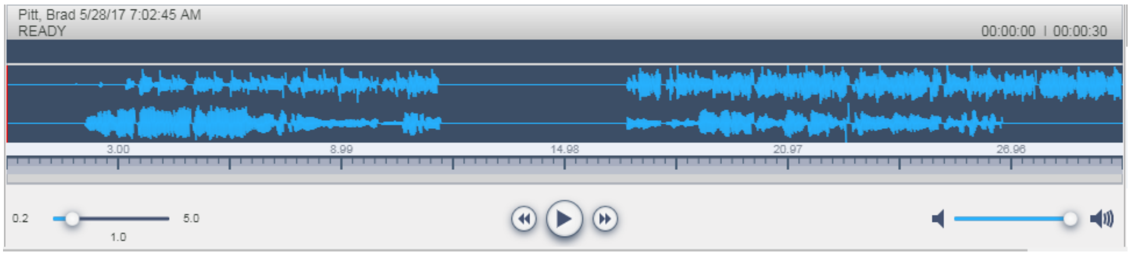
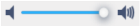
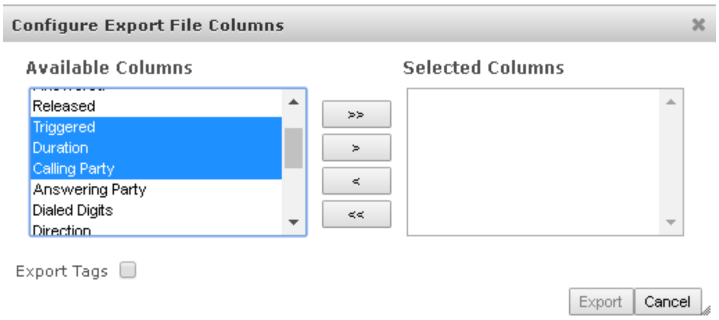


Table 6-45: Player Screen Overview

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	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.
0.2 —○— 5.0 1.0	Playback speed in milliseconds.
X	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.  Configure Export File Columns Available Columns Selected Columns Released Triggered Duration Calling Party Answering Party Dialed Digits Direction >> > < << Export Tags □ Export Cancel
✉	Email audio call information. When this option is selected, the Email Audio dialog opens. See Sending Email on page 103
🔍+	Save search call query. You can save the search query results and then easily retrieve these call details at a later time. See Searching for Calls on page 135
⤓	Download call information to your PC. When this option is selected, the Download Media dialog opens. See Downloading Call Recordings on page 159.

Listening to Call and Viewing Call Video

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

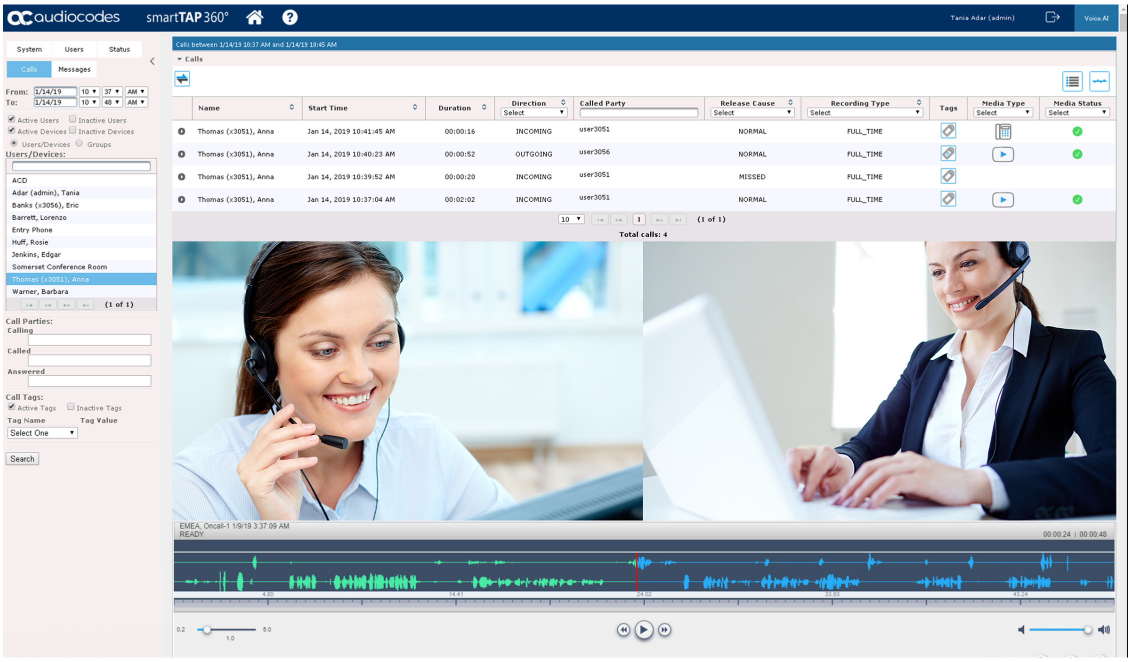
➢ To listen to a call and view call video:

1. Follow the instructions described in Searching for Calls on page 135 Searching for Calls on page 135to 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 ⏸ PAUSE while the call is playing, to allow the administrator to pause the player while playing the audio or video.

Figure 6-112: Viewing Video



Calls between 1/14/19 10:37 AM and 1/14/19 10:45 AM

Calls

	Name	Start Time	Duration	Direction	Called Party	Release Cause	Recording Type	Tags	Media Type	Media Status
▶	Thomas (x3051), Anna	Jan 14, 2019 10:41:45 AM	00:00:16	INCOMING	user3051	NORMAL	FULL_TIME	🏷	☎	✓
▶	Thomas (x3051), Anna	Jan 14, 2019 10:40:23 AM	00:00:52	OUTGOING	user3056	NORMAL	FULL_TIME	🏷	▶	✓
▶	Thomas (x3051), Anna	Jan 14, 2019 10:39:52 AM	00:00:20	INCOMING	user3051	MISSED	FULL_TIME	🏷		
▶	Thomas (x3051), Anna	Jan 14, 2019 10:37:04 AM	00:02:02	INCOMING	user3051	NORMAL	FULL_TIME	🏷	▶	✓

10 (1 of 1)

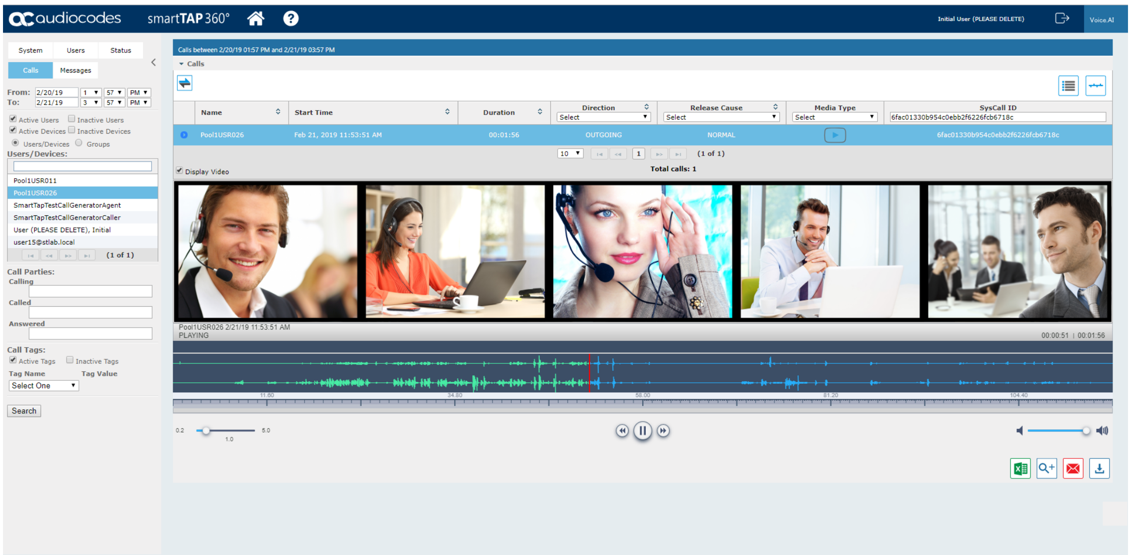
Total calls: 4

EMEA, Oncall-1 1/9/19 3:37:09 AM
READY
00:00:24 | 00:00:48

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).

You can also view multiple participants in a conference as shown in the figure below:

Figure 6-113: Multiple Conference Participants



Calls between 2/20/19 01:57 PM and 2/21/19 03:57 PM

Calls

	Name	Start Time	Duration	Direction	Release Cause	Media Type	SysCall ID
				Select	Select	Select	6fac01330b954c0ebb2f6226fcb6718c
▶	Pool1USR026	Feb 21, 2019 11:53:51 AM	00:01:56	OUTGOING	NORMAL	▶	6fac01330b954c0ebb2f6226fcb6718c

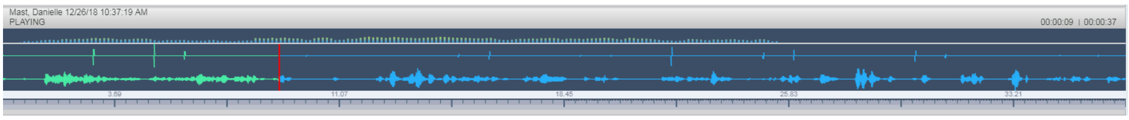
10 (1 of 1)

☑ Display Video

Total calls: 1

Pool1USR026 2/21/19 11:53:51 AM
PLAYING
00:00:51 | 00:01:56

Figure 6-114: Playback Audio Signaling Data



Mast, Danielle 12/26/18 10:37:19 AM
PLAYING

00:00:09 | 00:00:37

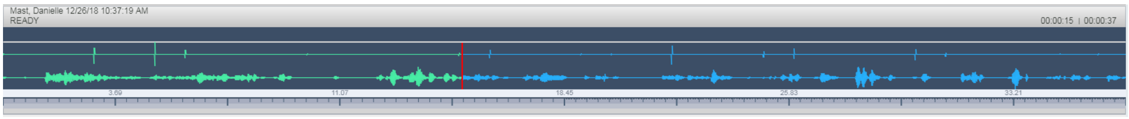
Information at the top-left hand side of the screen includes the user name, date and time and status e.g. “PLAYING”. On the top-right hand side of the screen includes the elapsed playback time and the total playing time.

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 6-115: Random Selection Point in Call Recording

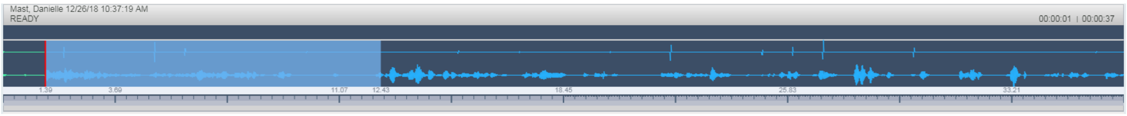


Mast, Danielle 12/26/18 10:37:19 AM
READY

00:00:15 | 00:00:37

   - 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 6-116: Highlighted Segment in Call Recording



Mast, Danielle 12/26/18 10:37:19 AM
READY

00:00:01 | 00:00:37

   - 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.

Skype for Business and Teams Desktop Sharing

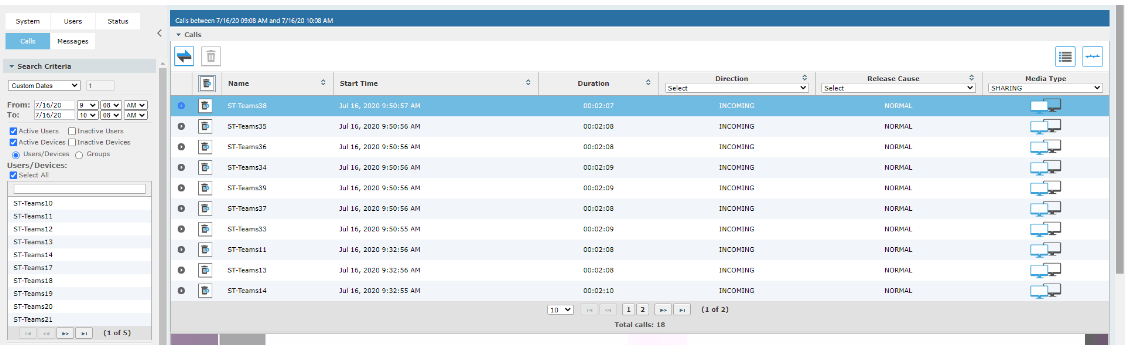
This section describes how to playback a desktop sharing recording.

➢ To playback desktop sharing recording :

1. Follow the instructions described in Searching for Calls on page 135 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 6-117: Media Type-Desktop Sharing with Teams



Custom Dates 1

From: 7/16/20 9 08 AM
To: 7/16/20 10 08 AM

☑ Active Users ☐ Inactive Users
☑ Active Devices ☐ Inactive Devices
● Users/Devices ○ Groups

Users/Devices:
☑ Select All

ST-Teams10
ST-Teams11
ST-Teams12
ST-Teams13
ST-Teams14
ST-Teams17
ST-Teams18
ST-Teams19
ST-Teams20
ST-Teams21
(1 of 5)

Calls between 7/16/20 09:08 AM and 7/16/20 10:08 AM

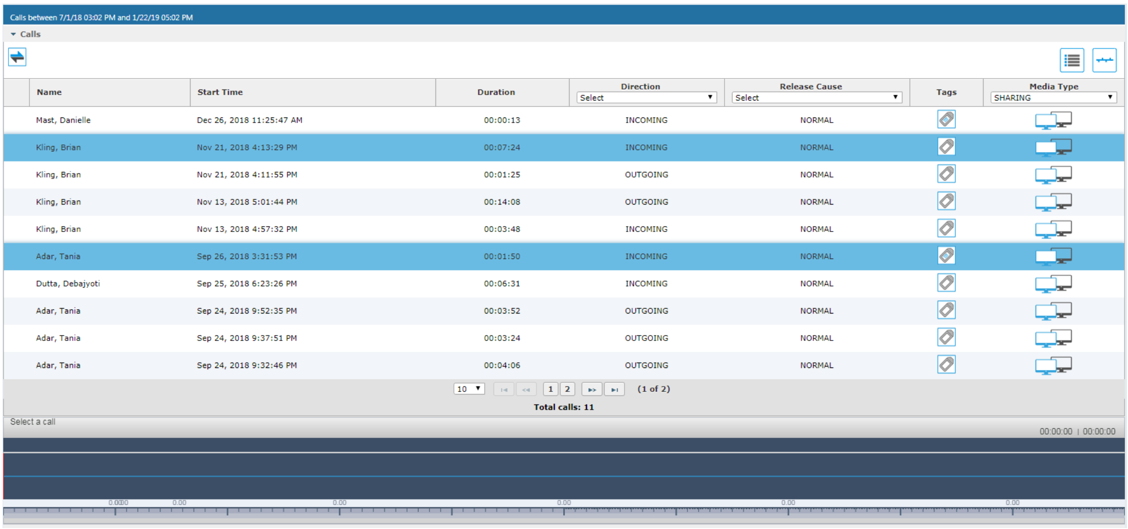
Calls

Name	Start Time	Duration	Direction Select	Release Cause Select	Media Type SHARING
ST-Teams38	Jul 16, 2020 9:50:57 AM	00:02:07	INCOMING	NORMAL	
ST-Teams35	Jul 16, 2020 9:50:56 AM	00:02:08	INCOMING	NORMAL	
ST-Teams36	Jul 16, 2020 9:50:56 AM	00:02:08	INCOMING	NORMAL	
ST-Teams34	Jul 16, 2020 9:50:56 AM	00:02:09	INCOMING	NORMAL	
ST-Teams39	Jul 16, 2020 9:50:56 AM	00:02:09	INCOMING	NORMAL	
ST-Teams37	Jul 16, 2020 9:50:56 AM	00:02:08	INCOMING	NORMAL	
ST-Teams33	Jul 16, 2020 9:50:55 AM	00:02:09	INCOMING	NORMAL	
ST-Teams11	Jul 16, 2020 9:32:56 AM	00:02:08	INCOMING	NORMAL	
ST-Teams13	Jul 16, 2020 9:32:56 AM	00:02:08	INCOMING	NORMAL	
ST-Teams14	Jul 16, 2020 9:32:55 AM	00:02:10	INCOMING	NORMAL	

10 1 2 (1 of 2)

Total calls: 18

Figure 6-118: Media Type-Desktop Sharing with Skype for Business



Calls between 7/1/18 03:02 PM and 1/22/19 05:02 PM

Calls

Name	Start Time	Duration	Direction Select	Release Cause Select	Tags	Media Type SHARING
Mast, Danielle	Dec 26, 2018 11:25:47 AM	00:00:13	INCOMING	NORMAL		
Kling, Brian	Nov 21, 2018 4:13:29 PM	00:07:24	INCOMING	NORMAL		
Kling, Brian	Nov 21, 2018 4:11:55 PM	00:01:25	OUTGOING	NORMAL		
Kling, Brian	Nov 13, 2018 5:01:44 PM	00:14:08	OUTGOING	NORMAL		
Kling, Brian	Nov 13, 2018 4:57:32 PM	00:03:48	INCOMING	NORMAL		
Adar, Tania	Sep 26, 2018 3:31:53 PM	00:01:50	INCOMING	NORMAL		
Dutta, Debajyoti	Sep 25, 2018 6:23:26 PM	00:06:31	INCOMING	NORMAL		
Adar, Tania	Sep 24, 2018 9:52:35 PM	00:03:52	OUTGOING	NORMAL		
Adar, Tania	Sep 24, 2018 9:37:51 PM	00:03:24	OUTGOING	NORMAL		
Adar, Tania	Sep 24, 2018 9:32:46 PM	00:04:06	OUTGOING	NORMAL		

10 1 2 (1 of 2)

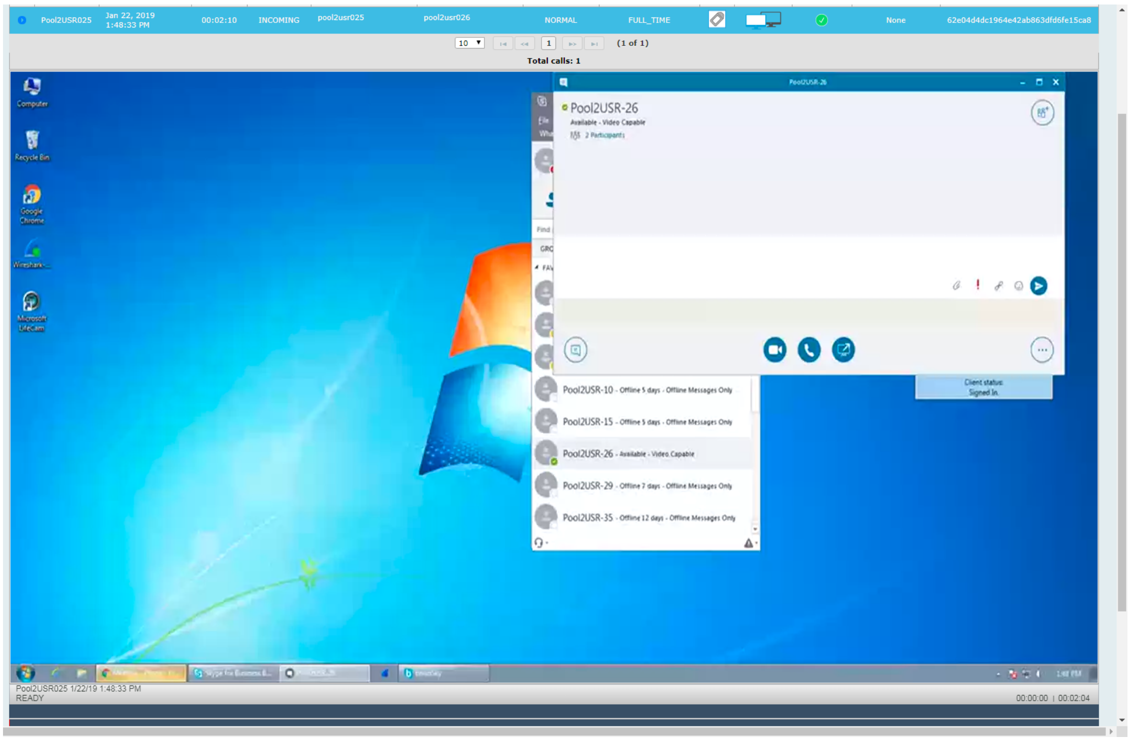
Total calls: 11

Select a call

00:00:00 | 00:00:00

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

Figure 6-119: Desktop Sharing Recording

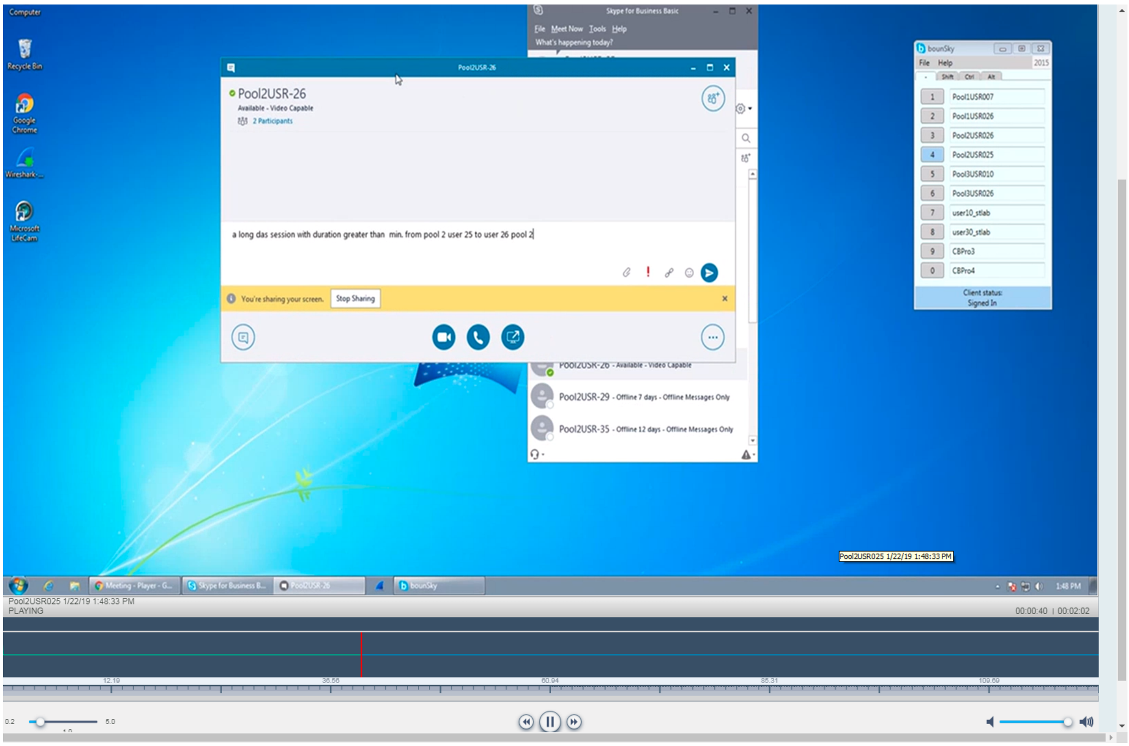


Pool2USR025 Jan 22, 2019 1:48:33 PM 00:02:10 INCOMING pool2usr025 pool2usr026 NORMAL FULL_TIME None 62e04d4dc1964e42ab863dfd6fe15ca8

Total calls: 1

10
1
(1 of 1)
Pool2USR-26
Available - Video Capable
2 Participants
Pool2USR-10 - Offline 5 days - Offline Messages Only
Pool2USR-15 - Offline 5 days - Offline Messages Only
Pool2USR-26 - Available - Video Capable
Pool2USR-29 - Offline 7 days - Offline Messages Only
Pool2USR-35 - Offline 12 days - Offline Messages Only
Client status: Signed In
Pool2USR025 1/22/19 1:48:33 PM
READY
00:00:00 | 00:02:04

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



a long das session with duration greater than min. from pool 2 user 25 to user 26 pool 2

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.

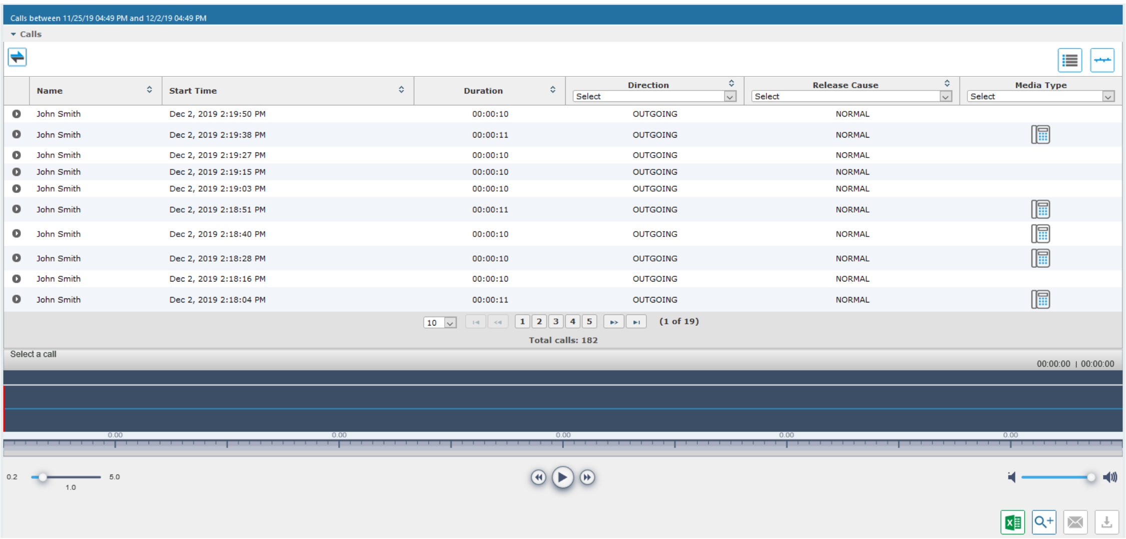
Time Line View

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 Searching for Calls on page 135Searching for Calls on page 135 to search for calls.

Figure 6-120: Calls List



Calls between 11/25/19 04:49 PM and 12/2/19 04:49 PM

Calls

	Name	Start Time	Duration	Direction Select	Release Cause Select	Media Type Select
●	John Smith	Dec 2, 2019 2:19:50 PM	00:00:10	OUTGOING	NORMAL	
●	John Smith	Dec 2, 2019 2:19:38 PM	00:00:11	OUTGOING	NORMAL	☎
●	John Smith	Dec 2, 2019 2:19:27 PM	00:00:10	OUTGOING	NORMAL	
●	John Smith	Dec 2, 2019 2:19:15 PM	00:00:10	OUTGOING	NORMAL	
●	John Smith	Dec 2, 2019 2:19:03 PM	00:00:10	OUTGOING	NORMAL	
●	John Smith	Dec 2, 2019 2:18:51 PM	00:00:11	OUTGOING	NORMAL	☎
●	John Smith	Dec 2, 2019 2:18:40 PM	00:00:10	OUTGOING	NORMAL	☎
●	John Smith	Dec 2, 2019 2:18:28 PM	00:00:10	OUTGOING	NORMAL	☎
●	John Smith	Dec 2, 2019 2:18:16 PM	00:00:10	OUTGOING	NORMAL	
●	John Smith	Dec 2, 2019 2:18:04 PM	00:00:11	OUTGOING	NORMAL	☎

10 1 2 3 4 5 (1 of 19)

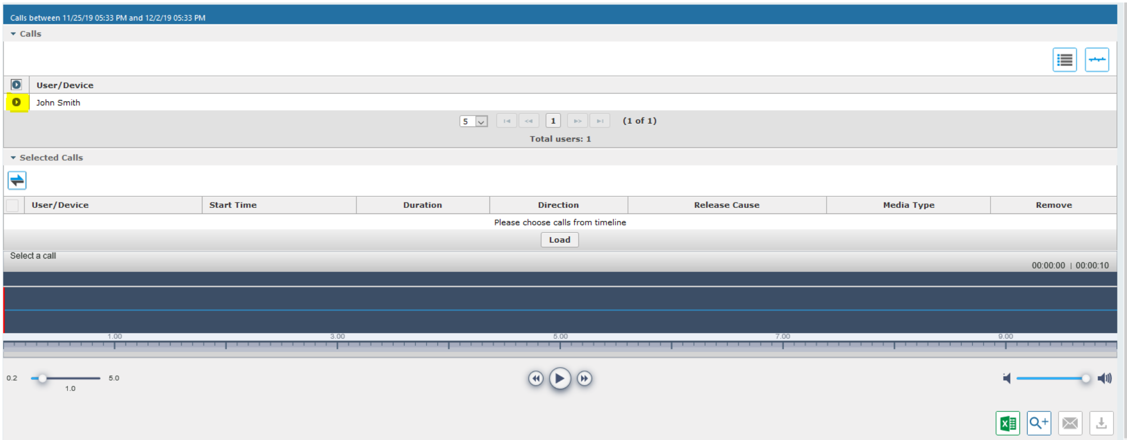
Total calls: 182

Select a call

00:00:00 | 00:00:00

2. Select the Timeline view icon . A screen similar to the following is displayed:

Figure 6-121: Select User in Timeline View



Calls between 11/25/19 05:33 PM and 12/2/19 05:33 PM

Calls

	User/Device
●	John Smith

5 1 (1 of 1)

Total users: 1

Selected Calls

	User/Device	Start Time	Duration	Direction	Release Cause	Media Type	Remove

Please choose calls from timeline

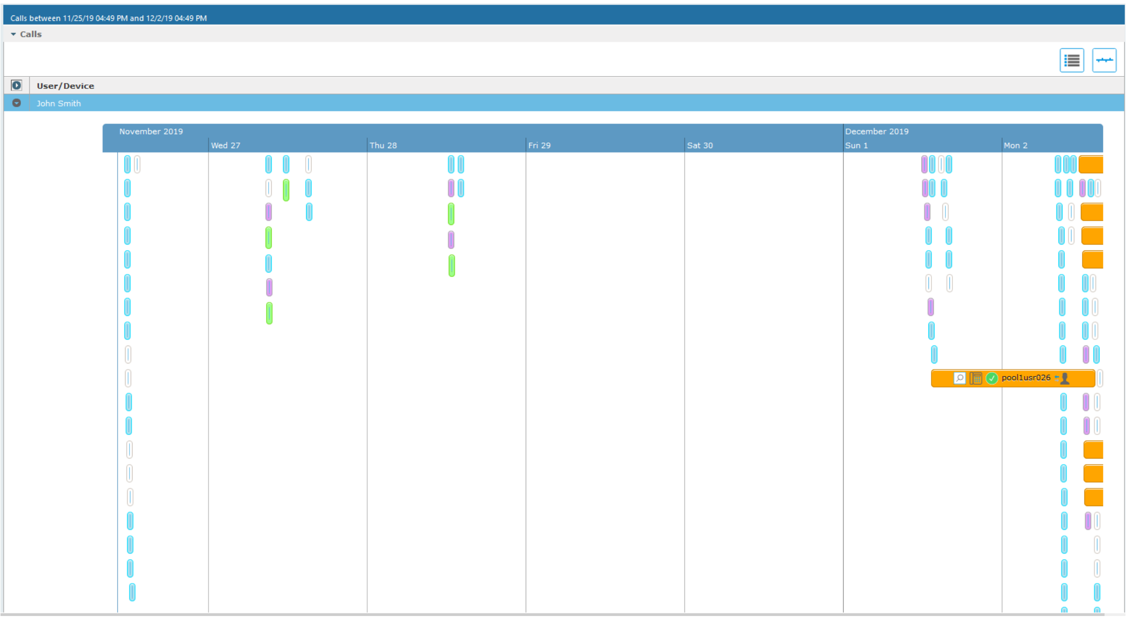
Load

Select a call

00:00:00 | 00:00:10

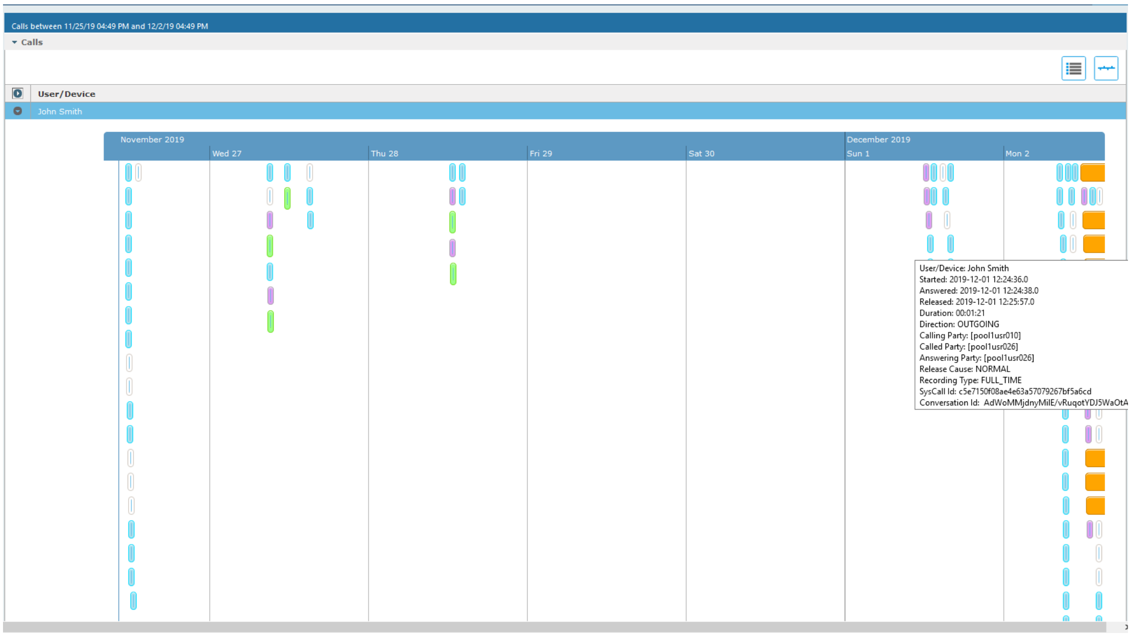
3. Select the arrow adjacent to the User/Device whose timeline you wish to view. The Calls List is displayed:

Figure 6-122: User Timeline



4. Hover over a call event to view details of the call.

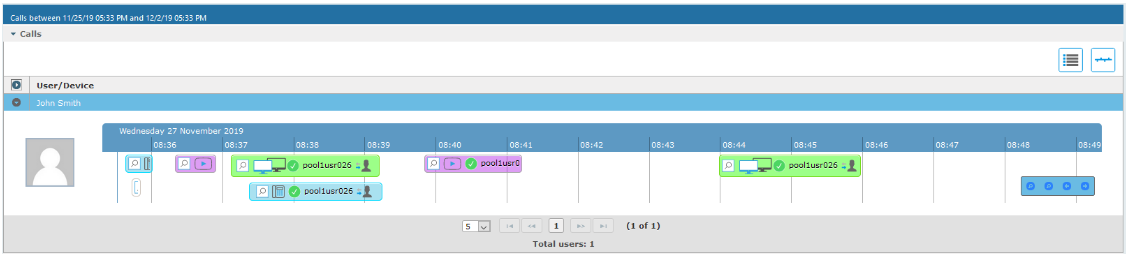
Figure 6-123: Call Event Details



User/Device: John Smith
Started: 2019-12-01 12:24:36.0
Answered: 2019-12-01 12:24:38.0
Released: 2019-12-01 12:25:57.0
Duration: 00:01:21
Direction: OUTGOING
Calling Party: [pool1usr010]
Called Party: [pool1usr026]
Answering Party: [pool1usr026]
Release Cause: NORMAL
Recording Type: FULL_TIME
SysCall Id: c5e7150f08ae4e63a57079267bf5a6cd
Conversation Id: AdWoMMjdnyMilE/vRuqotYDJ5WaOtA

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

Figure 6-124: Zoom In



Calls between 11/25/19 05:33 PM and 12/2/19 05:33 PM

Calls

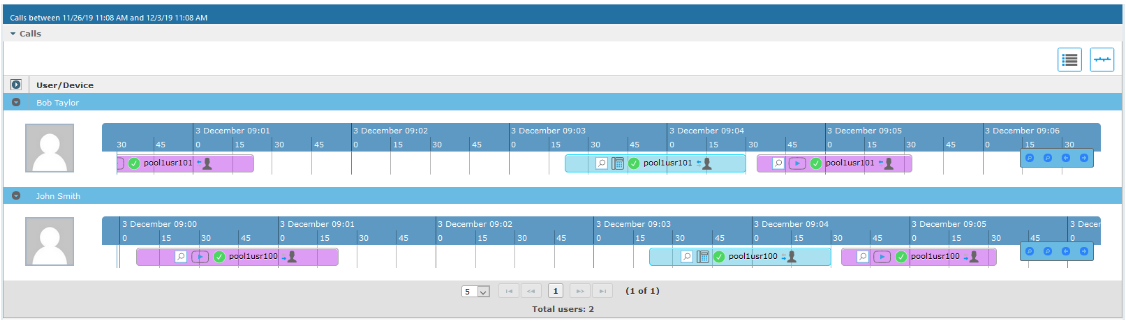
User/Device

John Smith

Total users: 1

- In timeline view, the calls are grouped according to their target type. Each target type is represented by a different color (see table below). 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 the player by clicking an icon in the timeline and then clicking the Load button.

Figure 6-125: Call Events from Multiple Timelines



Calls between 11/26/19 11:08 AM and 12/3/19 11:08 AM

Calls

User/Device

Bob Taylor

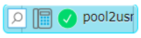
John Smith

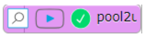
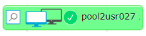
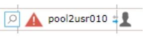
Total users: 2

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.
- If multiple selected segments include video or Desktop Sharing, the total playback time should not exceed six hours, otherwise the total playback time can be up to 24 hours.
- Only calls of different types can overlap:
  - An Audio call segment can overlap with a Desktop Sharing call segment
  - An Audio Video call segment can overlap with a Desktop Sharing call segment
  - An Audio call segment can't overlap with another Audio or Audio Video call segment
  - A Desktop Sharing call segment can't overlap with another Desktop Sharing call segment

Table 6-46: Call Events Description

Media Type	Description
 pool2usr	Represents an Audio call.

Media Type	Description
 pool2u	Represents a Video call
 pool2usr027	Represents a Desktop Sharing call
 pool2usr010	Represents a call that has no media. When a call is abandoned or missed, this target is displayed without the red warning.

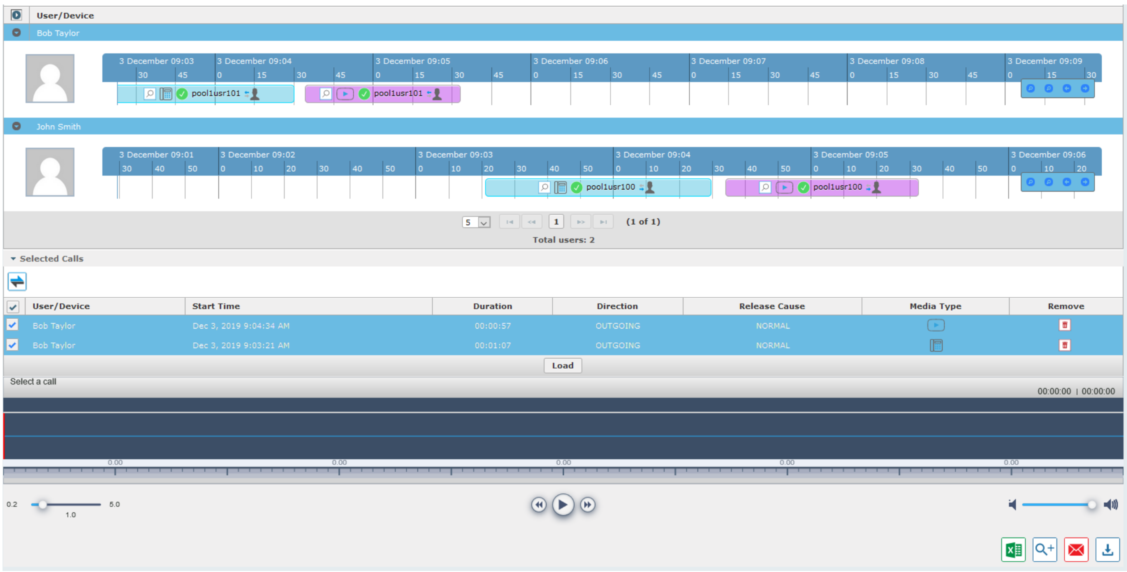
Each event includes different call information statuses as shown in the table below:

Table 6-47: 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.

1. Select the check box adjacent to each call that you wish to playback and click **Load**. The Media Player is loaded.

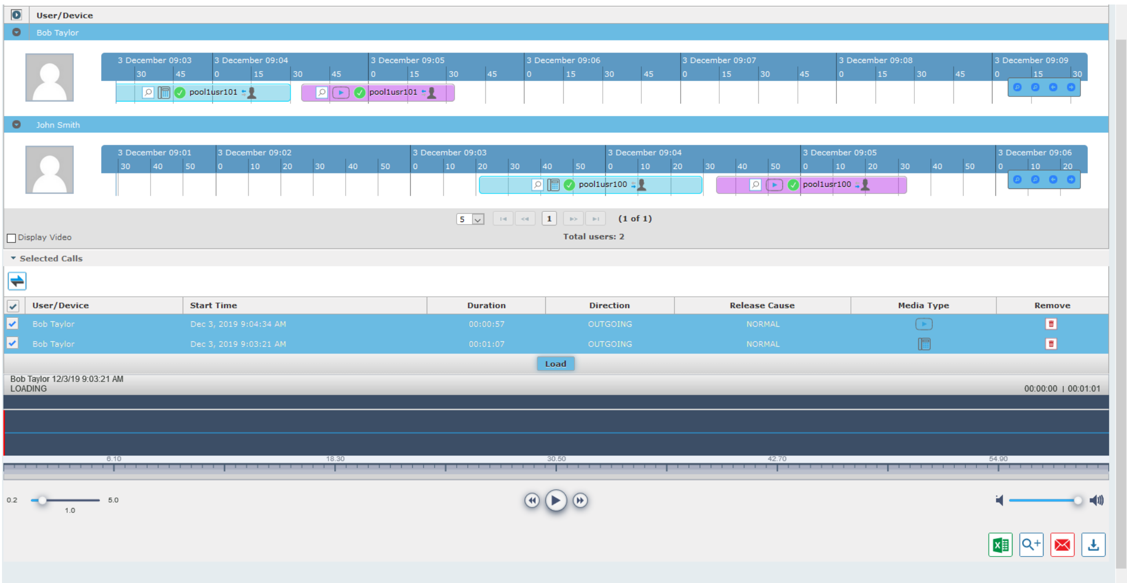
Figure 6-126: Load Media Player



☑	User/Device	Start Time	Duration	Direction	Release Cause	Media Type	Remove
☑	Bob Taylor	Dec 3, 2019 9:04:34 AM	00:00:57	OUTGOING	NORMAL	▶	✕
☑	Bob Taylor	Dec 3, 2019 9:03:21 AM	00:01:07	OUTGOING	NORMAL	▨	✕

The selected files are loaded to the Media Player.

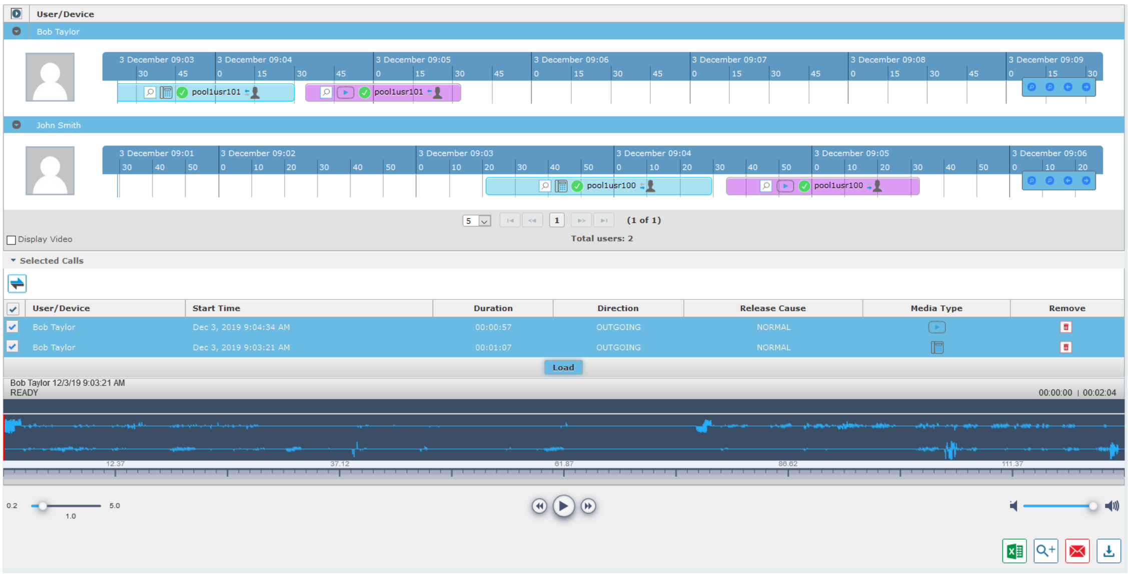
Figure 6-127: Loading Files to Media Player



☑	User/Device	Start Time	Duration	Direction	Release Cause	Media Type	Remove
☑	Bob Taylor	Dec 3, 2019 9:04:34 AM	00:00:57	OUTGOING	NORMAL	▶	✕
☑	Bob Taylor	Dec 3, 2019 9:03:21 AM	00:01:07	OUTGOING	NORMAL	▨	✕

Bob Taylor 12/3/19 9:03:21 AM
LOADING

Figure 6-128: Files Ready to Play



☑	User/Device	Start Time	Duration	Direction	Release Cause	Media Type	Remove
☑	Bob Taylor	Dec 3, 2019 9:04:34 AM	00:00:57	OUTGOING	NORMAL	▶	🗑
☑	Bob Taylor	Dec 3, 2019 9:03:21 AM	00:01:07	OUTGOING	NORMAL	▤	🗑

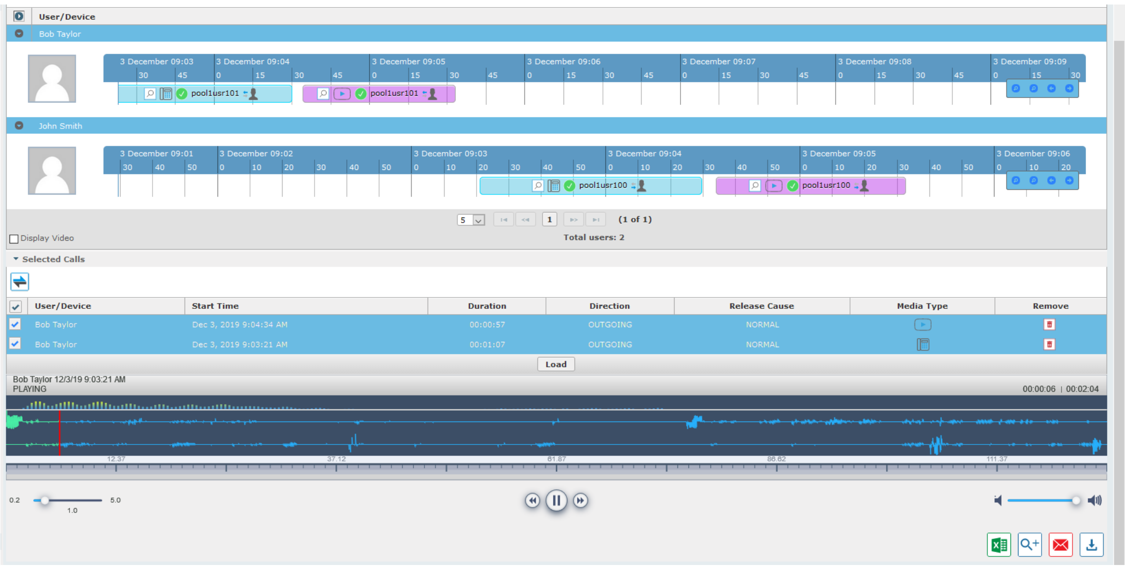
Load

Bob Taylor 12/3/19 9:03:21 AM
READY

00:00:00 | 00:02:04

2. Click ▶ to play the selected call.

Figure 6-129: Play Call



☑	User/Device	Start Time	Duration	Direction	Release Cause	Media Type	Remove
☑	Bob Taylor	Dec 3, 2019 9:04:34 AM	00:00:57	OUTGOING	NORMAL	▶	🗑
☑	Bob Taylor	Dec 3, 2019 9:03:21 AM	00:01:07	OUTGOING	NORMAL	▤	🗑

Load

Bob Taylor 12/3/19 9:03:21 AM
PLAYING

00:00:06 | 00:02:04

Downloading Call Recordings

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

Download with 'Display Video' selected is limited to five concurrent sessions.

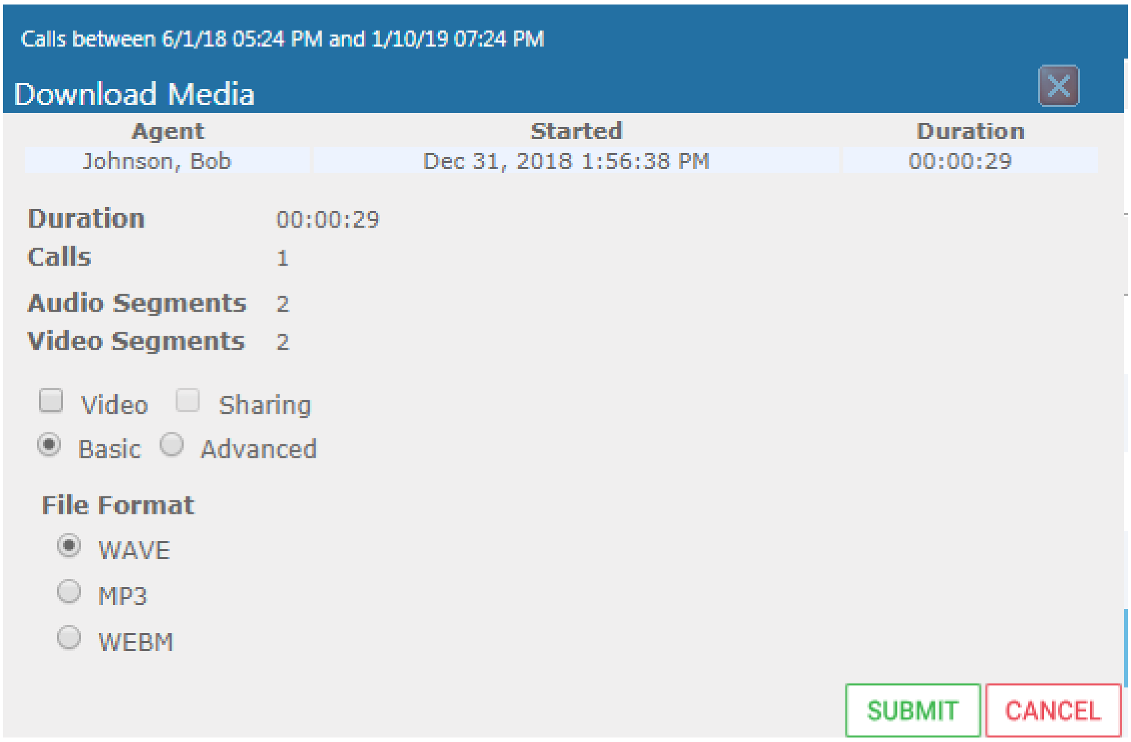
Downloading an Audio Call

This section describes how to download an audio call.

➢ To download an audio call:

1. Follow the instructions in Searching for Calls on page 135 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.
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 6-130: Basic Audio Download



Calls between 6/1/18 05:24 PM and 1/10/19 07:24 PM

Download Media

Agent	Started	Duration
Johnson, Bob	Dec 31, 2018 1:56:38 PM	00:00:29

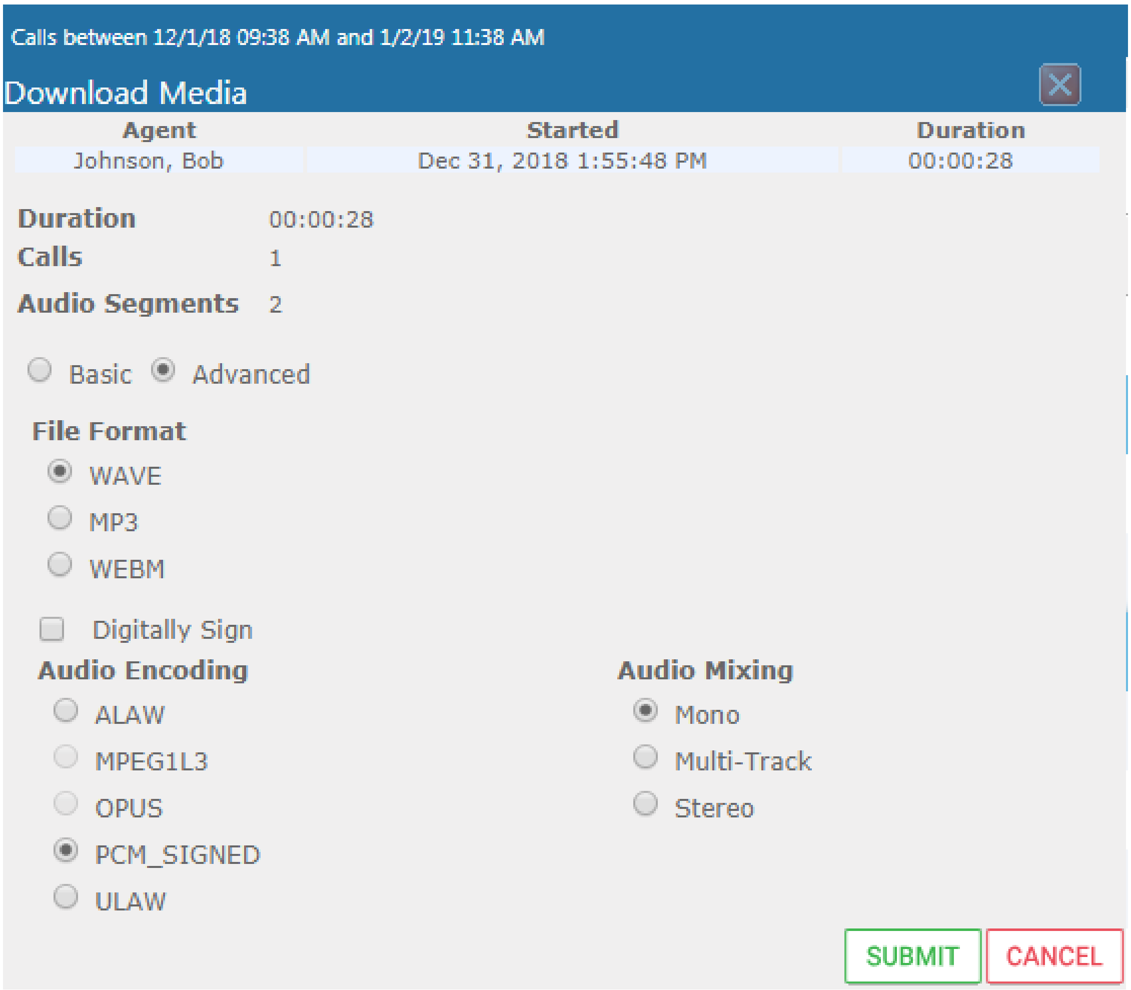
Duration 00:00:29
Calls 1
Audio Segments 2
Video Segments 2

□ Video □ Sharing
● Basic ○ Advanced

File Format

● WAVE
○ MP3
○ WEBM

Figure 6-131: Advanced Audio Download



Calls between 12/1/18 09:38 AM and 1/2/19 11:38 AM

Download Media

Agent	Started	Duration
Johnson, Bob	Dec 31, 2018 1:55:48 PM	00:00:28

Duration	00:00:28
Calls	1
Audio Segments	2

○ Basic ● Advanced

File Format

● WAVE
○ MP3
○ WEBM

□ Digitally Sign

Audio Encoding

○ ALAW
○ MPEG1L3
○ OPUS
● PCM_SIGNED
○ ULAW

Audio Mixing

● Mono
○ Multi-Track
○ Stereo

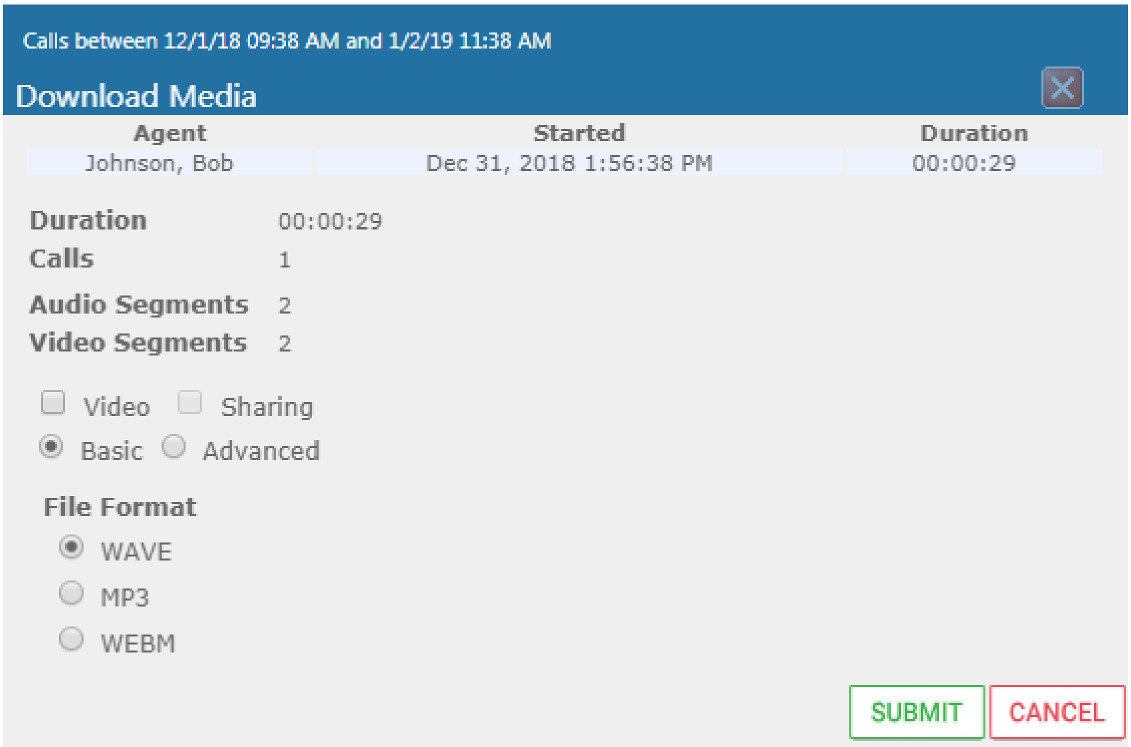
Downloading a Video Call

This section describes how to download a video call.

➢ To download a video call:

1. Follow the instructions in Searching for Calls on page 135Searching for Calls on page 135 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 6-132: Basic Video Download



Calls between 12/1/18 09:38 AM and 1/2/19 11:38 AM

Download Media

Agent	Started	Duration
Johnson, Bob	Dec 31, 2018 1:56:38 PM	00:00:29

Duration	00:00:29
Calls	1
Audio Segments	2
Video Segments	2

□ Video □ Sharing

● Basic ○ Advanced

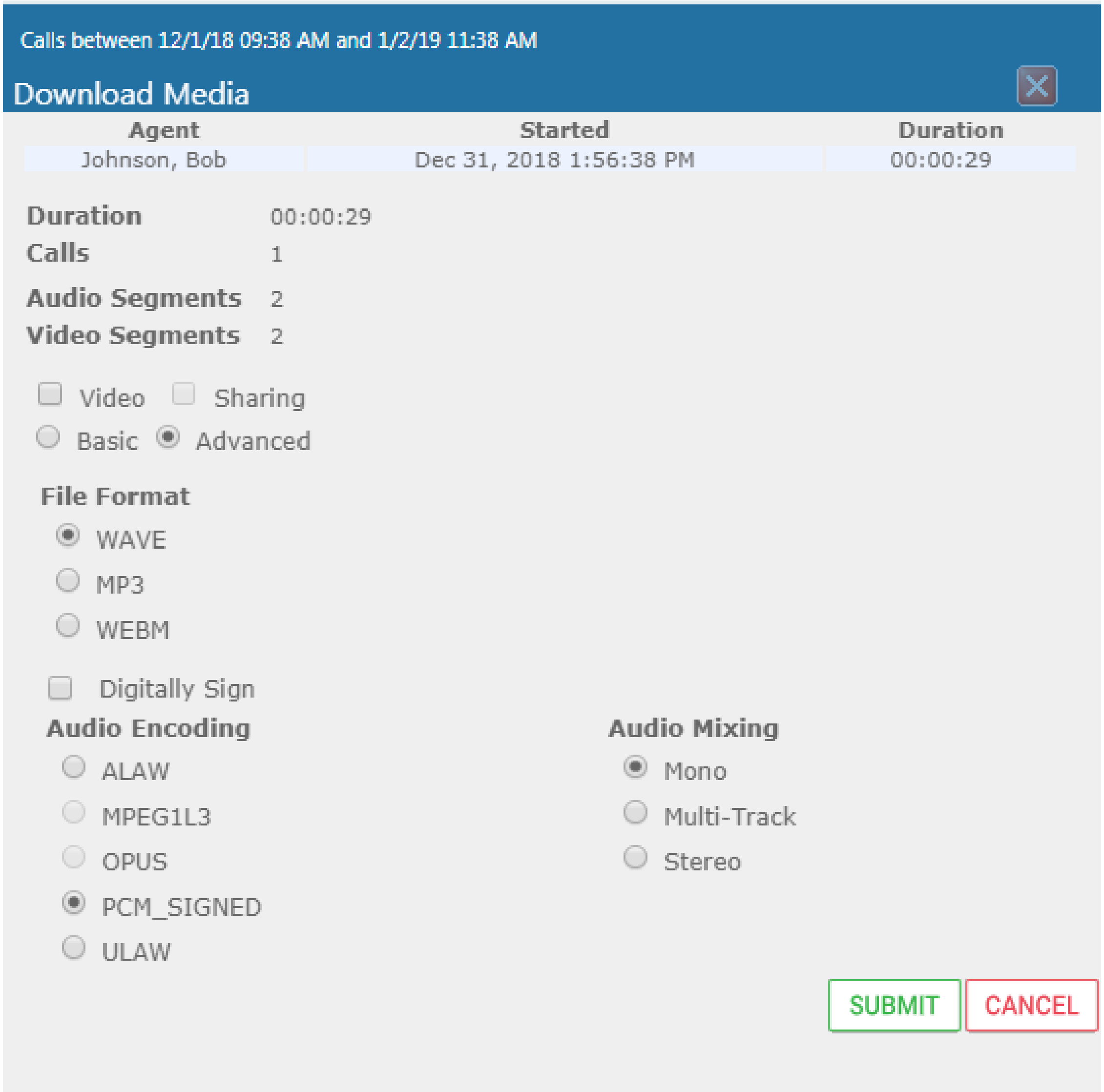
File Format

● WAVE

○ MP3

○ WEBM

Figure 6-133: Advanced Video Download



Calls between 12/1/18 09:38 AM and 1/2/19 11:38 AM

Download Media

Agent	Started	Duration
Johnson, Bob	Dec 31, 2018 1:56:38 PM	00:00:29

Duration 00:00:29
Calls 1
Audio Segments 2
Video Segments 2

□ Video □ Sharing
○ Basic ● Advanced

File Format
● WAVE
○ MP3
○ WEBM

□ Digitally Sign

Audio Encoding
○ ALAW
○ MPEG1L3
○ OPUS
● PCM_SIGNED
○ ULAW

Audio Mixing
● Mono
○ Multi-Track
○ Stereo

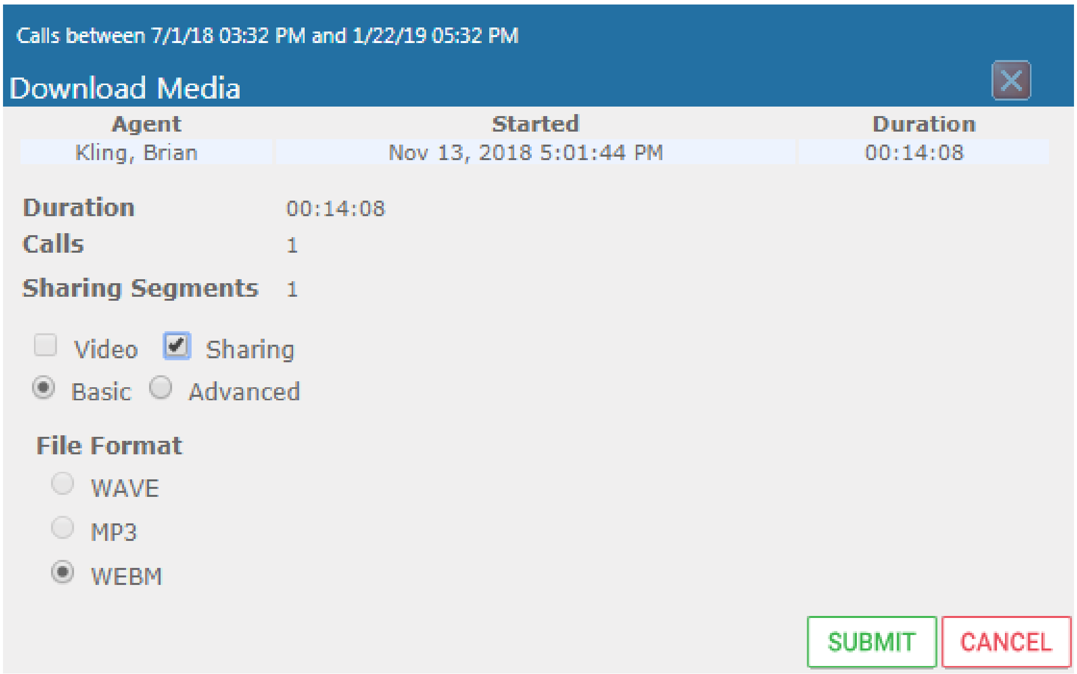
Downloading a Desktop Sharing Call

This section describes how to download a Desktop Sharing call.

➢ To download a desktop sharing call:

1. Follow the instructions in Searching for Calls on page 135 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 6-134: Downloading a Desktop Sharing Call



Calls between 7/1/18 03:32 PM and 1/22/19 05:32 PM

Download Media

Agent	Started	Duration
Kling, Brian	Nov 13, 2018 5:01:44 PM	00:14:08

Duration 00:14:08

Calls 1

Sharing Segments 1

☐ Video ☑ Sharing

● Basic ○ Advanced

File Format

○ WAVE

○ MP3

● WEBM

5. Use the table below as a reference.

Table 6-48: 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:	Basic

<table>
<tr><th>Field</th><th colspan="2">Description</th><th>Basic / Advanced</th></tr>
<tr><td></td><td colspan="2">✔ Wave
✔ MP3
■ 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 Configuring a Digital Signature on page 62 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="4">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>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>
</table>

Field	Description	Basic / Advanced
SUBMIT	Apply the changes.	
CANCEL	Cancel the changes.	

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

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.

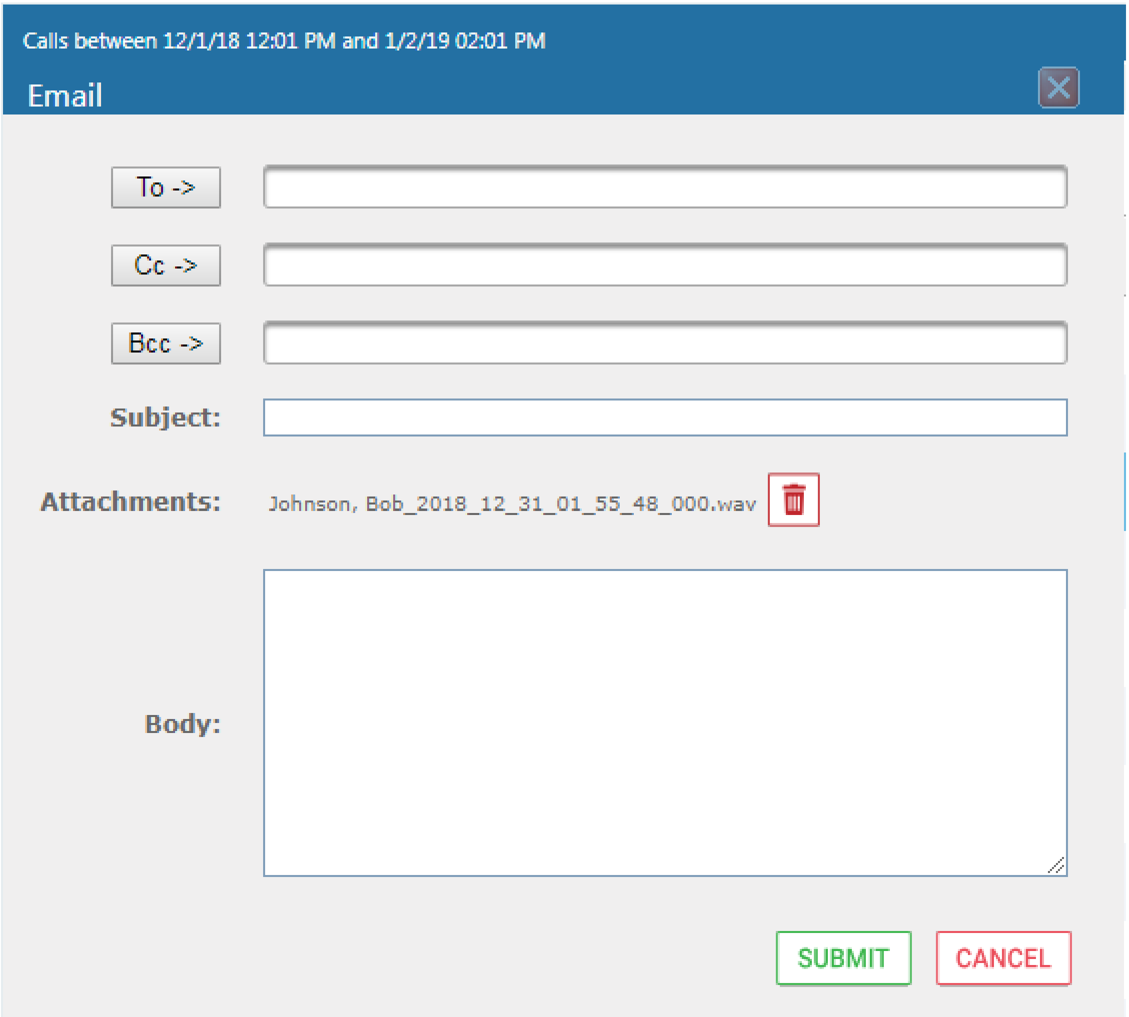
⚠ Video components cannot be sent by email.

➢ **To email a call:**

1. Follow the instructions in 'Searching for Calls' (see Searching for Calls on page 135 to find the call to email.

2. Select the call entry to email and then click the email button ✉; the Email screen opens.

Figure 6-135: Email Screen



Calls between 12/1/18 12:01 PM and 1/2/19 02:01 PM

Email

Attachments: Johnson, Bob_2018_12_31_01_55_48_000.wav

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 6-49: 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.

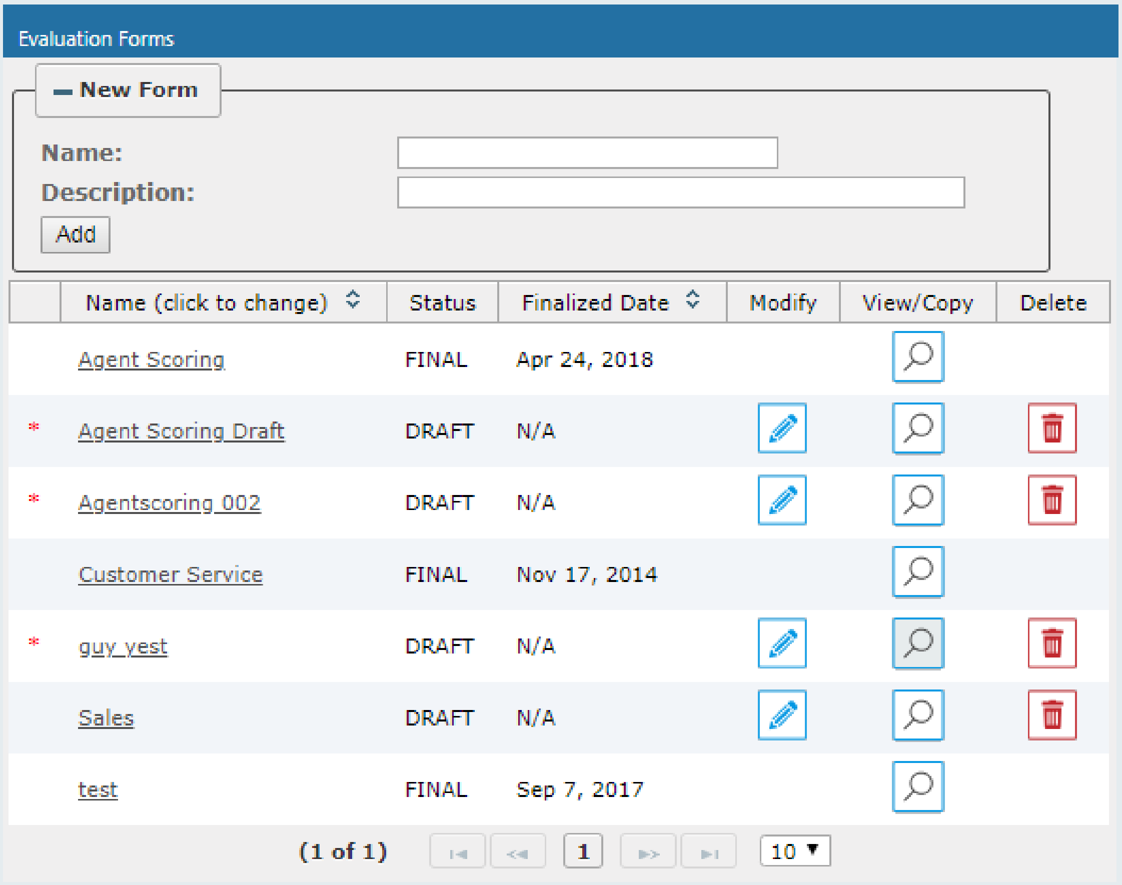
Field	Description
Attachments	List of attachments included with this email message. Clicking the X next to the attachment removes the attachment from the email.
Body	Body of the email.
SUBMIT	Sends the email.
CANCEL	Cancels the email.

6. Click SUBMIT to send the email.

Using the Evaluation Feature

The Evaluation tab accesses all functions related to the SmartTAP 360° 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 6-136: Evaluation Forms – New Form Subscreen



Evaluation Forms

— New Form

Name:

Description:

Add

	Name (click to change)	Status	Finalized Date	Modify	View/Copy	Delete
	Agent Scoring	FINAL	Apr 24, 2018		⌕	
*	Agent Scoring Draft	DRAFT	N/A	✎	⌕	🗑
*	Agentscoring 002	DRAFT	N/A	✎	⌕	🗑
	Customer Service	FINAL	Nov 17, 2014		⌕	
*	guy yest	DRAFT	N/A	✎	⌕	🗑
	Sales	DRAFT	N/A	✎	⌕	🗑
	test	FINAL	Sep 7, 2017		⌕	

Use the table below as reference.

Table 6-50: 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.

This section includes the following procedures:

- Adding a New Evaluation Form below
- Viewing and Copying an Evaluation Form on page 171
- Adding a New Section [Evaluation Forms] on page 172
- Adding Questions and Answers to an Evaluation Form on page 173
- Finalizing Forms on page 176

Adding a New Evaluation Form

This section describes how to add a new evaluation form.

➢ To add a new evaluation form:

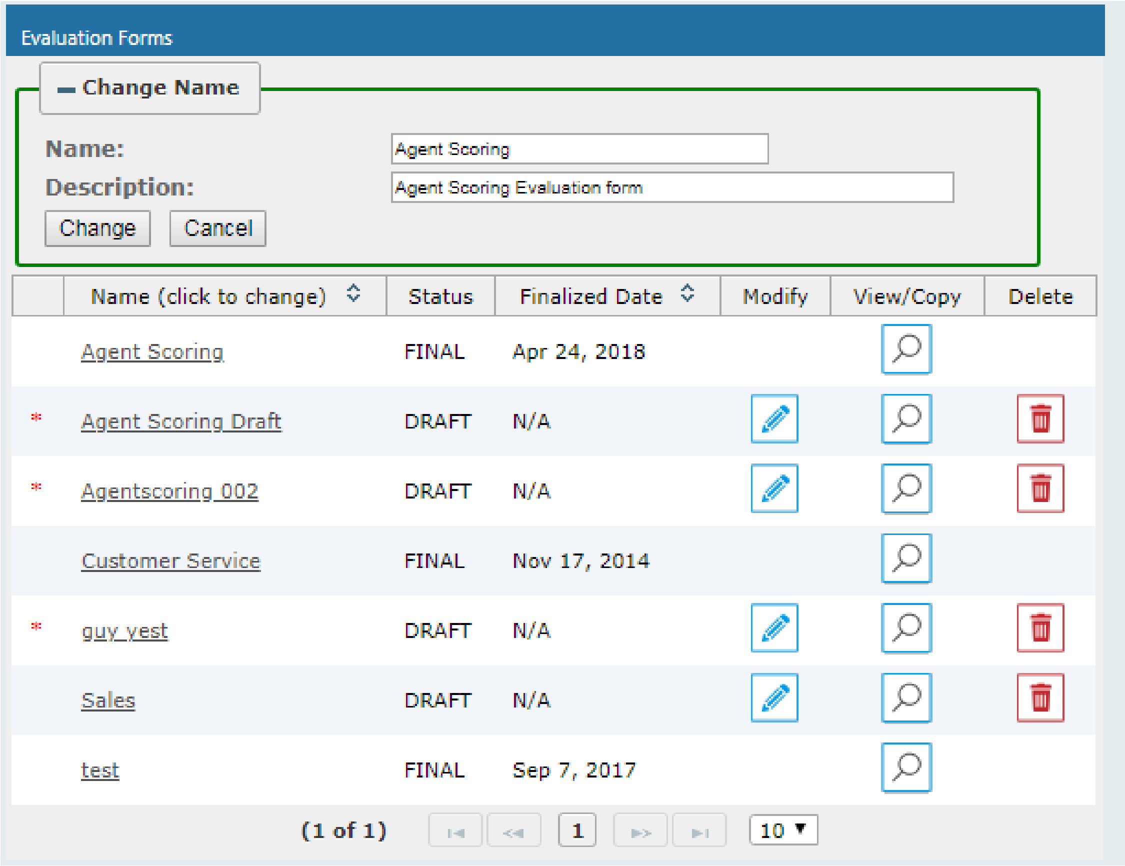
1. Open the Evaluation Forms screen (**Evaluation** tab > **Evaluation** Folder > **Evaluation Forms**).
2. In the New Form subscreen, enter the Name of the new form and a Description.
3. Click Add to create the form
4. The new form is added to the display with an (asterisk) * on the rightmost column.
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 6-137: Evaluation Forms



Evaluation Forms

— Change Name

Name: Agent Scoring

Description: Agent Scoring Evaluation form

Change Cancel

	Name (click to change)	Status	Finalized Date	Modify	View/Copy	Delete
	Agent Scoring	FINAL	Apr 24, 2018		🔍	
*	Agent Scoring Draft	DRAFT	N/A	✎	🔍	🗑
*	Agentscoring 002	DRAFT	N/A	✎	🔍	🗑
	Customer Service	FINAL	Nov 17, 2014		🔍	
*	guy yest	DRAFT	N/A	✎	🔍	🗑
	Sales	DRAFT	N/A	✎	🔍	🗑
	test	FINAL	Sep 7, 2017		🔍	

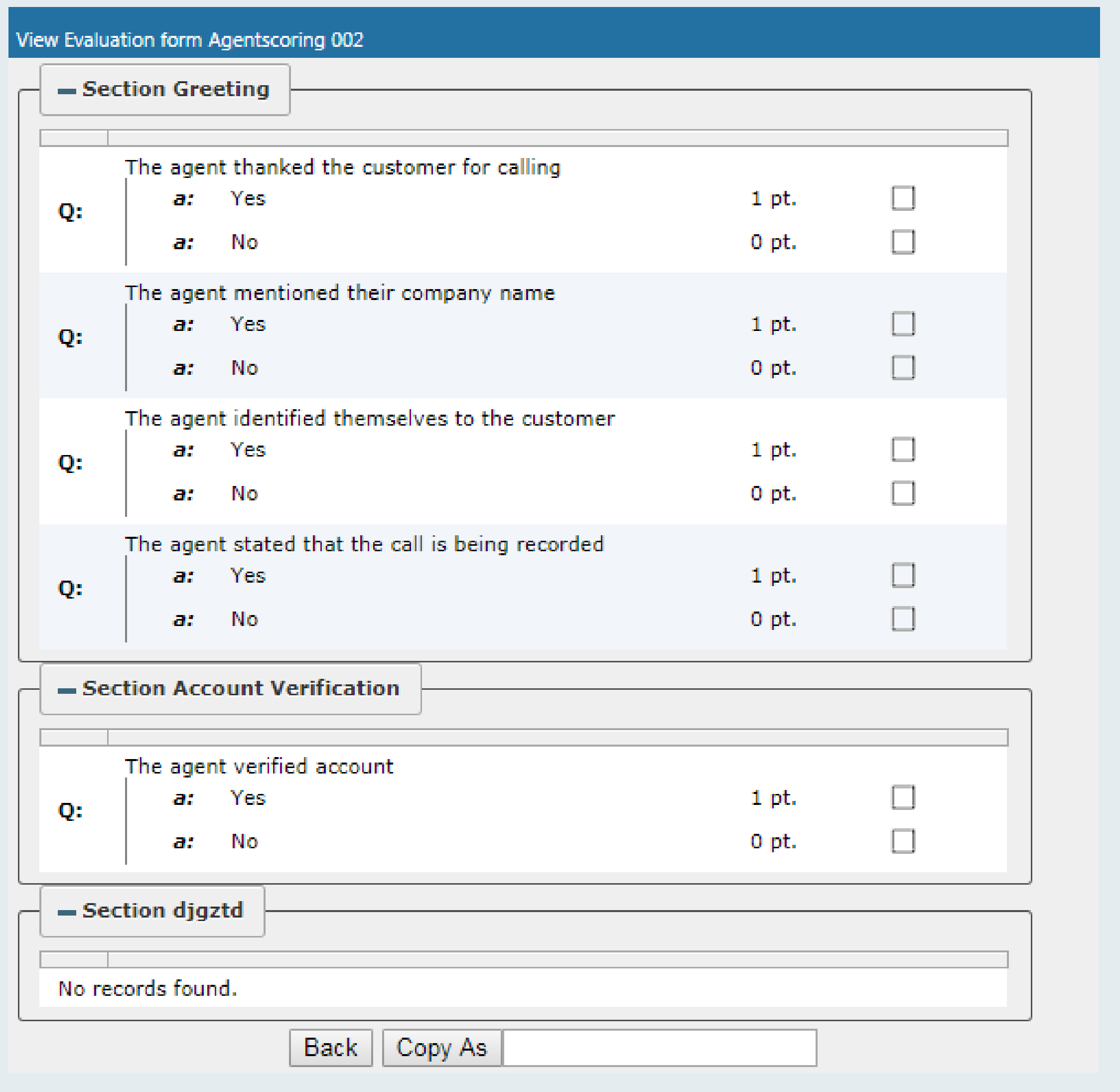
(1 of 1) 1 10

Table 6-51: 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)

Field	Description
*	The form is not completed and cannot be finalized.
✎	Click to modify the form.
🔍	Click to view or copy the form.
🗑	Click to delete the form.

Figure 6-138: View/Copy Evaluation



View Evaluation form Agentscoring 002

— Section Greeting

Q:	The agent thanked the customer for calling			
	a:	Yes	1 pt.	□
	a:	No	0 pt.	□
Q:	The agent mentioned their company name			
	a:	Yes	1 pt.	□
	a:	No	0 pt.	□
Q:	The agent identified themselves to the customer			
	a:	Yes	1 pt.	□
	a:	No	0 pt.	□
Q:	The agent stated that the call is being recorded			
	a:	Yes	1 pt.	□
	a:	No	0 pt.	□

— Section Account Verification

Q:	The agent verified account			
	a:	Yes	1 pt.	□
	a:	No	0 pt.	□

— Section djgztd

No records found.

Viewing and Copying an Evaluation Form

This section describes how to view and copy an evaluation form.

➢ To view/copy an evaluation 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 Copy As.
3. The View closes and the new form is added to the list of forms in the 'Evaluation Forms' screen.
4. Add a New Section.

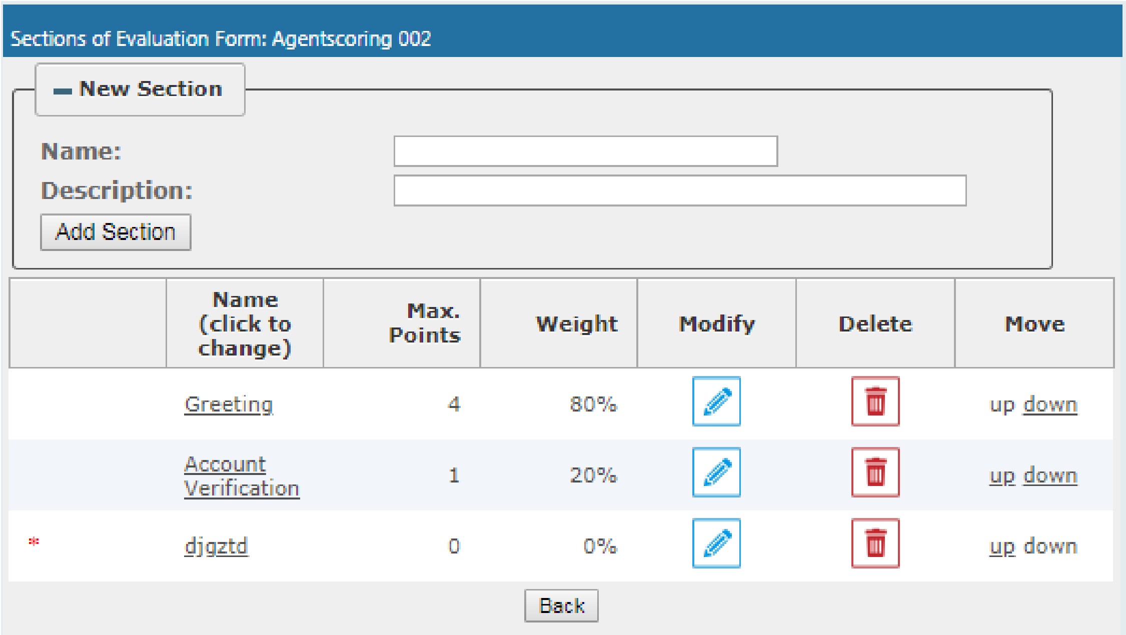
Adding a New Section [Evaluation Forms]

This section describes how to add a new section to an evaluation form.

➢ To add a new section to an evaluation form:

1. Open the form (**Evaluation** tab > **Evaluation** folder > **Evaluation Forms**).
2. Click ✎ on the row listing the form to change to open it.

Figure 6-139: Sections of Evaluation Form – New Section Subscreen



Sections of Evaluation Form: Agentscoring 002

New Section

Name:

Description:

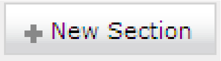
Add Section

	Name (click to change)	Max. Points	Weight	Modify	Delete	Move
	Greeting	4	80%	✎	🗑	up down
	Account Verification	1	20%	✎	🗑	up down
*	djgztd	0	0%	✎	🗑	up down

Back

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 6-52: Sections of Evaluation Form – Field Descriptions

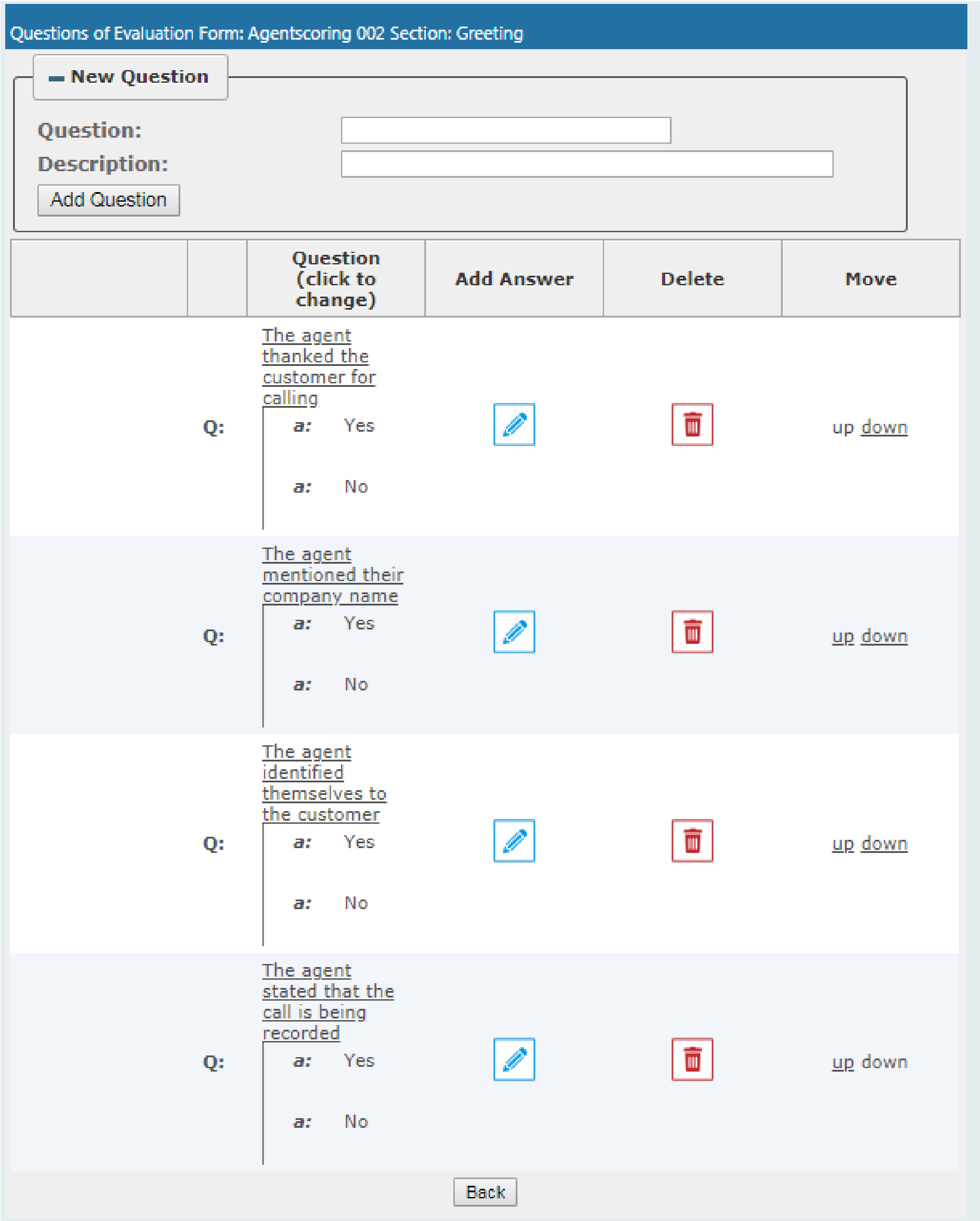
Field	Description
— New Section	Click to close the New Section subscreen.
 + New Section	Click to open the New Section subscreen.
Name (in new section subscreen)	The name of the new Section.
Description	The description of the new Section.
Add Section	Create a new section.

Adding Questions and Answers to an Evaluation Form

This section describes how to add questions to an evaluation form.

➢ To add New Questions [Evaluation Forms]:

Figure 6-140: Sections of Evaluation Form – New Questions Subscreen



Questions of Evaluation Form: Agentscoring 002 Section: Greeting

▬ New Question

Question:

Description:

Add Question

		Question (click to change)	Add Answer	Delete	Move
	Q:	The agent thanked the customer for calling a: Yes a: No	✎	🗑	up down
	Q:	The agent mentioned their company name a: Yes a: No	✎	🗑	up down
	Q:	The agent identified themselves to the customer a: Yes a: No	✎	🗑	up down
	Q:	The agent stated that the call is being recorded a: Yes a: No	✎	🗑	up down

Back

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

Field	Description
▬ New Question	Click to close the New Question subscreen.

Field	Description
+ 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 ✎ on the row listing the Form to change, to open it.
3. Click ✎ 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 6-54: 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.

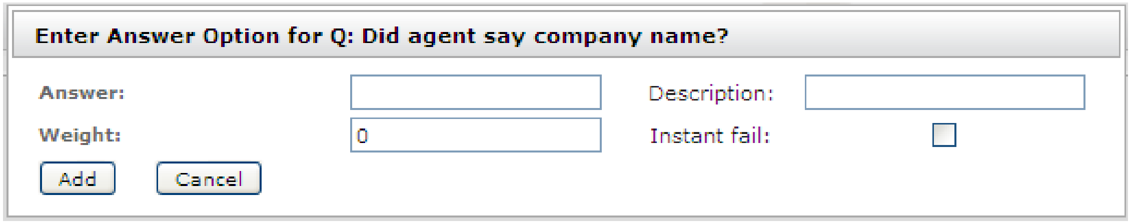
➢ To add a new answer:

1. Open the form (**Evaluation** tab > **Evaluation** folder > **Evaluation Forms** > **Form**).
2. Click ✎ on the row listing the Form to change, to open it.

3. Click ✎ on the row listing the Section to change, to open it.

4. Click ✎ on the row listing the Question to launch the Answer screen.

Figure 6-141: Sections of Evaluation Form - New Answer Subscreen



Enter Answer Option for Q: Did agent say company name?

Answer:		Description:	
Weight:	0	Instant fail:	□

5. Enter the new Answer information.

> ⚠ You must provide at least two answers for each question.

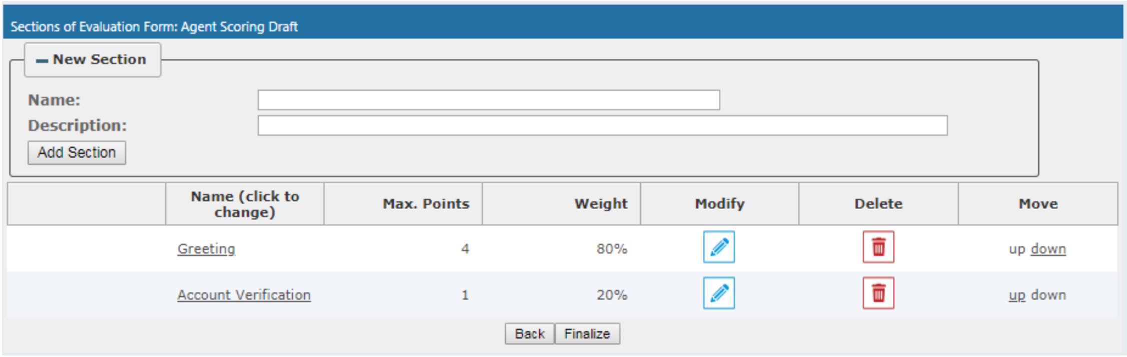
6. Click Add to create the new Answer; the new Answer will appear in the form with an asterisk * on the leftmost column indicating that the form is missing fields and cannot be finalized. There is a minimum of two (2) answers required before a form can be finalized.

Finalizing Forms

This section describes how to finalize forms.

➢ To finalize a Form [Evaluation Forms]:

Figure 6-142: Form Subscreen



Sections of Evaluation Form: Agent Scoring Draft

Name:	
Description:	

	Name (click to change)	Max. Points	Weight	Modify	Delete	Move
	Greeting	4	80%	✎	🗑	up down
	Account Verification	1	20%	✎	🗑	up down

➢ 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 ✎ is no longer available to change the form.

Performing an Evaluation

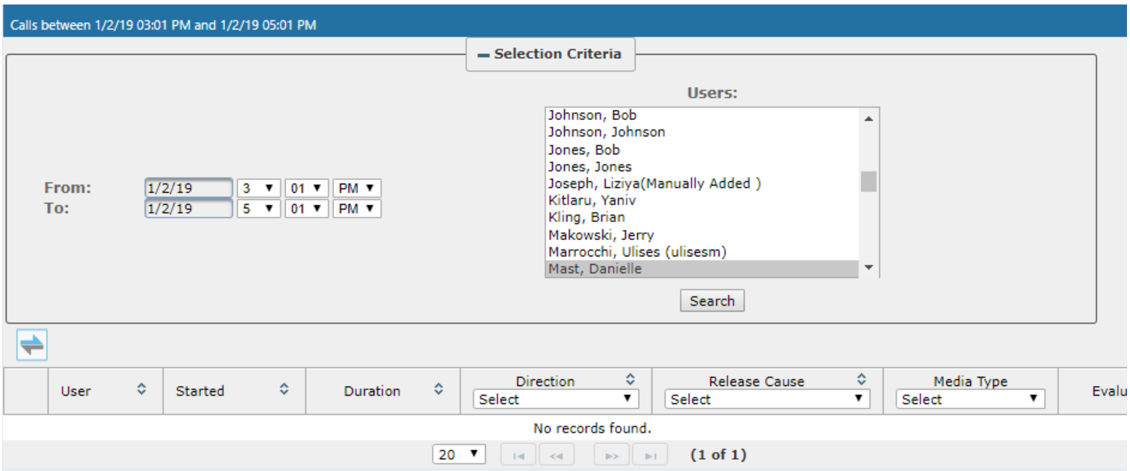
An administrator with privileges to perform an evaluation selects a finalized evaluation form, selects the call to evaluate, and from the Perform Evaluation screen, selects the appropriate answers to the questions in the evaluation form.

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

Table 6-55: 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 6-143: Call Search/Selection Evaluation Form



Calls between 1/2/19 03:01 PM and 1/2/19 05:01 PM

Selection Criteria

From: 1/2/19 3 01 PM
To: 1/2/19 5 01 PM

Users:
Johnson, Bob
Johnson, Johnson
Jones, Bob
Jones, Jones
Joseph, Liziya(Manually Added)
Kitlaru, Yaniv
Kling, Brian
Makowski, Jerry
Marrocchi, Ulises (ulisesm)
Mast, Danielle

Search

User	Started	Duration	Direction Select	Release Cause Select	Media Type Select	Evalu

No records found.

20 (1 of 1)

Table 6-56: 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

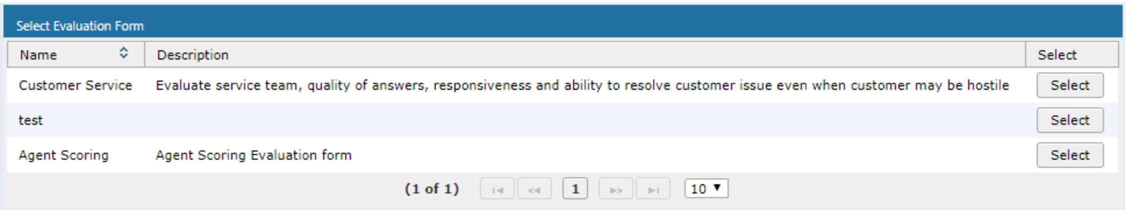
Field	Description
	up showing one month at a time. Use the dropdown to change the time of day.
Users	Users whose account is enabled in SmartTAP 360°.
Search	Click to search and display results in the Evaluation screen.
⇄	Launch the Add and Remove Columns dialog.
User/Device	User/Device name. Clicking 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 - 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.

Field	Description
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).

Figure 6-144: Select Evaluation Form

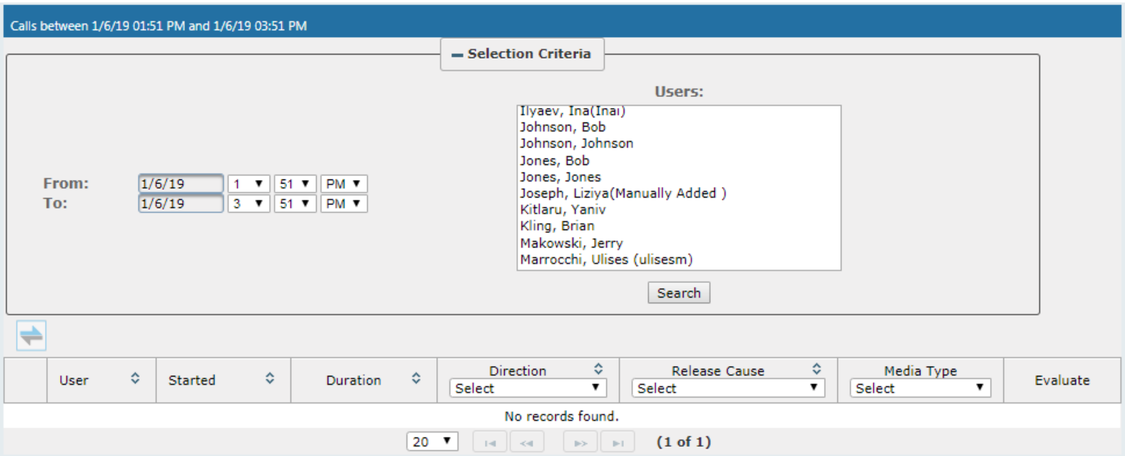


Select Evaluation Form

Name	Description	Select
Customer Service	Evaluate service team, quality of answers, responsiveness and ability to resolve customer issue even when customer may be hostile	Select
test		Select
Agent Scoring	Agent Scoring Evaluation form	Select

(1 of 1) 1 10

Figure 6-145: Evaluation Form User Selection



Calls between 1/6/19 01:51 PM and 1/6/19 03:51 PM

Selection Criteria

From: 1/6/19 1 51 PM
To: 1/6/19 3 51 PM

Users:
Ilyaev, Ina(Inai)
Johnson, Bob
Johnson, Johnson
Jones, Bob
Jones, Jones
Joseph, Liziya(Manually Added)
Kitlaru, Yaniv
Kling, Brian
Makowski, Jerry
Marrocchi, Ulises (ulisesm)

Search

User	Started	Duration	Direction Select	Release Cause Select	Media Type Select	Evaluate

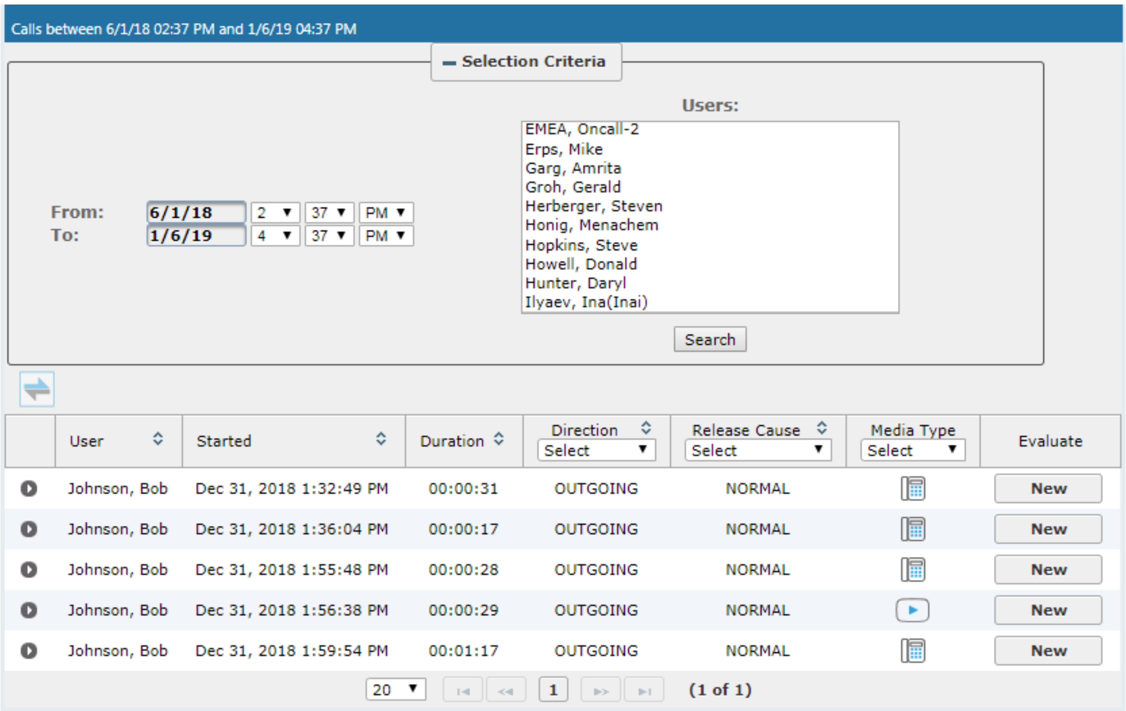
No records found.

20 (1 of 1)

2. Select the user to evaluate, select a search date range and then click Search. A list of call records for the selected user is displayed.

3. 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 6-146: Select Call to Evaluate



Calls between 6/1/18 02:37 PM and 1/6/19 04:37 PM

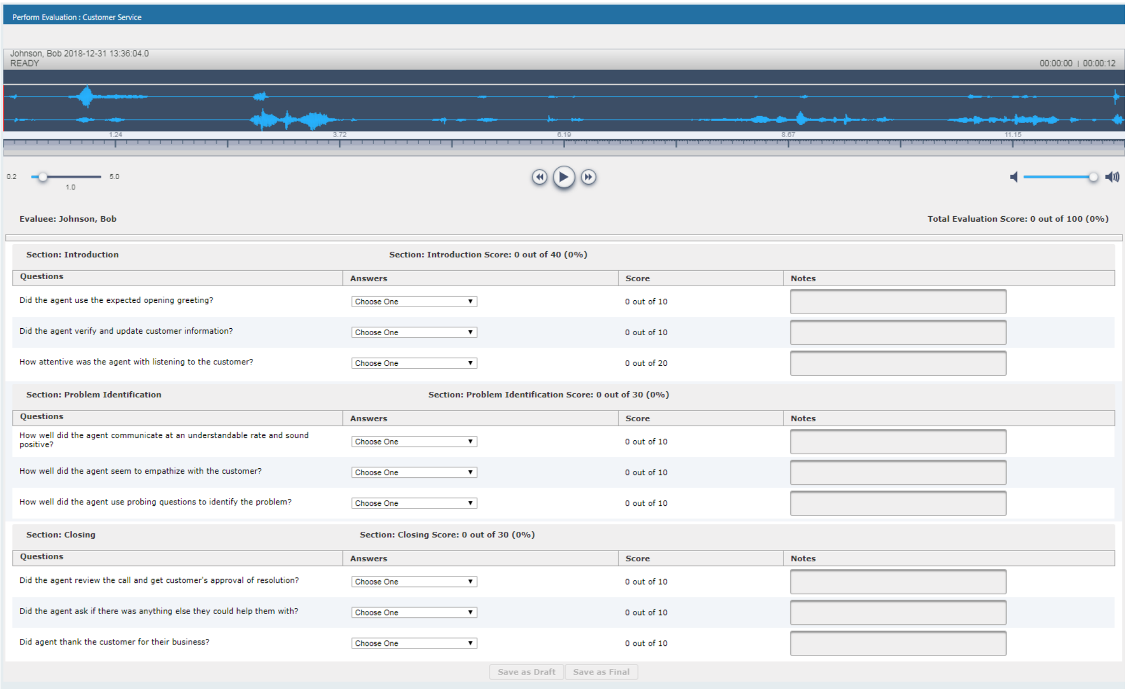
From: 6/1/18 2 37 PM
To: 1/6/19 4 37 PM

Users:
EMEA, Oncall-2
Erps, Mike
Garg, Amrita
Groh, Gerald
Herberger, Steven
Honig, Menachem
Hopkins, Steve
Howell, Donald
Hunter, Daryl
Ilyaev, Ina(Inai)

	User	Started	Duration	Direction Select	Release Cause Select	Media Type Select	Evaluate
▶	Johnson, Bob	Dec 31, 2018 1:32:49 PM	00:00:31	OUTGOING	NORMAL	☎	New
▶	Johnson, Bob	Dec 31, 2018 1:36:04 PM	00:00:17	OUTGOING	NORMAL	☎	New
▶	Johnson, Bob	Dec 31, 2018 1:55:48 PM	00:00:28	OUTGOING	NORMAL	☎	New
▶	Johnson, Bob	Dec 31, 2018 1:56:38 PM	00:00:29	OUTGOING	NORMAL	▶	New
▶	Johnson, Bob	Dec 31, 2018 1:59:54 PM	00:01:17	OUTGOING	NORMAL	☎	New

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

Figure 6-147: Perform Evaluation Screen



Perform Evaluation : Customer Service

Johnson, Bob 2018-12-31 13:36:04.0
READY

Evaluee: Johnson, Bob

Total Evaluation Score: 0 out of 100 (0%)

Section: Introduction — Section: Introduction Score: 0 out of 40 (0%)

Questions	Answers	Score	Notes
Did the agent use the expected opening greeting?	Choose One ▼	0 out of 10	
Did the agent verify and update customer information?	Choose One ▼	0 out of 10	
How attentive was the agent with listening to the customer?	Choose One ▼	0 out of 20	

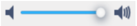
Section: Problem Identification — Section: Problem Identification Score: 0 out of 30 (0%)

Questions	Answers	Score	Notes
How well did the agent communicate at an understandable rate and sound positive?	Choose One ▼	0 out of 10	
How well did the agent seem to empathize with the customer?	Choose One ▼	0 out of 10	
How well did the agent use probing questions to identify the problem?	Choose One ▼	0 out of 10	

Section: Closing — Section: Closing Score: 0 out of 30 (0%)

Questions	Answers	Score	Notes
Did the agent review the call and get customer's approval of resolution?	Choose One ▼	0 out of 10	
Did the agent ask if there was anything else they could help them with?	Choose One ▼	0 out of 10	
Did agent thank the customer for their business?	Choose One ▼	0 out of 10	

Table 6-57: Perform Evaluation Screen

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

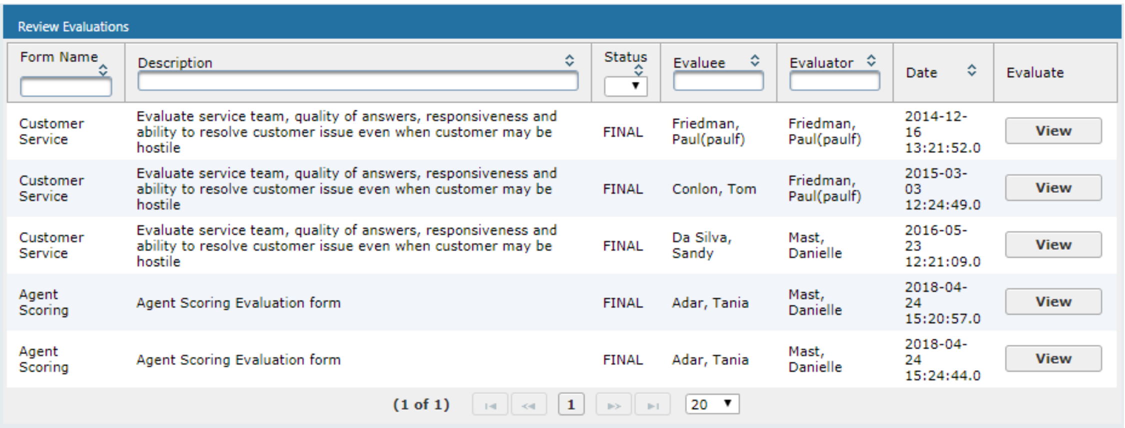
Field	Description
Save as Final	Save Evaluation as Final. The Save as Final button will only be available after all answers are scored.

➢ 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 6-148: Review Evaluations



Review Evaluations

Form Name	Description	Status	Evaluee	Evaluator	Date	Evaluate
Customer Service	Evaluate service team, quality of answers, responsiveness and ability to resolve customer issue even when customer may be hostile	FINAL	Friedman, Paul(paulf)	Friedman, Paul(paulf)	2014-12-16 13:21:52.0	View
Customer Service	Evaluate service team, quality of answers, responsiveness and ability to resolve customer issue even when customer may be hostile	FINAL	Conlon, Tom	Friedman, Paul(paulf)	2015-03-03 12:24:49.0	View
Customer Service	Evaluate service team, quality of answers, responsiveness and ability to resolve customer issue even when customer may be hostile	FINAL	Da Silva, Sandy	Mast, Danielle	2016-05-23 12:21:09.0	View
Agent Scoring	Agent Scoring Evaluation form	FINAL	Adar, Tania	Mast, Danielle	2018-04-24 15:20:57.0	View
Agent Scoring	Agent Scoring Evaluation form	FINAL	Adar, Tania	Mast, Danielle	2018-04-24 15:24:44.0	View

Table 6-58: 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.

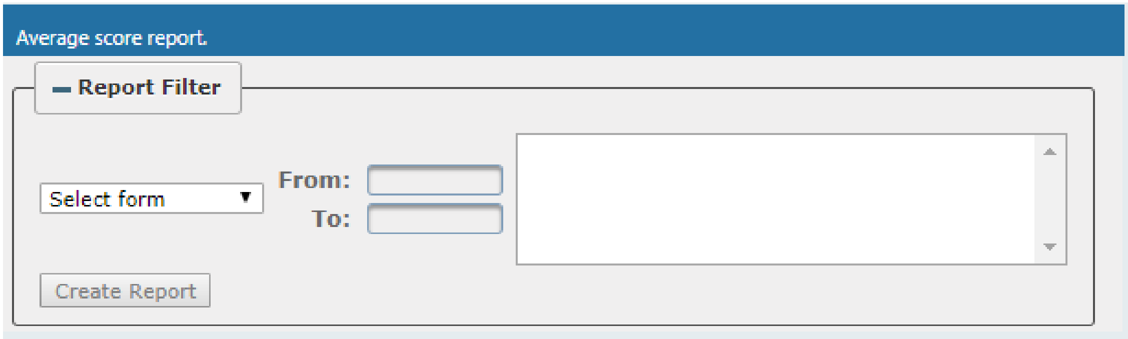
Field	Description
Description	Release cause for the call. Clicking this header sorts the search results in Ascending/Descending order alternating with each click. The dropdown entry shows only the matching results.
Status	Status of the Evaluation. Clicking this header sorts the search results in Ascending/Descending 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:

1. Open the Average score report screen (**Evaluation** tab > **Evaluation** folder > **Report**).

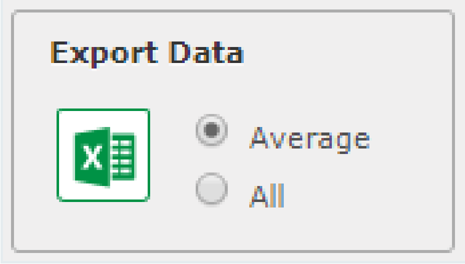


2. Select the evaluation by entering the search data into the report filter area.

3. Click Create Report to create the report; the report is displayed on the screen.

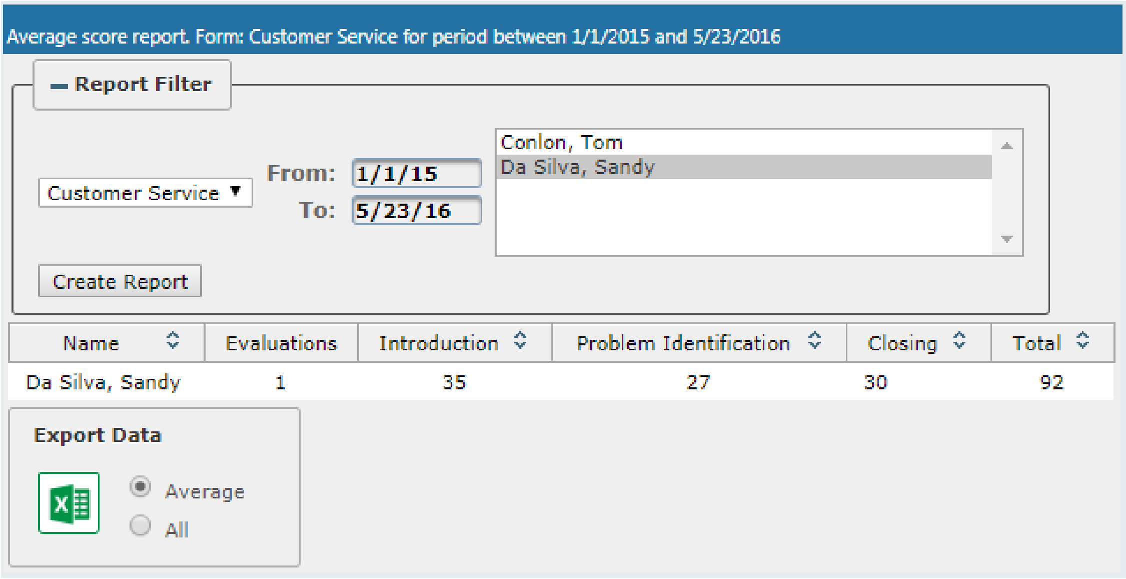
➢ To export a report (to Excel):

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.

Figure 6-149: Average Score Report


Average score report. Form: Customer Service for period between 1/1/2015 and 5/23/2016

▬ Report Filter

Customer Service ▼ From: 1/1/15 To: 5/23/16

Conlon, Tom
Da Silva, Sandy

Create Report

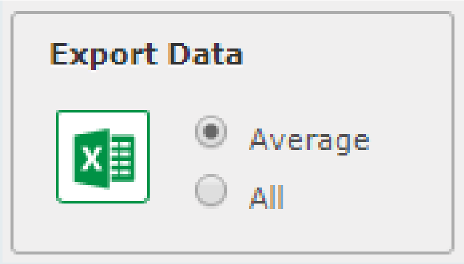
Name	Evaluations	Introduction	Problem Identification	Closing	Total
Da Silva, Sandy	1	35	27	30	92

Export Data

● Average
○ All

Table 6-59: Average Score Report – Field Descriptions

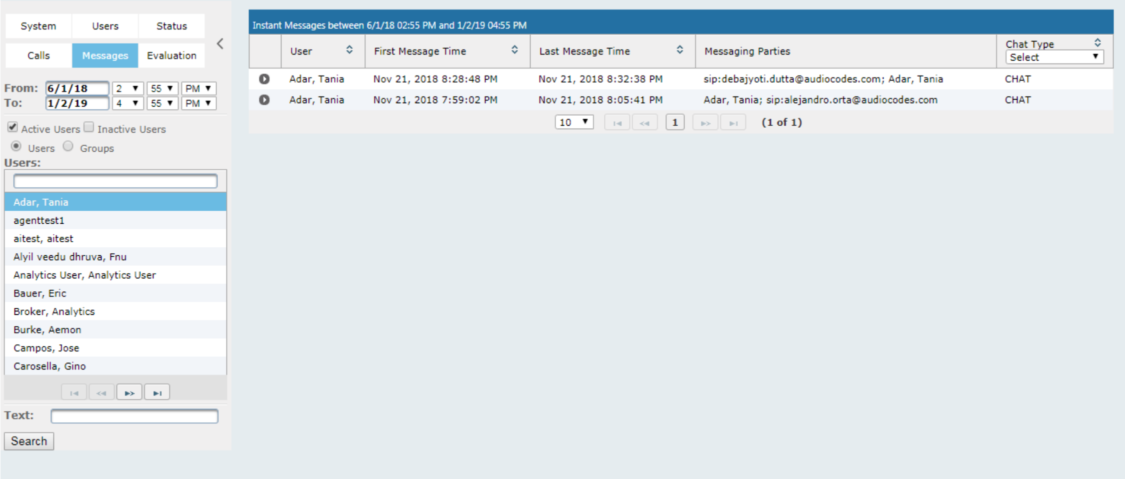
Field	Description
▬ Report Filter	Click to hide the report filter.

Field	Description
+ 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 360°; can be changed by the user.
To:	Search before this call date(s). Automatically populated by SmartTAP 360°; can be changed by the user.
List of users	List of evaluees. Automatically populated by SmartTAP 360°; 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.

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 6-150: Managing Messages



From: 6/1/18 2 55 PM
To: 1/2/19 4 55 PM

☑ Active Users □ Inactive Users

● Users ○ Groups

Users:

- Adar, Tania
- agenttest1
- aitest, aitest
- Alyil veedu dhruva, Fnu
- Analytics User, Analytics User
- Bauer, Eric
- Broker, Analytics
- Burke, Aemon
- Campos, Jose
- Carosella, Gino

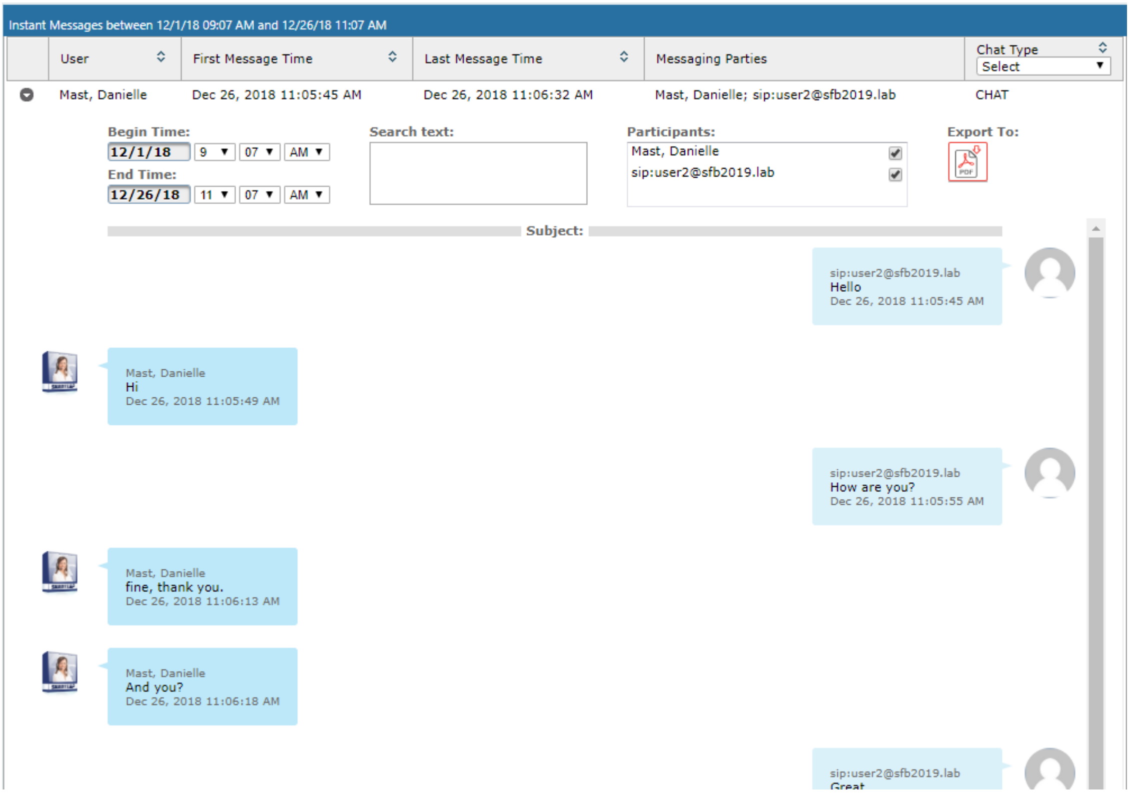
Text:

Instant Messages between 6/1/18 02:55 PM and 1/2/19 04:55 PM

	User	First Message Time	Last Message Time	Messaging Parties	Chat Type Select
●	Adar, Tania	Nov 21, 2018 8:28:48 PM	Nov 21, 2018 8:32:38 PM	sip:debajyoti.dutta@audiocodes.com; Adar, Tania	CHAT
●	Adar, Tania	Nov 21, 2018 7:59:02 PM	Nov 21, 2018 8:05:41 PM	Adar, Tania; sip:alejandro.orta@audiocodes.com	CHAT

10 1 (1 of 1)

Figure 6-151: Instant Message Display



Instant Messages between 12/1/18 09:07 AM and 12/26/18 11:07 AM

	User	First Message Time	Last Message Time	Messaging Parties	Chat Type Select
●	Mast, Danielle	Dec 26, 2018 11:05:45 AM	Dec 26, 2018 11:06:32 AM	Mast, Danielle; sip:user2@sfb2019.lab	CHAT

Begin Time: 12/1/18 9 07 AM
End Time: 12/26/18 11 07 AM

Search text:

Participants:
Mast, Danielle ☑
sip:user2@sfb2019.lab ☑

Subject:

sip:user2@sfb2019.lab
Hello
Dec 26, 2018 11:05:45 AM

Mast, Danielle
Hi
Dec 26, 2018 11:05:49 AM

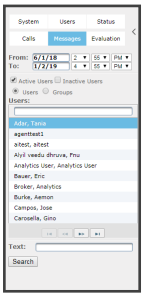
sip:user2@sfb2019.lab
How are you?
Dec 26, 2018 11:05:55 AM

Mast, Danielle
fine, thank you.
Dec 26, 2018 11:06:13 AM

Mast, Danielle
And you?
Dec 26, 2018 11:06:18 AM

sip:user2@sfb2019.lab
Great

Table 6-60: Search Messages Navigation Screen - Messages Tab

Search Messages Navigation	Field	Description
 System Users Status Calls Messages Evaluation From: 6/1/18 2 55 PM To: 1/2/19 4 55 PM ☑ Active Users ☐ Inactive Users ● Users ○ Groups Users: Adar, Tania agenttest1 aitest, aitest Alyil veedu dhruva, Fnu Analytics User, Analytics User Bauer, Eric Broker, Analytics Burke, Aemon Campos, Jose Carosella, Gino Text: Search	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 360° application.
	Inactive Users	Users whose account has been deleted from the SmartTAP 360° 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.

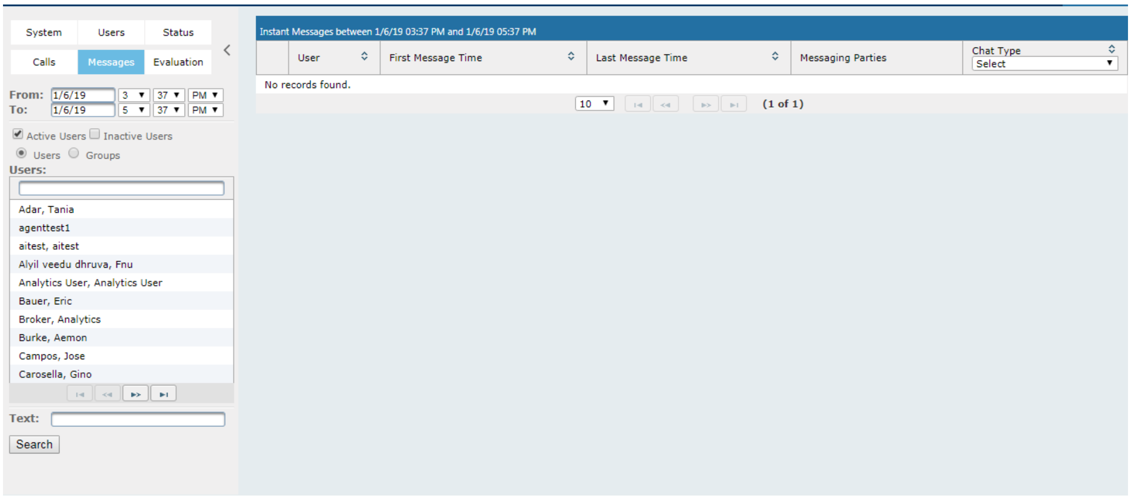
Searching for Messages

This section shows how to search for messages.

➢ To search for messages:

1. Click the **Messages** tab to open the Search Messages screen.

Figure 6-152: Instant Message Search



From: 1/6/19 3 ▾ 37 ▾ PM ▾
To: 1/6/19 5 ▾ 37 ▾ PM ▾

☑ Active Users ☐ Inactive Users

● Users ○ Groups

Users:

Adar, Tania
agenttest1
aitest, aitest
Alyil veedu dhruva, Fnu
Analytics User, Analytics User
Bauer, Eric
Broker, Analytics
Burke, Aemon
Campos, Jose
Carosella, Gino

Text:

Instant Messages between 1/6/19 03:37 PM and 1/6/19 05:37 PM

	User	First Message Time	Last Message Time	Messaging Parties	Chat Type Select ▾
No records found.					

10 ▾ (1 of 1)

2. In the Search Navigation screen (left side of the screen), enter the time range, and then select the type of Users.

> 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 360°'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 "File Transfer Messages" in Searching for Messages on the previous page).

Table 6-61: 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.
> <	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	'+apple ~macintosh' Find messages that contain the word 'apple', but if the message also contains the

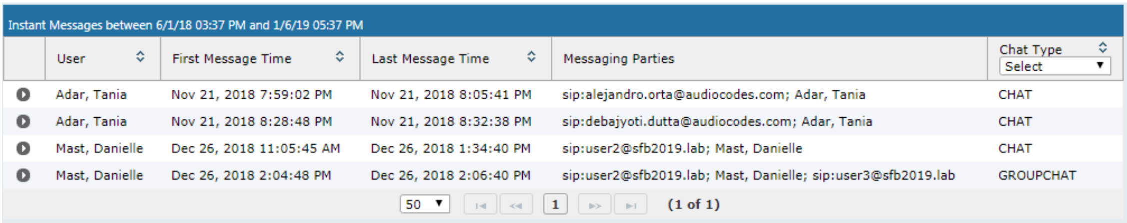
Operator	Description	Example
	negative. A message containing such a word is rated lower than others, but is not excluded altogether, as it would be with the - operator.	word 'macintosh', rate it lower than if message does not.
*	The asterisk serves as the truncation (or wildcard) operator. Unlike the 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".

Some words (also known as stopwords) are ignored in full-text searches. In SmartTAP 360°, 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.

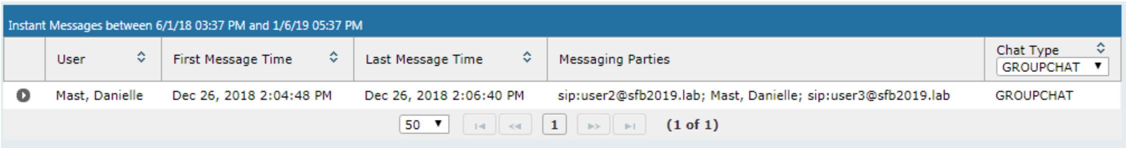
Figure 6-153: Search Messages Results-Person-to-Person Chat



Instant Messages between 6/1/18 03:37 PM and 1/6/19 05:37 PM

	User	First Message Time	Last Message Time	Messaging Parties	Chat Type Select
●	Adar, Tania	Nov 21, 2018 7:59:02 PM	Nov 21, 2018 8:05:41 PM	sip:alejandro.orta@audiocodes.com; Adar, Tania	CHAT
●	Adar, Tania	Nov 21, 2018 8:28:48 PM	Nov 21, 2018 8:32:38 PM	sip:debajyoti.dutta@audiocodes.com; Adar, Tania	CHAT
●	Mast, Danielle	Dec 26, 2018 11:05:45 AM	Dec 26, 2018 1:34:40 PM	sip:user2@sfb2019.lab; Mast, Danielle	CHAT
●	Mast, Danielle	Dec 26, 2018 2:04:48 PM	Dec 26, 2018 2:06:40 PM	sip:user2@sfb2019.lab; Mast, Danielle; sip:user3@sfb2019.lab	GROUPCHAT

Figure 6-154: Search Messages Results-Group Chat



Instant Messages between 6/1/18 03:37 PM and 1/6/19 05:37 PM

	User	First Message Time	Last Message Time	Messaging Parties	Chat Type GROUPCHAT
●	Mast, Danielle	Dec 26, 2018 2:04:48 PM	Dec 26, 2018 2:06:40 PM	sip:user2@sfb2019.lab; Mast, Danielle; sip:user3@sfb2019.lab	GROUPCHAT

The search result fields are described in the table below.

Table 6-62: Search Messages Results

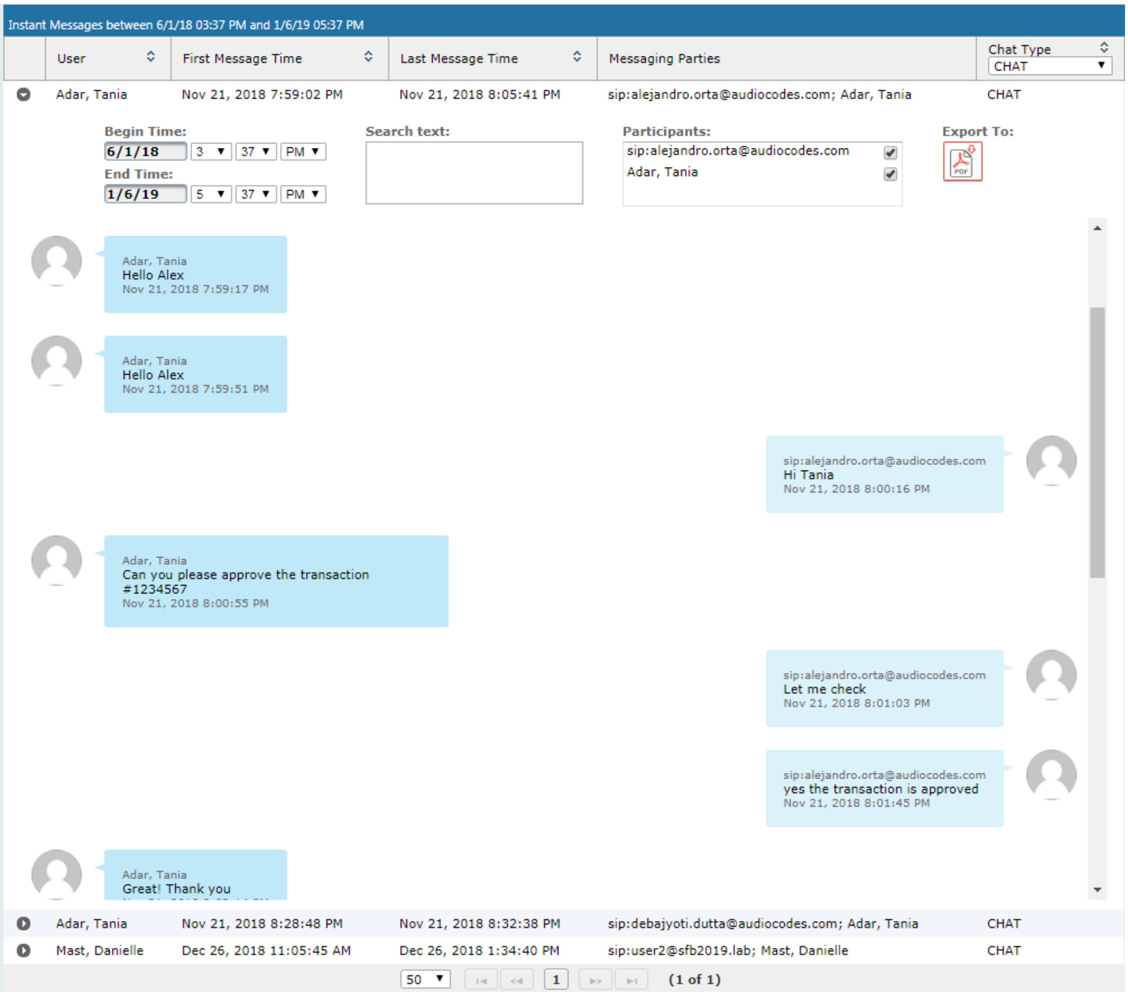
Field	Description
User	User name. Clicking this header sorts the search results in

Field	Description
	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 “File Transfer Messages” in Searching for Messages on page 188).

Figure 6-155: Search Messages Results-Person to Person Chat



Instant Messages between 6/1/18 03:37 PM and 1/6/19 05:37 PM

	User	First Message Time	Last Message Time	Messaging Parties	Chat Type CHAT
●	Adar, Tania	Nov 21, 2018 7:59:02 PM	Nov 21, 2018 8:05:41 PM	sip:alejandro.orta@audiocodes.com; Adar, Tania	CHAT

Begin Time: 6/1/18 3 37 PM

End Time: 1/6/19 5 37 PM

Search text:

Participants:
sip:alejandro.orta@audiocodes.com ☑
Adar, Tania ☑

Export To:

Adar, Tania
Hello Alex
Nov 21, 2018 7:59:17 PM

Adar, Tania
Hello Alex
Nov 21, 2018 7:59:51 PM

sip:alejandro.orta@audiocodes.com
Hi Tania
Nov 21, 2018 8:00:16 PM

Adar, Tania
Can you please approve the transaction #1234567
Nov 21, 2018 8:00:55 PM

sip:alejandro.orta@audiocodes.com
Let me check
Nov 21, 2018 8:01:03 PM

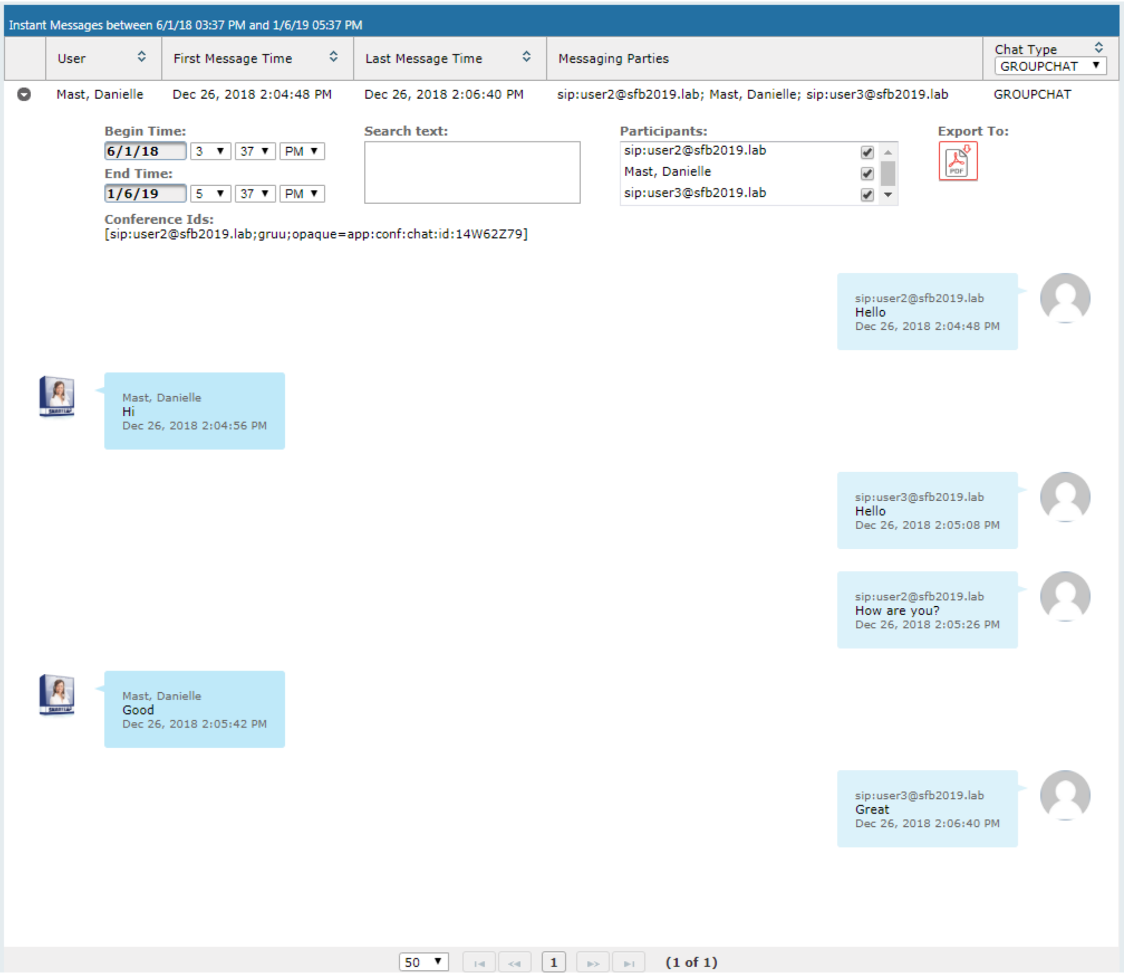
sip:alejandro.orta@audiocodes.com
yes the transaction is approved
Nov 21, 2018 8:01:45 PM

Adar, Tania
Great! Thank you

	User	First Message Time	Last Message Time	Messaging Parties	Chat Type
●	Adar, Tania	Nov 21, 2018 8:28:48 PM	Nov 21, 2018 8:32:38 PM	sip:debajyoti.dutta@audiocodes.com; Adar, Tania	CHAT
●	Mast, Danielle	Dec 26, 2018 11:05:45 AM	Dec 26, 2018 1:34:40 PM	sip:user2@sfb2019.lab; Mast, Danielle	CHAT

50 1 (1 of 1)

Figure 6-156: Group Chat Recording



Instant Messages between 6/1/18 03:37 PM and 1/6/19 05:37 PM

	User	First Message Time	Last Message Time	Messaging Parties	Chat Type GROUPCHAT
	Mast, Danielle	Dec 26, 2018 2:04:48 PM	Dec 26, 2018 2:06:40 PM	sip:user2@sfb2019.lab; Mast, Danielle; sip:user3@sfb2019.lab	GROUPCHAT

Begin Time: 6/1/18 3 37 PM

End Time: 1/6/19 5 37 PM

Search text:

Participants:
- sip:user2@sfb2019.lab ☑
- Mast, Danielle ☑
- sip:user3@sfb2019.lab ☑

Export To:

Conference Ids:
[sip:user2@sfb2019.lab;gruu;opaque=app:conf:chat:id:14W62Z79]

sip:user2@sfb2019.lab
Hello
Dec 26, 2018 2:04:48 PM

Mast, Danielle
Hi
Dec 26, 2018 2:04:56 PM

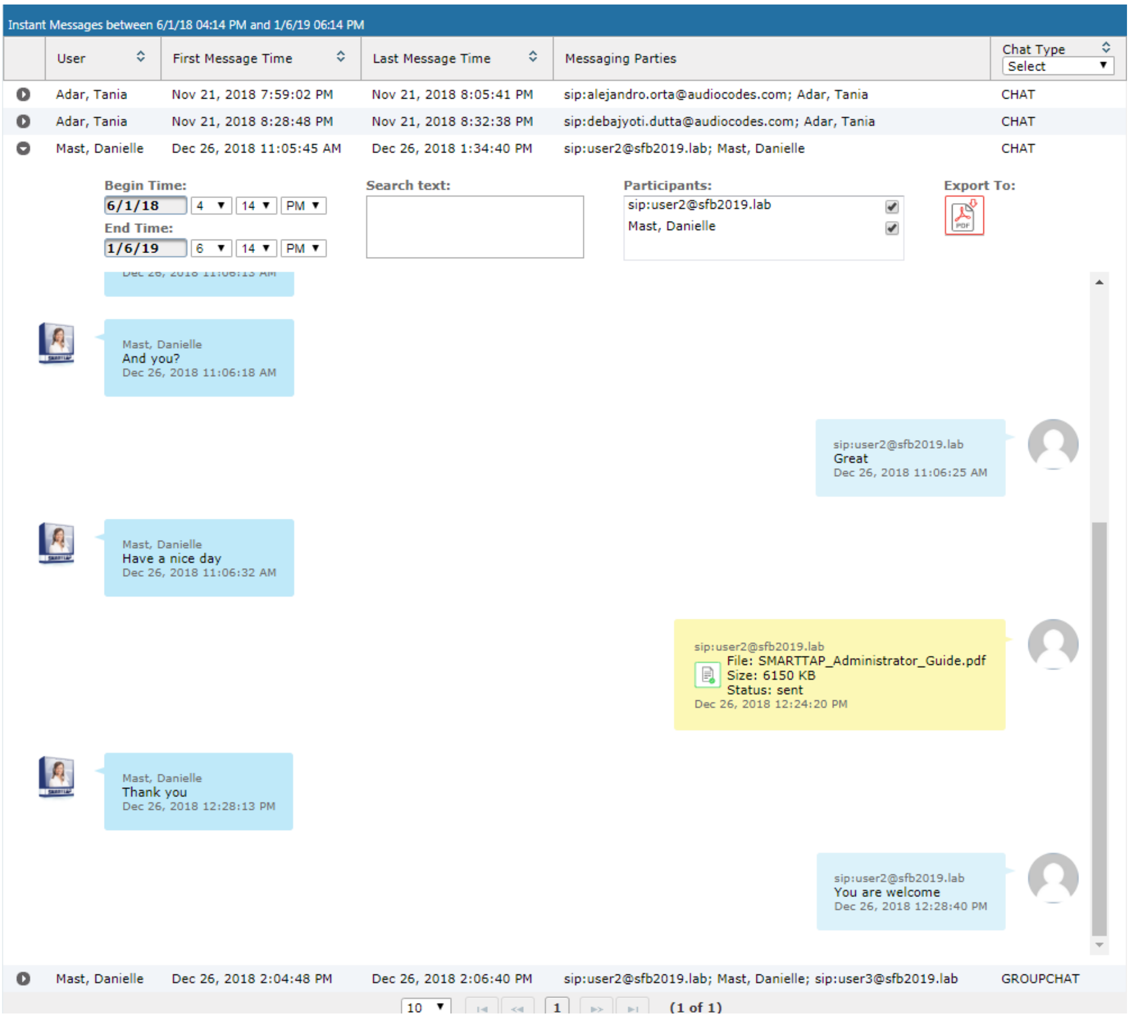
sip:user3@sfb2019.lab
Hello
Dec 26, 2018 2:05:08 PM

sip:user2@sfb2019.lab
How are you?
Dec 26, 2018 2:05:26 PM

Mast, Danielle
Good
Dec 26, 2018 2:05:42 PM

sip:user3@sfb2019.lab
Great
Dec 26, 2018 2:06:40 PM

Figure 6-157: File Transfer Messages



Instant Messages between 6/1/18 04:14 PM and 1/6/19 06:14 PM

	User	First Message Time	Last Message Time	Messaging Parties	Chat Type Select
●	Adar, Tania	Nov 21, 2018 7:59:02 PM	Nov 21, 2018 8:05:41 PM	sip:alejandro.orta@audiocodes.com; Adar, Tania	CHAT
●	Adar, Tania	Nov 21, 2018 8:28:48 PM	Nov 21, 2018 8:32:38 PM	sip:debajyoti.dutta@audiocodes.com; Adar, Tania	CHAT
●	Mast, Danielle	Dec 26, 2018 11:05:45 AM	Dec 26, 2018 1:34:40 PM	sip:user2@sfb2019.lab; Mast, Danielle	CHAT

Begin Time: 6/1/18 4 14 PM

End Time: 1/6/19 6 14 PM

Search text:

Participants:
sip:user2@sfb2019.lab ☑
Mast, Danielle ☑

Export To: PDF

Dec 26, 2018 11:06:13 AM

Mast, Danielle
And you?
Dec 26, 2018 11:06:18 AM

sip:user2@sfb2019.lab
Great
Dec 26, 2018 11:06:25 AM

Mast, Danielle
Have a nice day
Dec 26, 2018 11:06:32 AM

sip:user2@sfb2019.lab
File: SMARTTAP_Administrator_Guide.pdf
Size: 6150 KB
Status: sent
Dec 26, 2018 12:24:20 PM

Mast, Danielle
Thank you
Dec 26, 2018 12:28:13 PM

sip:user2@sfb2019.lab
You are welcome
Dec 26, 2018 12:28:40 PM

●	Mast, Danielle	Dec 26, 2018 2:04:48 PM	Dec 26, 2018 2:06:40 PM	sip:user2@sfb2019.lab; Mast, Danielle; sip:user3@sfb2019.lab	GROUPCHAT

10 1 (1 of 1)

Table 6-63: Message Conversation Content – Field Descriptions

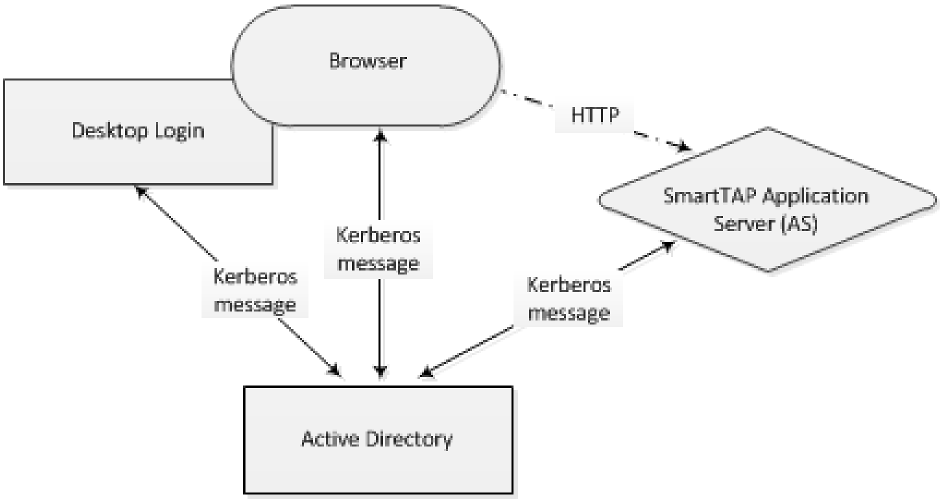
Field	Description
Begin Time	Specifies the time of the first message of the conversation.
End Time	Specifies the time of the last message of the conversation.
Search text	Filters the conversation display to show messages containing the search text. In addition, this field allows the searching for filenames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

⚠ SmartTAP 360° displays a collection of messages in one conversation based on the time and participants.

7 Single Sign-On for SmartTAP 360°

This chapter describes the Single Sign-On functionality for SmartTAP 360°. 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 360° 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 360° to authenticate. When SSO is 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 opens the Welcome page. This allows for a streamlined entry to the SmartTAP 360° Web interface and for quick access to to different SmartTAP 360° pages.

Figure 7-1: Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) Web Authentication Service



- Before getting started, contact AudioCodes support to make sure your network is SSO-ready. In some environments, problems may arise if users from two different domains attempt to perform SSO to the SmartTAP 360° server.
- SSO was successfully tested with both Client Users and the SmartTAP 360° server on the same domain with a single LDAP Active Directory server.
- SSO was successfully tested with Client Users on one domain and with the SmartTAP 360° server on a separate domain, with one-way forest trust between the domains.

Prerequisites

LDAP configuration is optional if all Clients using SSO were manually added to the SmartTAP 360° database. If they were not manually added, then LDAP must be configured so that SmartTAP 360° can validate the user and find the user's Roles/Permissions (see Configuring SSL on page 85

Terms

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

Table 7-1: Terms

Term	Meaning
{username}	New domain user required for SmartTAP 360° 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 360° 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 360° server. Must be in the form {machine name}.{domain}. Example: SmartTAP 360°.myDomain.local. If a CNAME alias is used to map an unfriendly machine name to a friendlier one such as SmartTAP 360°, 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 360°.myDomain.local@MYDOMAIN.LOCAL

Single Sign-On Variables

- **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} ______________________________

Validate the Hostname to be Used for the Principal Name

A CNAME alias for the SmartTAP 360° 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 360° and Wireshark run in order to see what hostname the Client machine will use when requesting a ticket from Kerberos.

Windows KTPASS Command and Choice of User

Active Directory must then be commanded to map the HTTP service on the SmartTAP 360° 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 360° does not need this file to be exported. The Client obtains an encrypted version of the keytab and sends it to SmartTAP 360° as part of the authentication process.

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.

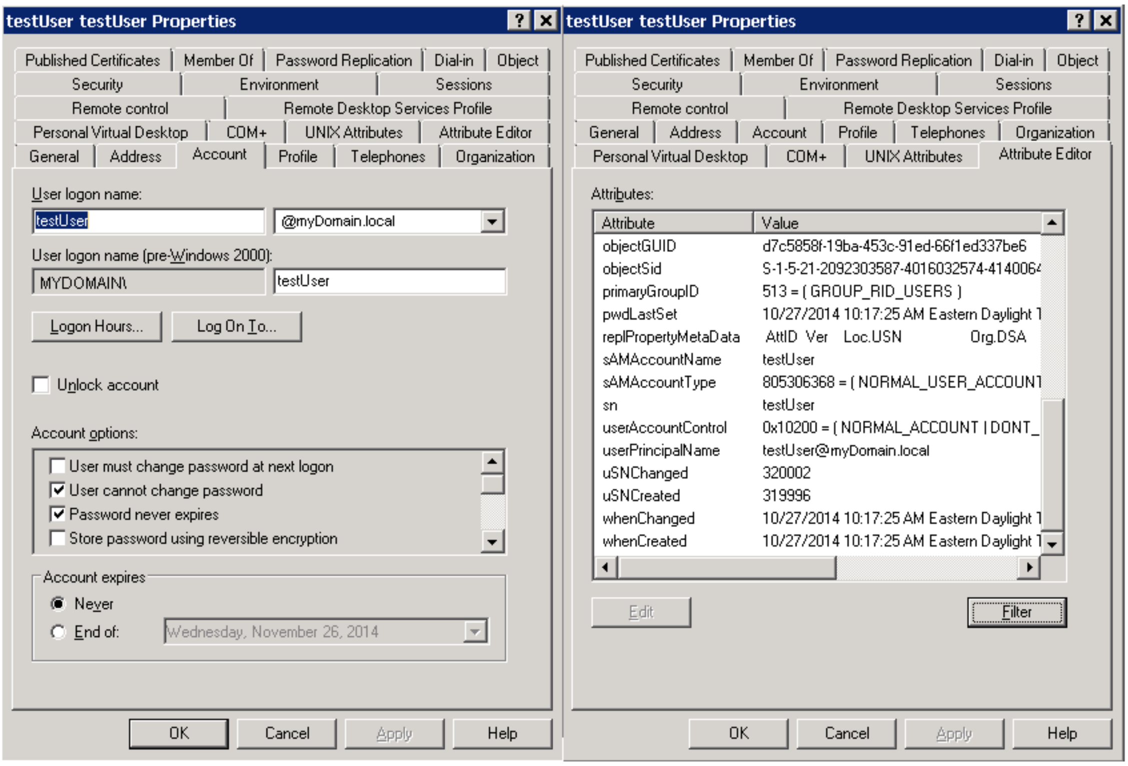
Instead of entering the password, the domain administrator can use the -pass * option. The user is then prompted for the password. Although more secure, in some cases this changes the user's password within Active Directory. If this user is used by SmartTAP 360° for SSO only, this is acceptable. If the 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 360° – one for SSO and one for LDAP. For simplicity, try to use two different users for LDAP and SSO to facilitate troubleshooting and configuration.

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 7-2: Before Running the ktpass Command



User logon name: testUser @myDomain.local

User logon name (pre-Windows 2000): MYDOMAIN\ testUser

□ Unlock account

Account options:

- □ User must change password at next logon
- ☑ User cannot change password
- ☑ Password never expires
- □ Store password using reversible encryption

Account expires

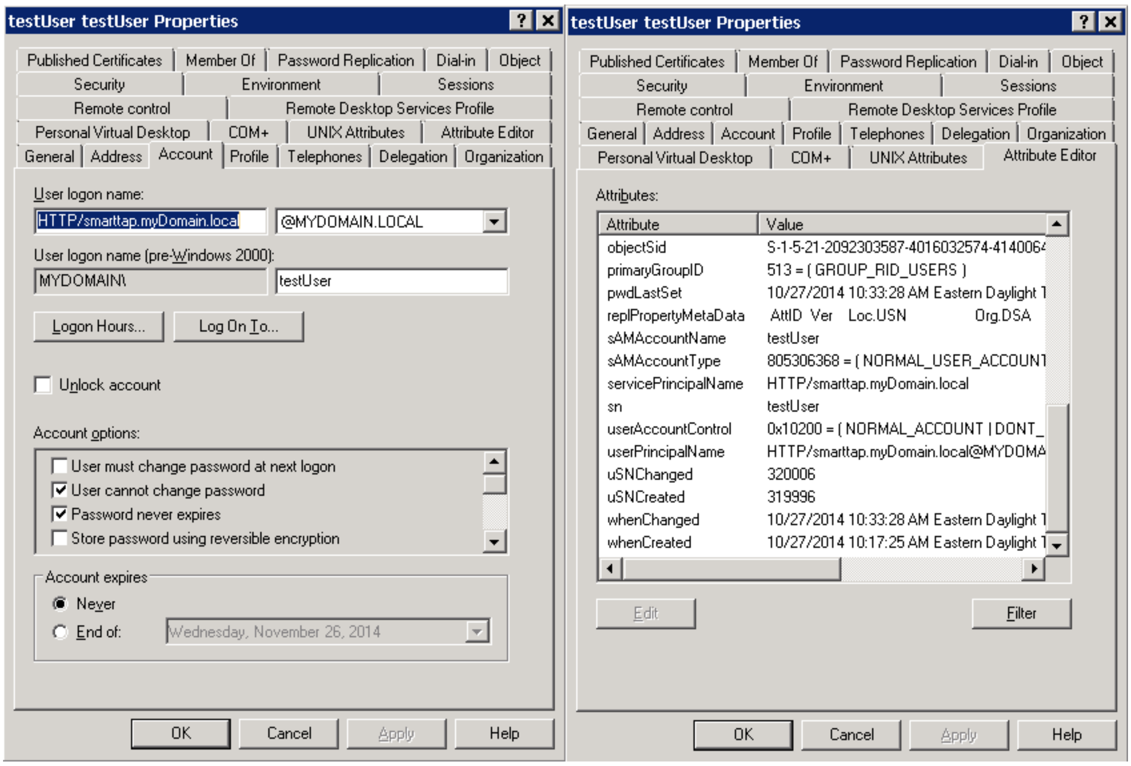
● Never

○ End of: Wednesday, November 26, 2014

Attributes:

Attribute	Value
objectGUID	d7c5858f-19ba-453c-91ed-66f1ed337be6
objectSid	S-1-5-21-2092303587-4016032574-4140064
primaryGroupID	513 = (GROUP_RID_USERS)
pwdLastSet	10/27/2014 10:17:25 AM Eastern Daylight T
replPropertyMetaData	AttID Ver Loc.USN Org.DSA
sAMAccountName	testUser
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT
sn	testUser
userAccountControl	0x10200 = (NORMAL_ACCOUNT | DONT_
userPrincipalName	testUser@myDomain.local
uSNChanged	320002
uSNCreated	319996
whenChanged	10/27/2014 10:17:25 AM Eastern Daylight T
whenCreated	10/27/2014 10:17:25 AM Eastern Daylight T

Figure 7-3: After Running the ktpass Command



User logon name:

HTTP/smarttap.myDomain.local @MYDOMAIN.LOCAL

User logon name (pre-Windows 2000):

MYDOMAIN\ testUser

Logon Hours... Log On To...

□ Unlock account

Account options:

□ User must change password at next logon
☑ User cannot change password
☑ Password never expires
□ Store password using reversible encryption

Account expires

● Never
○ End of: Wednesday, November 26, 2014

Attributes:

Attribute	Value
objectSid	S-1-5-21-2092303587-4016032574-414006
primaryGroupID	513 = (GROUP_RID_USERS)
pwdLastSet	10/27/2014 10:33:28 AM Eastern Daylight T
replPropertyMetaData	AttID Ver Loc.USN Org.DSA
sAMAccountName	testUser
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT
servicePrincipalName	HTTP/smarttap.myDomain.local
sn	testUser
userAccountControl	0x10200 = (NORMAL_ACCOUNT | DONT_
userPrincipalName	HTTP/smarttap.myDomain.local@MYDOMA
uSNChanged	320006
uSNCreated	319996
whenChanged	10/27/2014 10:33:28 AM Eastern Daylight T
whenCreated	10/27/2014 10:17:25 AM Eastern Daylight T

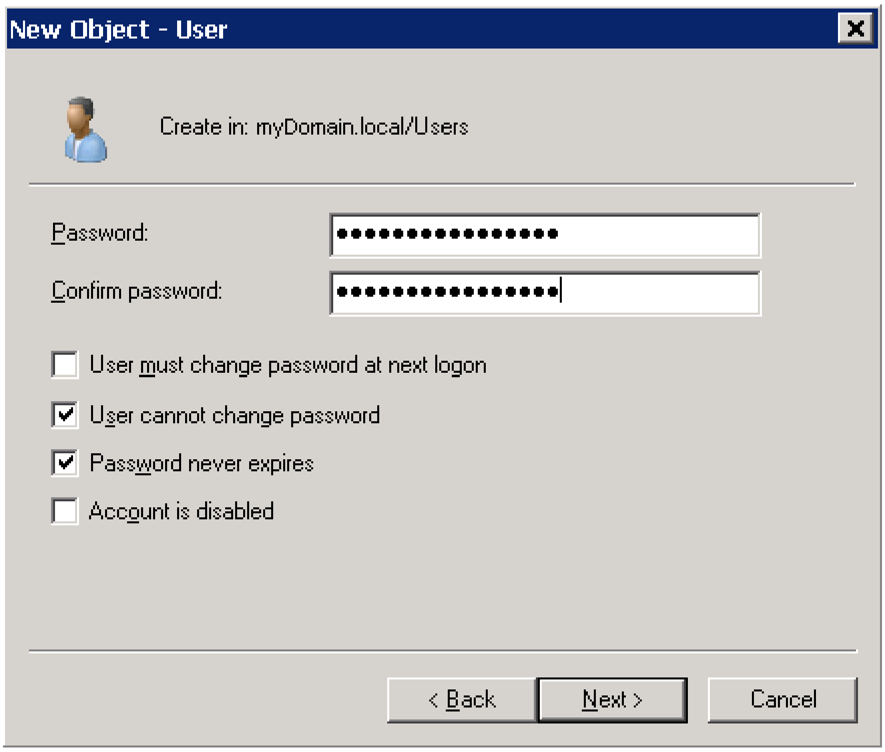
Configuring Active Directory for Single Sign-On

This section describes the steps required for configuring the Active Directory for Single Sign-On.

- **Create a New Domain User:**

  A dedicated user called 'Single Sign On User' or 'SSO User' is required on the domain for the SmartTAP 360° Application Server to use for authenticating clients login attempts. The SSO User is only to be used within SmartTAP 360° and should not be used to log into any machine on the domain, including the SmartTAP 360° 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 7-4: Create a New Domain User



Create in: myDomain.local/Users

Password: ●●●●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●●●●

□ User must change password at next logon

☑ User cannot change password

☑ Password never expires

□ Account is disabled

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
```

The Level of the Encryption Used:. SmartTAP 360° 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.

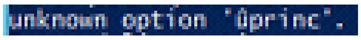
Example:

```
ktpass -princ HTTP/SmartTAP 360°.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 360° 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.

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 360° 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 360° 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.

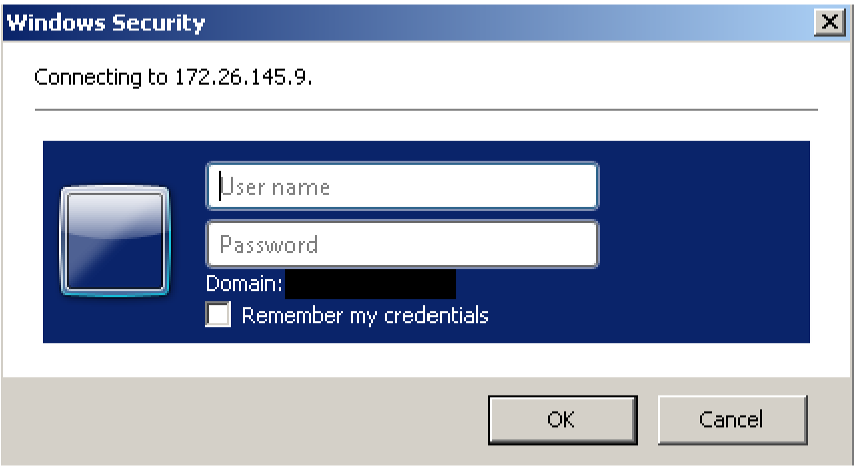
Error 1385: Logon failure: the user has not been granted the requested logon type at this computer indicates that the password is correct but the SSO user is disallowed from running the command. This is acceptable for testing purposes.

Single Sign-On Client Browser Settings

After enabling SSO on SmartTAP 360° , the Web server requests that each client's Web browser negotiate authentication. Most browsers are configured to prompt the authentication negotiation request without making any changes and present this condition to users differently.

- **Internet Explorer**

  When browsing to the SmartTAP 360° Web server, IE prompts the user for credentials. This is not the SmartTAP 360° login form but rather a prompt from IE. The user could enter the domain credentials to log in but this would not be SSO.



Windows Security

Connecting to 172.26.145.9.

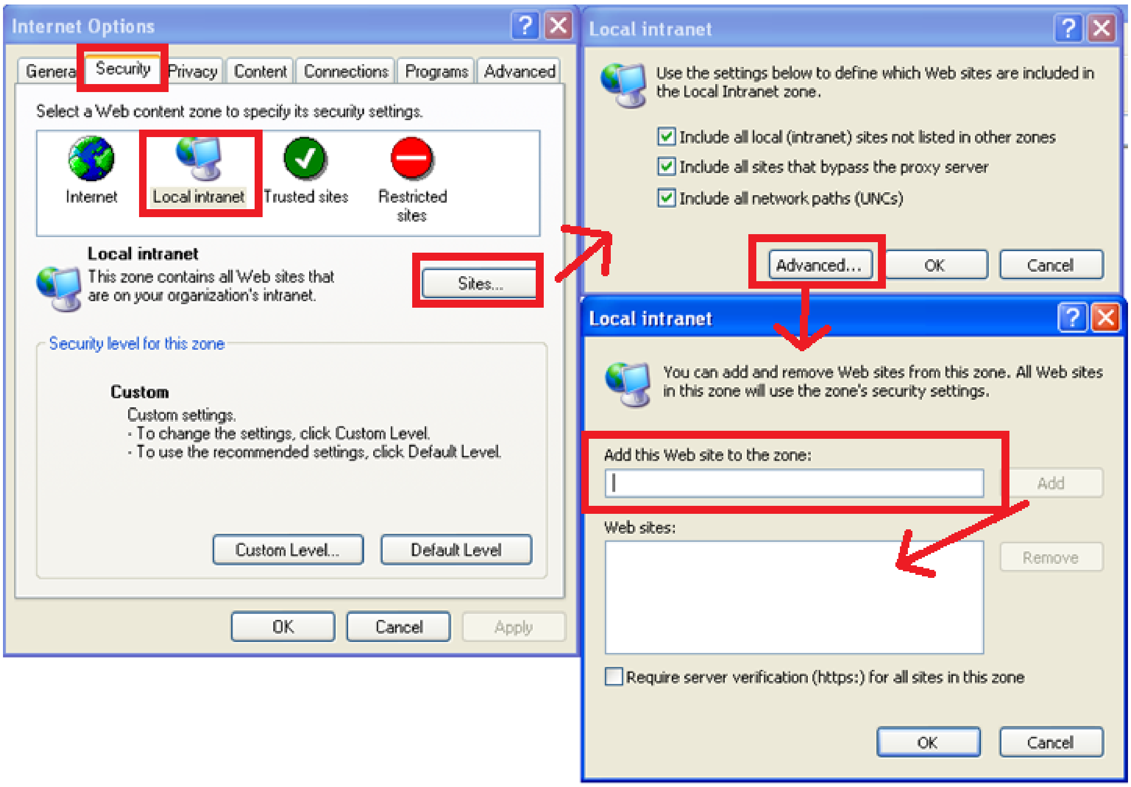
Domain: [redacted]

You must allow IE to negotiate with the SmartTAP 360° Web server. Each browser features a different way of enabling this security feature. IE must be configured to 'trust' the SmartTAP 360° server. IE must be instructed that the SmartTAP 360° server is part of the local intranet so that IE can send proper authentication to the SmartTAP 360° Web server.

a. In IE, open Internet Options > Security tab > Local Intranet zone > Sites… > Advanced… > add the SmartTAP 360° FQDN to the local Intranet zone.

b. Click **OK** to close all windows. All IE instances must be closed.

Figure 7-5: Internet Explorer Browser Settings



Select a Web content zone to specify its security settings.

Local intranet
This zone contains all Web sites that are on your organization's intranet.

Custom
Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.

Use the settings below to define which Web sites are included in the Local Intranet zone.

☑ Include all local (intranet) sites not listed in other zones
☑ Include all sites that bypass the proxy server
☑ Include all network paths (UNCs)

You can add and remove Web sites from this zone. All Web sites in this zone will use the zone's security settings.

Add this Web site to the zone:

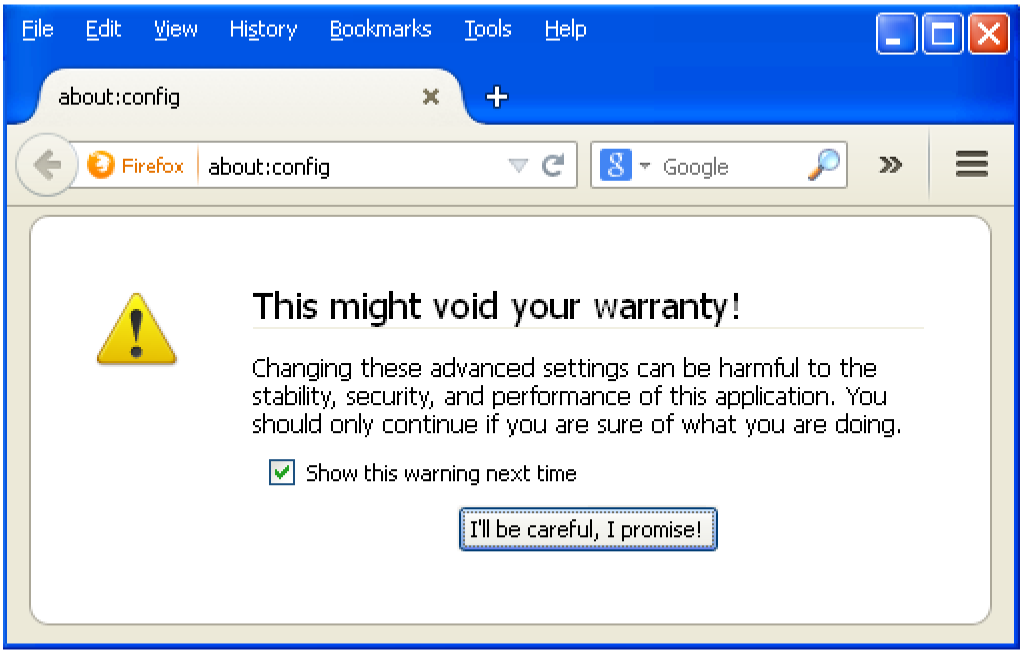
□ Require server verification (https:) for all sites in this zone

Firefox Browser Settings

Firefox issues a 401 error code instead of negotiating security.

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

Figure 7-6: Firefox Advanced Settings



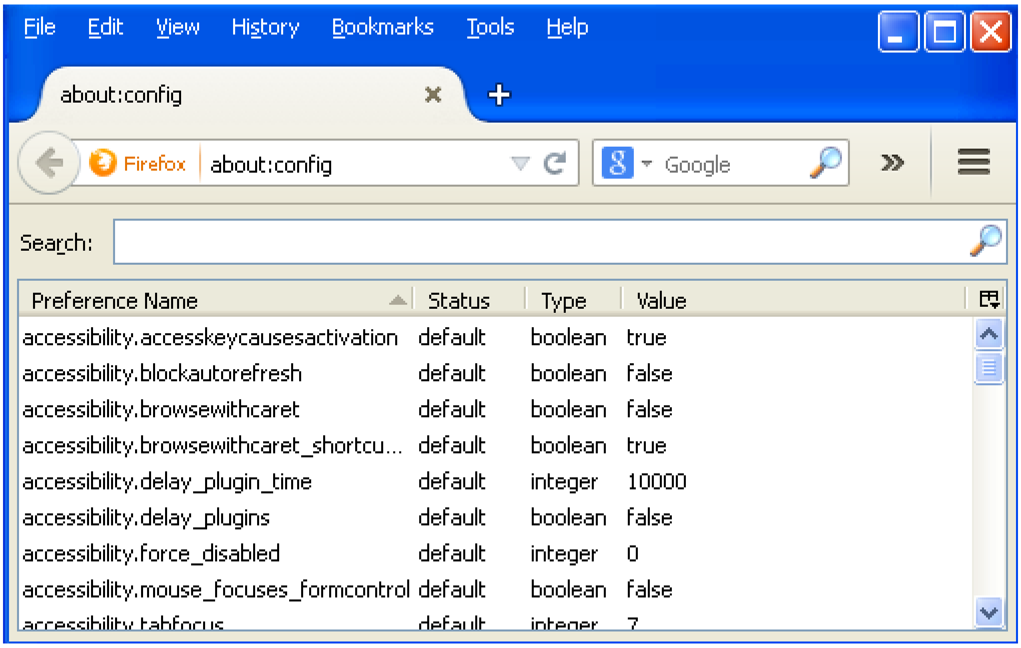
This might void your warranty!

Changing these advanced settings can be harmful to the stability, security, and performance of this application. You should only continue if you are sure of what you are doing.

☑ Show this warning next time

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

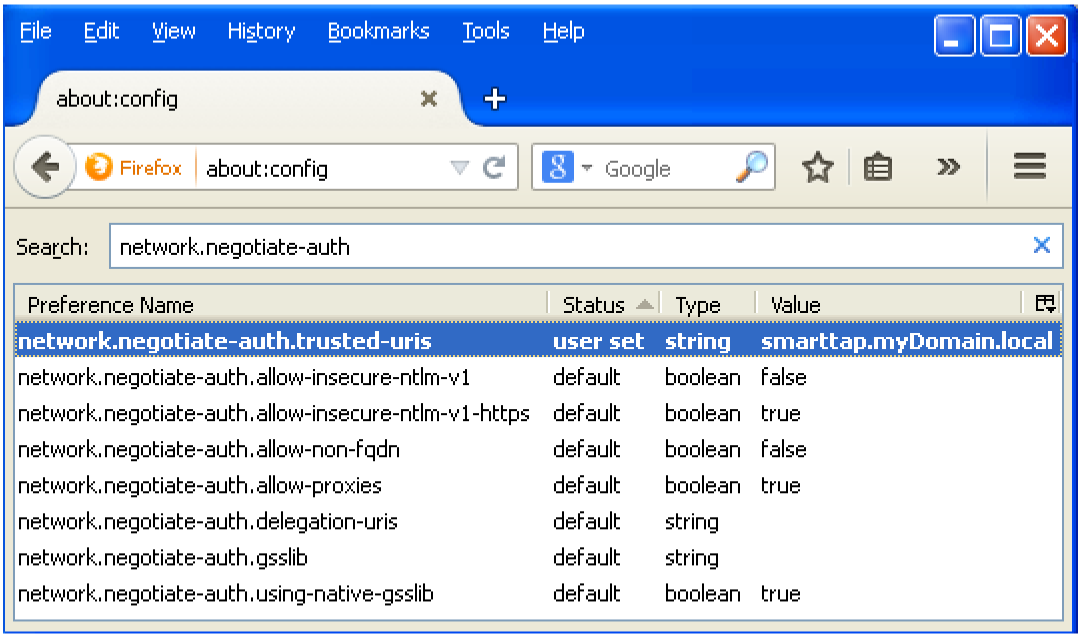
Figure 7-7: Firefox about:config



Preference Name	Status	Type	Value
accessibility.accesskeycausesactivation	default	boolean	true
accessibility.blockautorefresh	default	boolean	false
accessibility.browsewithcaret	default	boolean	false
accessibility.browsewithcaret_shortcu...	default	boolean	true
accessibility.delay_plugin_time	default	integer	10000
accessibility.delay_plugins	default	boolean	false
accessibility.force_disabled	default	integer	0
accessibility.mouse_focuses_formcontrol	default	boolean	false
accessibility.tabfocus	default	integer	7

c. In the 'Search' field, enter network.negotiate-auth to show all negotiation options. SmartTAP 360° 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 7-8: Firefox about:config



Search: network.negotiate-auth

Preference Name	Status	Type	Value
network.negotiate-auth.trusted-uris	**user set**	**string**	**smarttap.myDomain.local**
network.negotiate-auth.allow-insecure-ntlm-v1	default	boolean	false
network.negotiate-auth.allow-insecure-ntlm-v1-https	default	boolean	true
network.negotiate-auth.allow-non-fqdn	default	boolean	false
network.negotiate-auth.allow-proxies	default	boolean	true
network.negotiate-auth.delegation-uris	default	string	
network.negotiate-auth.gsslib	default	string	
network.negotiate-auth.using-native-gsslib	default	boolean	true

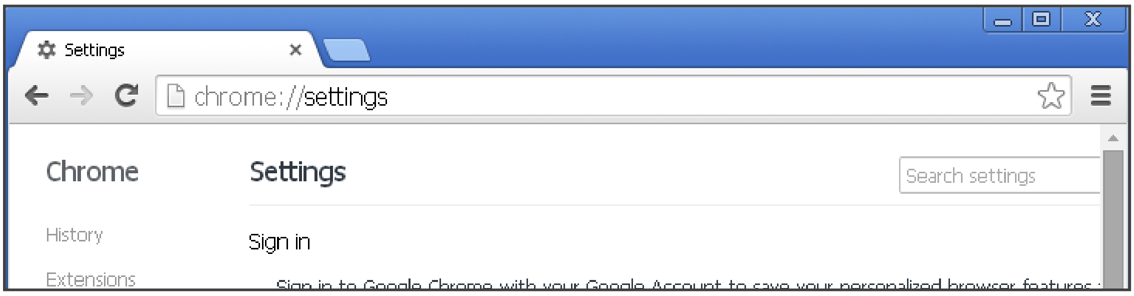
⚠ Additional changes may be required for Firefox. If SSO does not function immediately after these changes, see Single Sign- On Client Browser Settings on page 203Troubleshooting . [Tested: Firefox 32.0.3 on Windows XP and Windows 7. Also Firefox 35.0.1 on Windows 7].

Google Chrome

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.

a. 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.

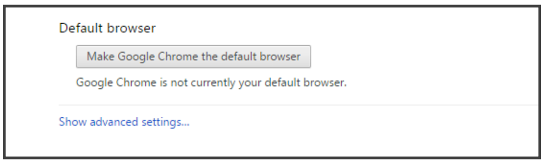
Figure 7-9: Google Chrome Browser Settings



Sign in to Google Chrome with your Google Account to save your personalized browser features

b. 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 7-10: Google Chrome Browser Settings – Show advanced settings

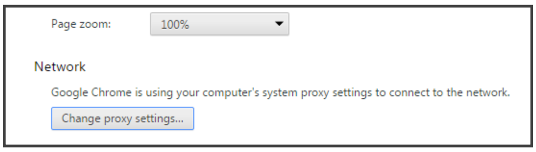

Default browser
Make Google Chrome the default browser

Google Chrome is not currently your default browser.

Show advanced settings...

c. 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 7-11: Google Chrome Browser Settings – Change proxy settings

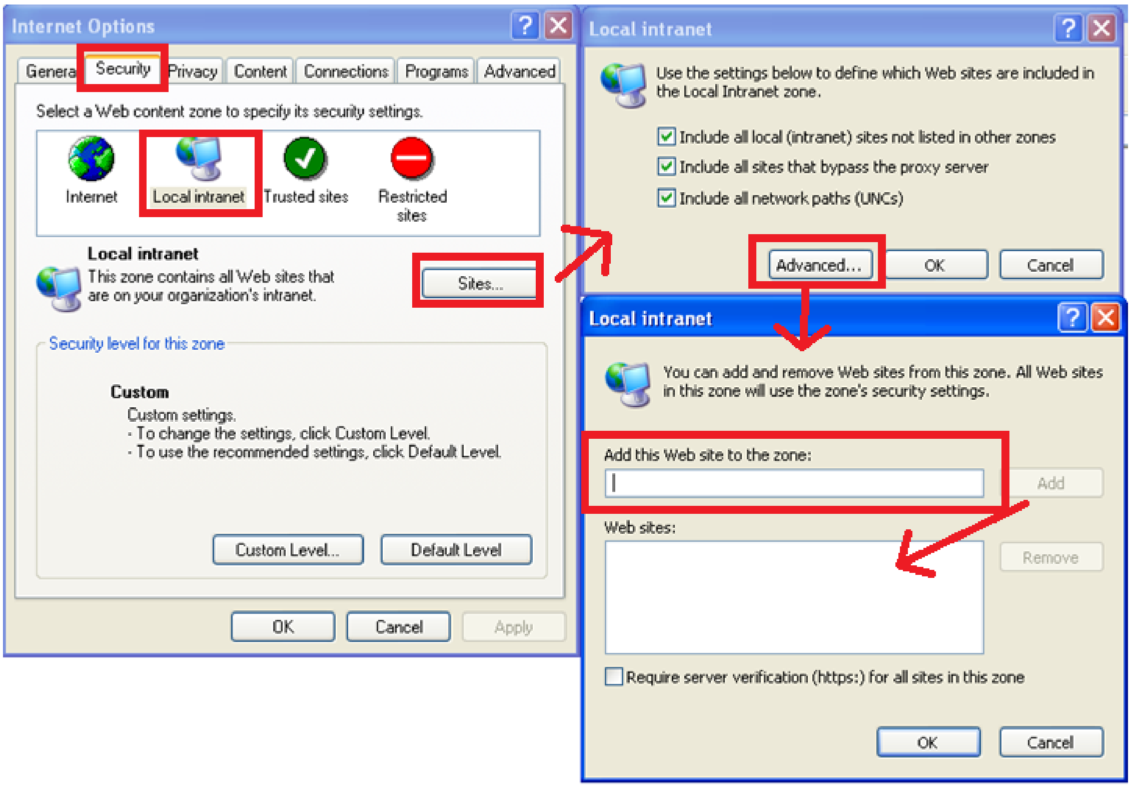

Page zoom: 100%

Google Chrome is using your computer's system proxy settings to connect to the network.

d. Follow the same instructions as IE (Security tab > Local Intranet zone > Sites... > Advanced... > add the SmartTAP 360° FQDN to the local Intranet zone).

e. Close all Google Chrome windows and restart; SSO now functions.

Figure 7-12: Google Chrome Browser Settings – Adding a Web Site to the Zone



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a Web content zone to specify its security settings.

Internet | Local intranet | Trusted sites | Restricted sites

Local intranet
This zone contains all Web sites that are on your organization's intranet.

Sites...

Security level for this zone

Custom
Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.

Custom Level... | Default Level

OK | Cancel | Apply

Local intranet

Use the settings below to define which Web sites are included in the Local Intranet zone.

☑ Include all local (intranet) sites not listed in other zones
☑ Include all sites that bypass the proxy server
☑ Include all network paths (UNCs)

Advanced... | OK | Cancel

Local intranet

You can add and remove Web sites from this zone. All Web sites in this zone will use the zone's security settings.

Add this Web site to the zone:

Add

Web sites:

Remove

☐ Require server verification (https:) for all sites in this zone

OK | Cancel

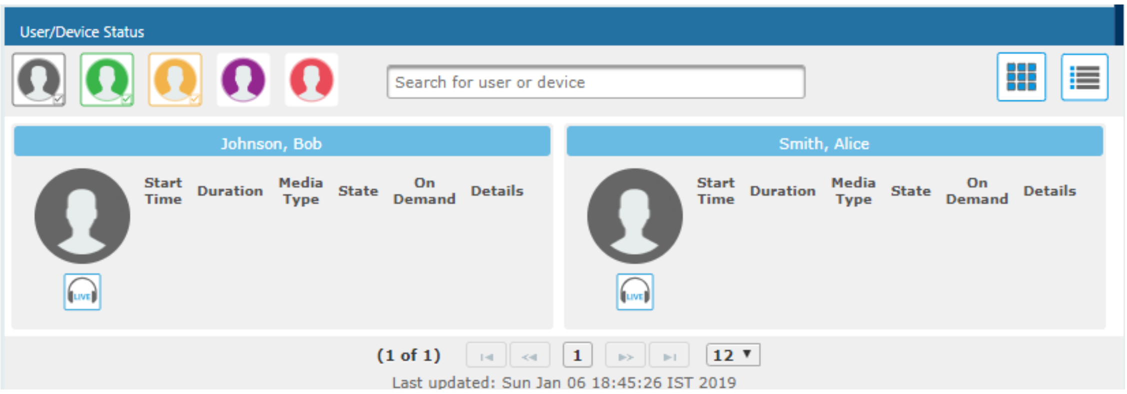
Testing Single Sign-On

After logging into the domain computer and configuring the browser to trust the SmartTAP 360° server as described in previous sections, you can browse to the SmartTAP 360° Web server, preferably via the SmartTAP 360° server's FQDN. You may briefly see the Redirecting notification:

Redirecting

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 7-13: Browsing to the SmartTAP 360° Web Server



User/Device Status

Search for user or device

Johnson, Bob

Start Time	Duration	Media Type	State	On Demand	Details

Smith, Alice

Start Time	Duration	Media Type	State	On Demand	Details

(1 of 1) 1 12

Last updated: Sun Jan 06 18:45:26 IST 2019

If an error page is displayed, or if the normal login form for SmartTAP 360° is displayed, SSO has malfunctioned – see Troubleshooting Single Sign-On below.

Troubleshooting Single Sign-On

Frequently Asked Questions

When SSO is enabled, how can I log in as the default SmartTAP 360° administrative user?

SSO is enabled, so all login attempts will automatically attempt SSO as the domain user logged into the client machine. The SmartTAP 360° 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 360° via SSO. The form login page of SmartTAP 360° must be accessed in order to log in as this user.

It is recommended that a domain user be given valid SmartTAP 360° permissions to make system changes so that the default SmartTAP 360° administrative user can be removed.

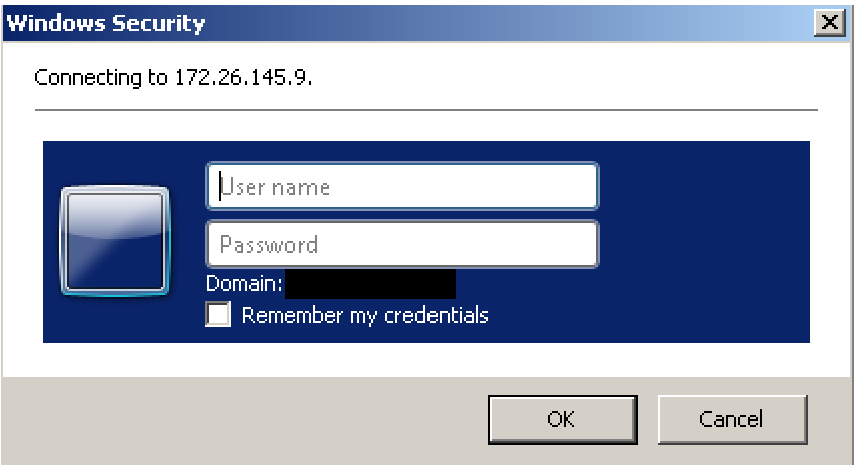
How can the form login page be accessed for non-SSO logins?

There are a few ways to do this:

- Browse to the SmartTAP 360° 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 360° 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 360° 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 360° 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):



Connecting to 172.26.145.9.

Domain: [redacted]

This prompt is prompting for the client's domain credentials, not the SmartTAP 360° 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 360° as that user.
- Clicking 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.

Troubleshooting

- **HTTP Error Codes**

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

Table 7-2: HTTP Error Codes

Error Code	Description
400 – Bad Request	Indicates that part of the HTTP Request is malformed. When using SmartTAP 360° 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 360° 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 360°.xml file for the SmartTAP 360° 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 360° 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 Troubleshooting Single Sign-On on the previous pageFirefox Browser Settings .
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

Error Code	Description
	occur if the user manually browses to a page they're not allowed to access. Another cause is if SmartTAP 360° cannot determine the User Roles/Permissions for this user. Make sure the user performing SSO is part of the domain and that SmartTAP 360° can find this loginId through LDAP or in its own database. Make sure LDAP is configured correctly and can communicate with Active Directory.

SmartTAP 360° 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 360° server (see Appendix Troubleshooting Single Sign-On on page 208Firefox Browser Settings) though instances occur in which the Firefox browser does not attempt to authenticate even when the SmartTAP 360° 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 Resetting the Configuration to Firefox Browser 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 360°.

- 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 360° GUI.
    - Validate whether the user's password was changed or not - see Verify the User Credentials.
    - To resolve the error, reset the SSO user's password, re-enter this same password into the SmartTAP 360° 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 360° 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 360°. 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 360° from a Firefox browser, with trusted site configured.

Troubleshooting with More Detailed SmartTAP 360° 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 360° logging.

The loggers can be configured through the SmartTAP 360° 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 360°.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
```

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 360°. To do this, see the Mozilla guide at https://support.mozilla.org/en-US/kb/reset-preferences-fix-problems.

⚠ 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.

Refresh Firefox

This section instructs you how to refresh Firefox.

a. Click the menu button ≡, click help ? and select Troubleshooting Information; the Troubleshooting Information tab opens.

b. Click the Refresh Firefox button in the uppermost right corner of the Troubleshooting Information tab.

c. 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.

d. If previously set, the 'Trusted URIs' configuration will be lost. Follow the steps in the Firefox Browser configuration to assign the SmartTAP 360° server as a trusted server.

e. Attempt SSO again; if SSO still doesn't work, delete Firefox preference files as shown in the next section.

Delete Firefox Preference Files

This section instructs you how to delete Firefox preference files.

➢ To delete Firefox preference files:

a. Click the menu button ≡, click help ? and select Troubleshooting Information; the Troubleshooting Information tab opens.

b. Under the Application Basics section, click Show Folder; a window opens displaying your profile files.

c. Click the menu button ≡ and then click Exit ⏻.

d. 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.

e. Close the profile folder and open Firefox.

f. If previously set, the 'Trusted URIs' configuration will be lost. Follow the steps in the Firefox Browser configuration to assign the SmartTAP 360° server as a trusted server.

g. Attempt SSO again; if SSO still does not work, uninstall and reinstall Firefox as shown in the next section.

Uninstall & Reinstall Firefox

a. Uninstall Firefox through the Windows Control Panel.

b. Make sure all Firefox data stored in the following locations is removed:

C:\Users\<user>\AppData\Local\Mozilla\
C:\Users\<user>\AppData\Roaming\Mozilla\
[Optional] Reboot the machine.

c. Reinstall the latest version of Firefox. It may be a good idea to download the latest version from Mozilla again, to be safe.

d. After the installation, follow the steps in the Firefox Browser configuration to assign the SmartTAP 360° server as a trusted server.

e. Attempt SSO again.

8 SmartTAP 360° Skype for Business Toolbar

The SmartTAP 360° Skype for Business Toolbar functions in conjunction with the Skype for Business 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 360° GUI separately.The toolbar is by default not enabled and must be installed / configured by AudioCodes, a certified AudioCodes Partner or by your local IT expert.

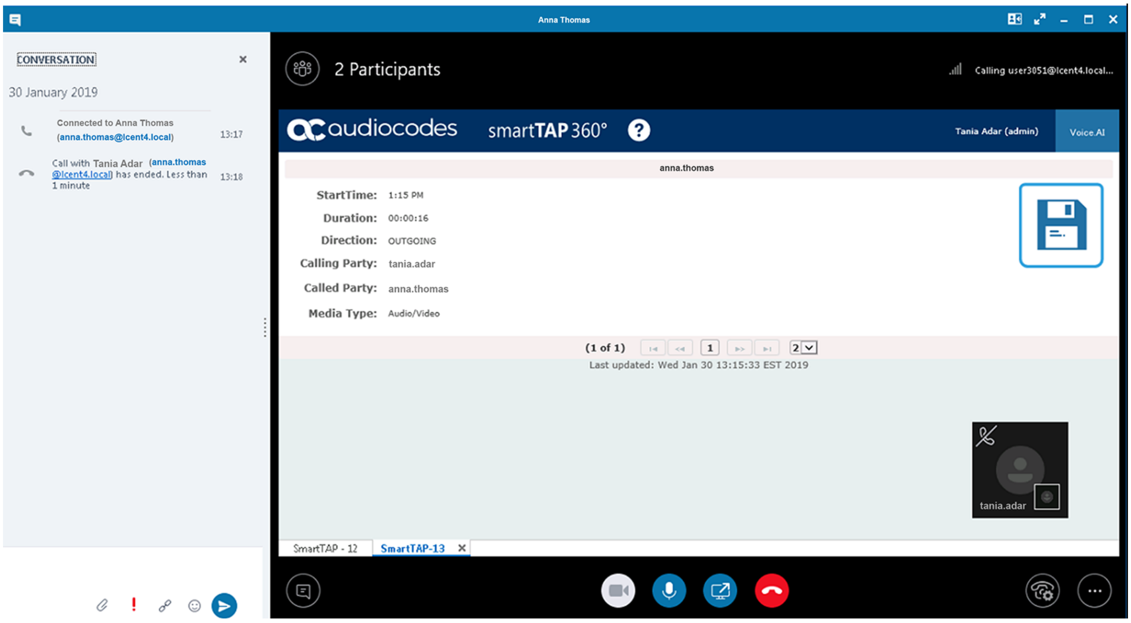
⚠ To learn more about Microsoft Skype for Business CWE, refer to: http://msdn.microsoft.com/en-us/library/office/jj933101(v=office.15).aspx

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 8-1: SmartTAP 360°: Save On Demand (SOD)



30 January 2019

Connected to Anna Thomas (anna.thomas@lcent4.local) 13:17

Call with Tania Adar (anna.thomas@lcent4.local) has ended. Less than 1 minute 13:18

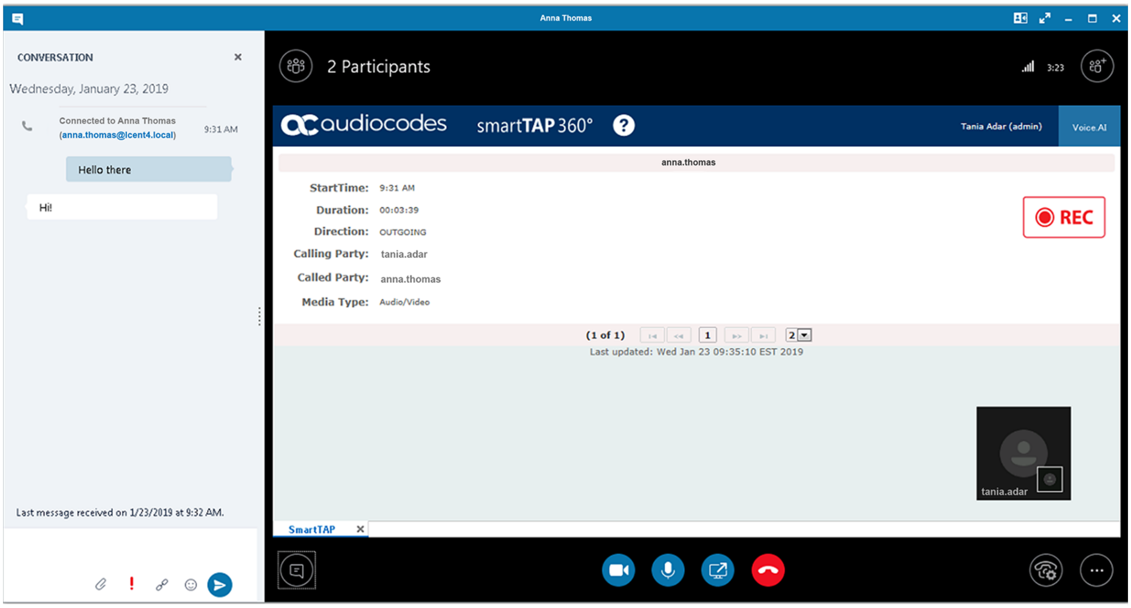
anna.thomas

StartTime: 1:15 PM
Duration: 00:00:16
Direction: OUTGOING
Calling Party: tania.adar
Called Party: anna.thomas
Media Type: Audio/Video

(1 of 1) 1 2

Last updated: Wed Jan 30 13:15:33 EST 2019

Figure 8-2: Record on Demand (ROD)



Wednesday, January 23, 2019

Connected to Anna Thomas (anna.thomas@lcent4.local) 9:31 AM

Hello there

Hi!

Last message received on 1/23/2019 at 9:32 AM.

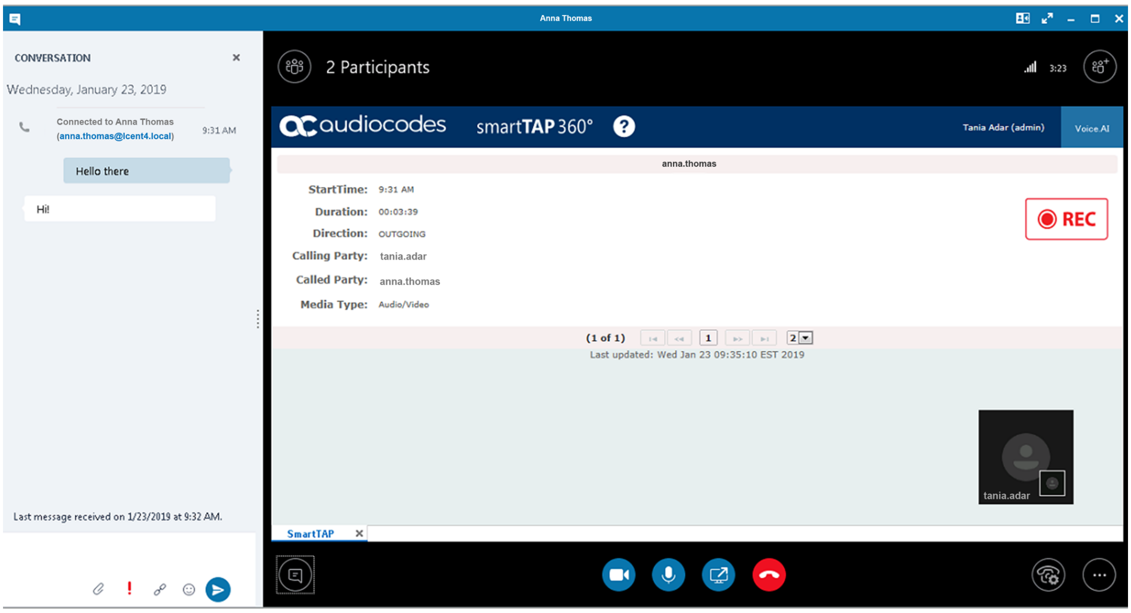
anna.thomas

StartTime: 9:31 AM
Duration: 00:03:39
Direction: OUTGOING
Calling Party: tania.adar
Called Party: anna.thomas
Media Type: Audio/Video

(1 of 1) 1 2

Last updated: Wed Jan 23 09:35:10 EST 2019

Figure 8-3: SmartTAP 360° Skype for Business CWE Toolbar (Pause / Resume)



Anna Thomas

CONVERSATION

Wednesday, January 23, 2019

Connected to Anna Thomas (anna.thomas@lcent4.local) 9:31 AM

Hello there

Hi!

Last message received on 1/23/2019 at 9:32 AM.

2 Participants 3:23

audiocodes smartTAP 360° Tania Adar (admin) Voice.AI

anna.thomas

StartTime: 9:31 AM

Duration: 00:03:39

Direction: OUTGOING

Calling Party: tania.adar

Called Party: anna.thomas

Media Type: Audio/Video

(1 of 1) 1 2

Last updated: Wed Jan 23 09:35:10 EST 2019

9 Media Exporter

Media Exporter is a separate desktop application useful for compliance officers or for those who need to download bulk calls from SmartTAP 360° for a specific user or for all users within a date/time range.

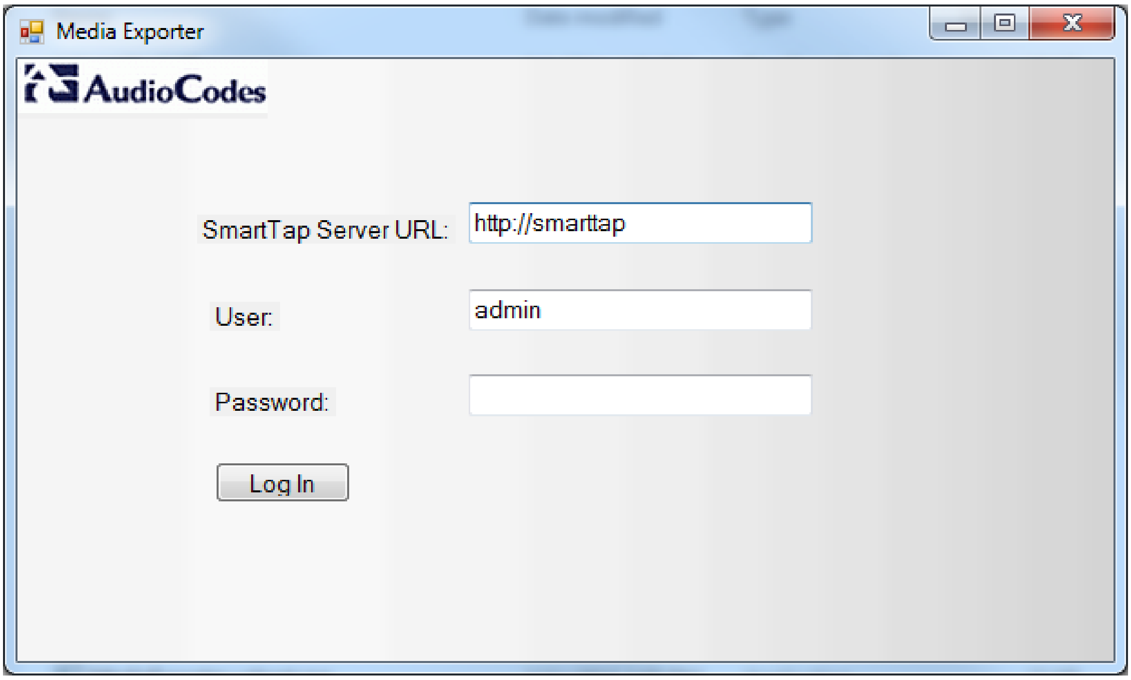
> ⚠ The number of exported recordings is limited to 1500. The download time depends on the system specifications and load. It takes approximately 10-15 minutes to download 100 call recordings with an average duration of 5 minutes on an idle system with 4 cores. It is not recommended to export a higher number of records during system working hours.

The search parameters are similar to the SmartTAP 360° UI. Administrators must enter their credentials to access the application. Security credentials assigned by SmartTAP 360° determine which users will be visible and whose associated calls will be available for downloading.

> ⚠ 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 360° URL to be used to access the SmartTAP 360° UI
   - Enter the username (same as that used to access the SmartTAP 360° UI)
   - Enter the password

Figure 9-1: Credentials



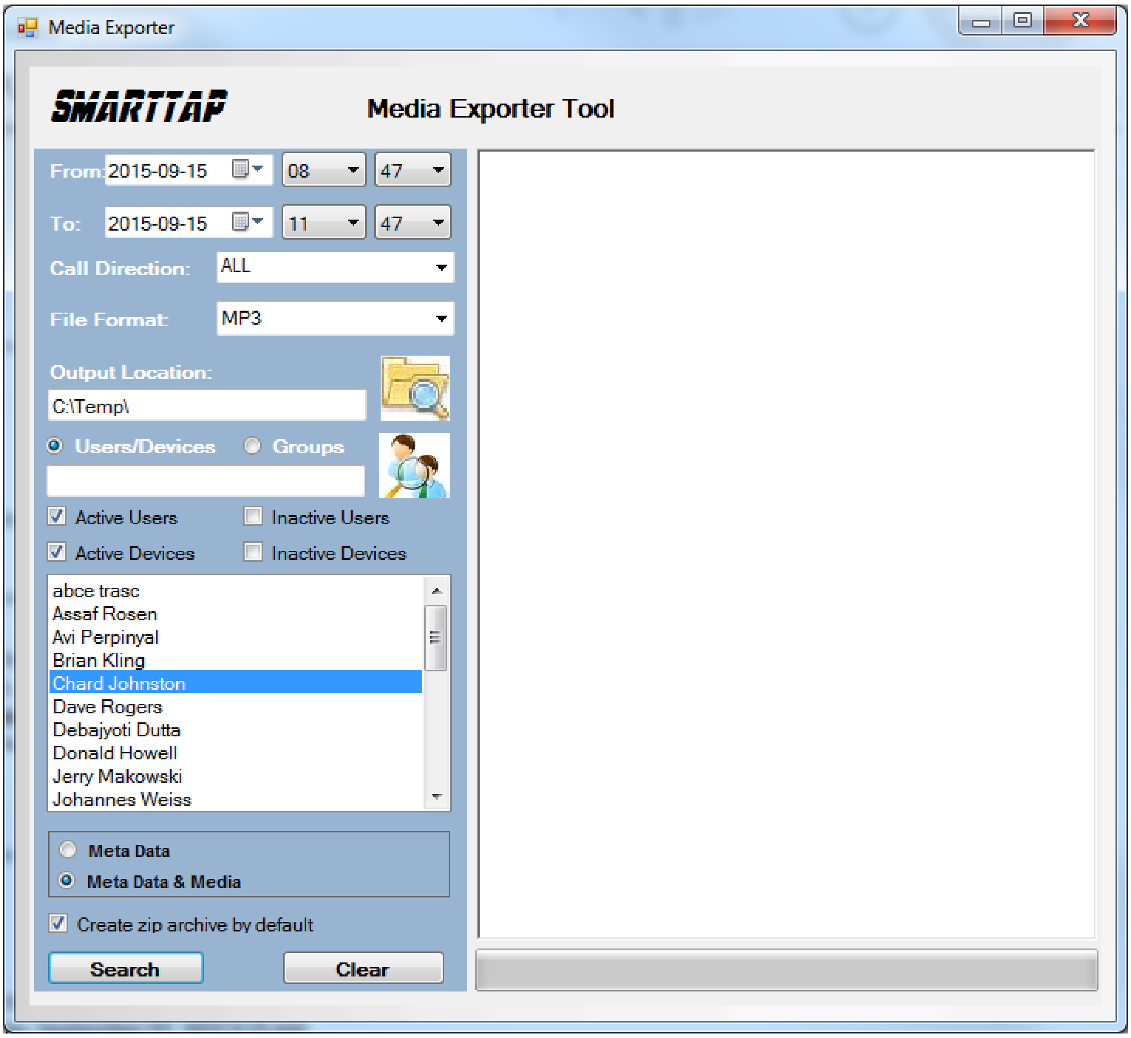
SmartTap Server URL: http://smarttap

User: admin

Password:

3. Enter the Search Criteria.

Figure 9-2: Enter the Search Criteria



From: 2015-09-15 08 47

To: 2015-09-15 11 47

Call Direction: ALL

File Format: MP3

Output Location: C:\Temp\

● Users/Devices ○ Groups

☑ Active Users ☐ Inactive Users

☑ Active Devices ☐ Inactive Devices

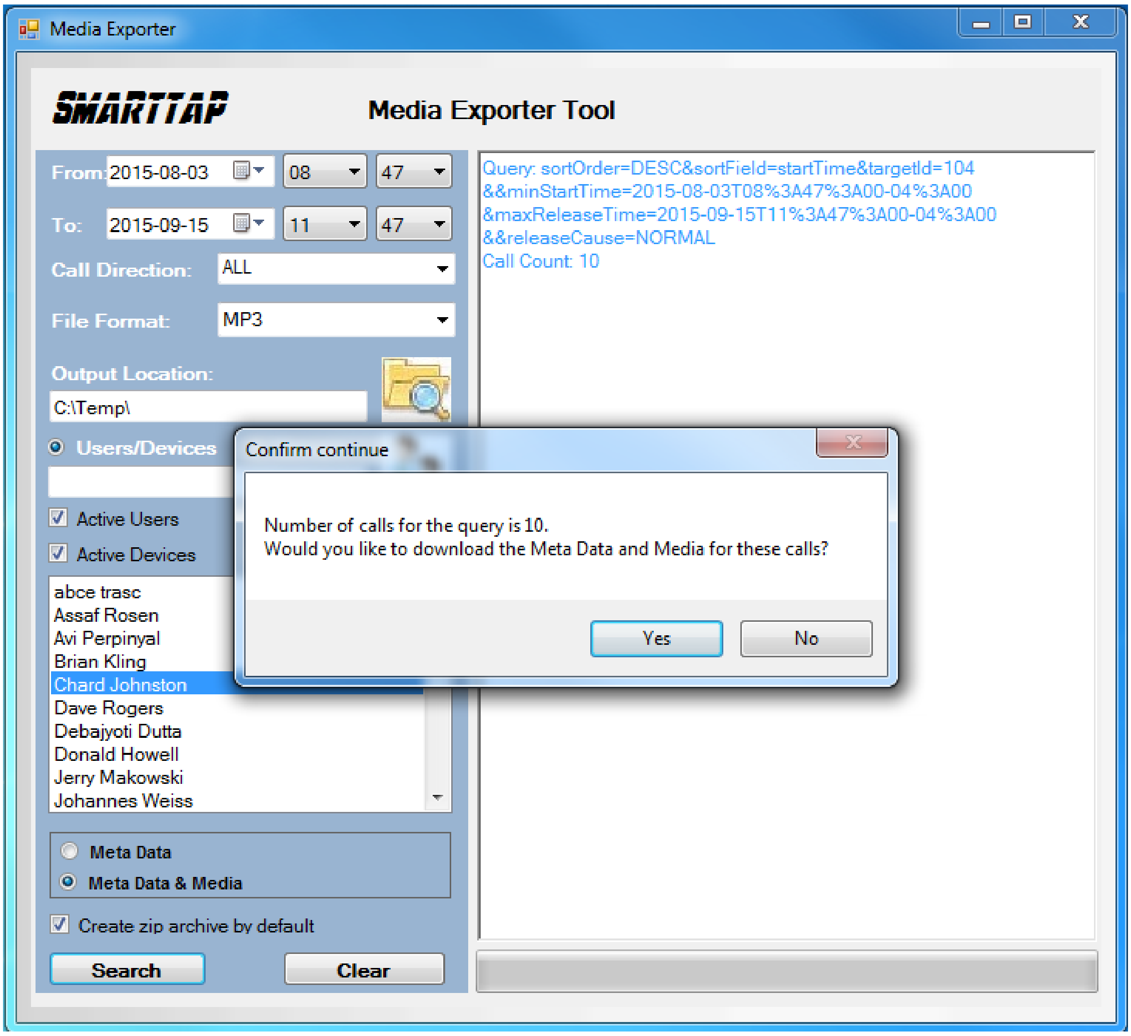
abce trasc
Assaf Rosen
Avi Perpinyal
Brian Kling
Chard Johnston
Dave Rogers
Debajyoti Dutta
Donald Howell
Jerry Makowski
Johannes Weiss

○ Meta Data
● Meta Data & Media

☑ Create zip archive by default

- The following search criteria definitions are identical to those of the SmartTAP 360° Web interface:
  - 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 9-3: Search Results



From: 2015-08-03 08 47

To: 2015-09-15 11 47

Call Direction: ALL

File Format: MP3

Output Location: C:\Temp\

● Users/Devices

☑ Active Users

☑ Active Devices

abce trasc
Assaf Rosen
Avi Perpinyal
Brian Kling
Chard Johnston
Dave Rogers
Debajyoti Dutta
Donald Howell
Jerry Makowski
Johannes Weiss

○ Meta Data
● Meta Data & Media

☑ Create zip archive by default

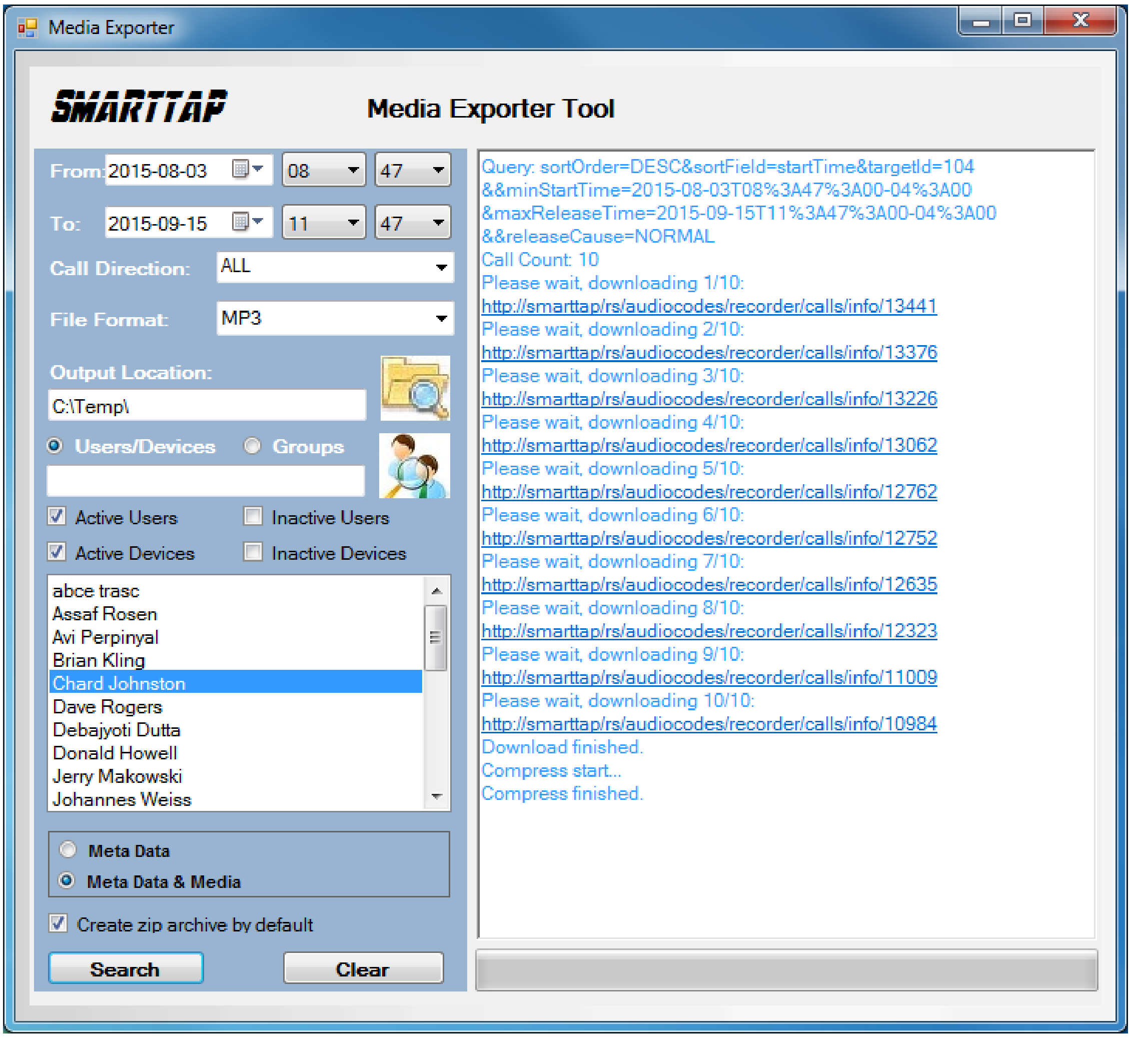
Query: sortOrder=DESC&sortField=startTime&targetId=104
&&minStartTime=2015-08-03T08%3A47%3A00-04%3A00
&maxReleaseTime=2015-09-15T11%3A47%3A00-04%3A00
&&releaseCause=NORMAL
Call Count: 10

Confirm continue

Number of calls for the query is 10.
Would you like to download the Meta Data and Media for these calls?

4. Select Yes to start downloading the calls.

Figure 9-4: Downloading



From: 2015-08-03 08 47

To: 2015-09-15 11 47

Call Direction: ALL

File Format: MP3

Output Location: C:\Temp\

● Users/Devices ○ Groups

☑ Active Users ☐ Inactive Users

☑ Active Devices ☐ Inactive Devices

abce trasc
Assaf Rosen
Avi Perpinyal
Brian Kling
Chard Johnston
Dave Rogers
Debajyoti Dutta
Donald Howell
Jerry Makowski
Johannes Weiss

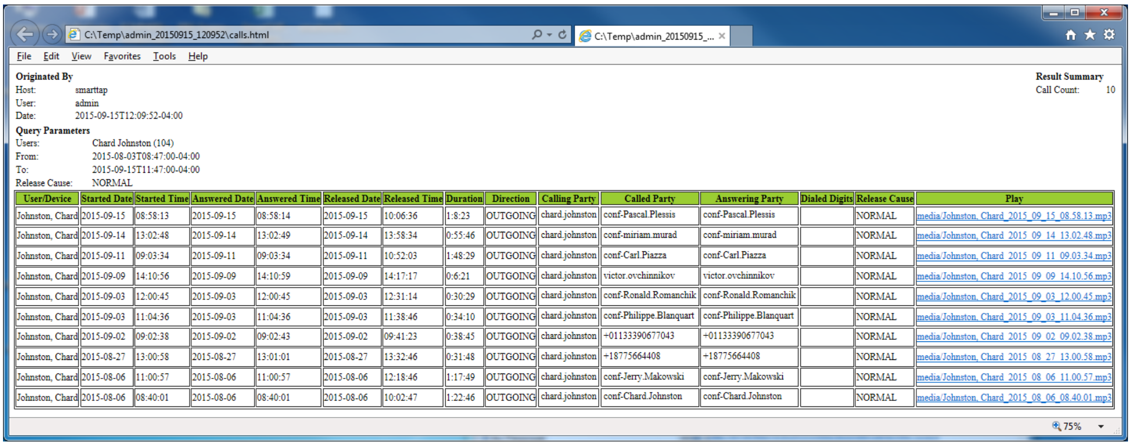
○ Meta Data
● Meta Data & Media

☑ Create zip archive by default

```
Query: sortOrder=DESC&sortField=startTime&targetId=104
&&minStartTime=2015-08-03T08%3A47%3A00-04%3A00
&maxReleaseTime=2015-09-15T11%3A47%3A00-04%3A00
&&releaseCause=NORMAL
Call Count: 10
Please wait, downloading 1/10:
http://smarttap/rs/audiocodes/recorder/calls/info/13441
Please wait, downloading 2/10:
http://smarttap/rs/audiocodes/recorder/calls/info/13376
Please wait, downloading 3/10:
http://smarttap/rs/audiocodes/recorder/calls/info/13226
Please wait, downloading 4/10:
http://smarttap/rs/audiocodes/recorder/calls/info/13062
Please wait, downloading 5/10:
http://smarttap/rs/audiocodes/recorder/calls/info/12762
Please wait, downloading 6/10:
http://smarttap/rs/audiocodes/recorder/calls/info/12752
Please wait, downloading 7/10:
http://smarttap/rs/audiocodes/recorder/calls/info/12635
Please wait, downloading 8/10:
http://smarttap/rs/audiocodes/recorder/calls/info/12323
Please wait, downloading 9/10:
http://smarttap/rs/audiocodes/recorder/calls/info/11009
Please wait, downloading 10/10:
http://smarttap/rs/audiocodes/recorder/calls/info/10984
Download finished.
Compress start...
Compress finished.
```

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

Figure 9-5: Call Manifest


C:\Temp\admin_20150915_120952\calls.html
C:\Temp\admin_20150915_...
File Edit View Favorites Tools Help
75%

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

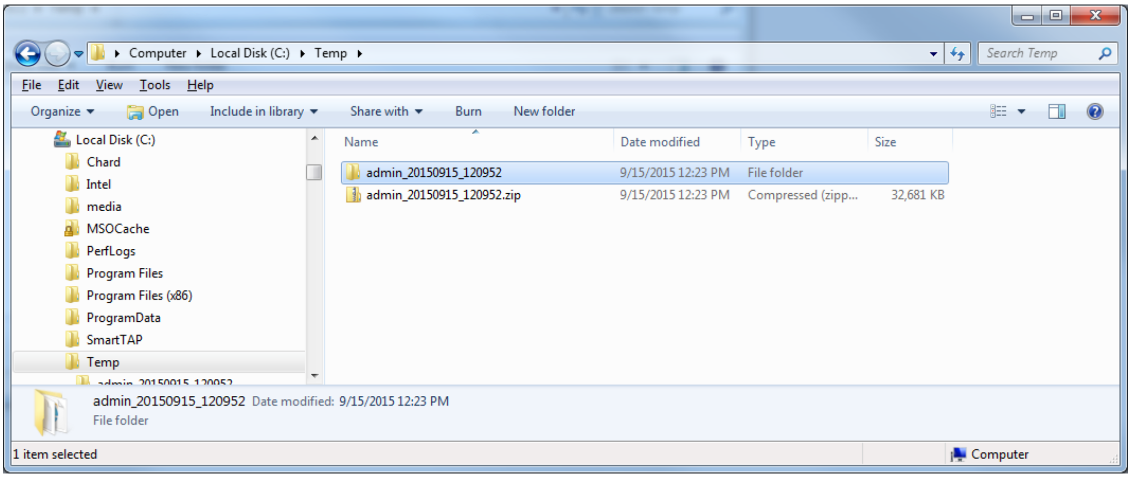
Result Summary
Call Count: 10

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 9-6: Output Location

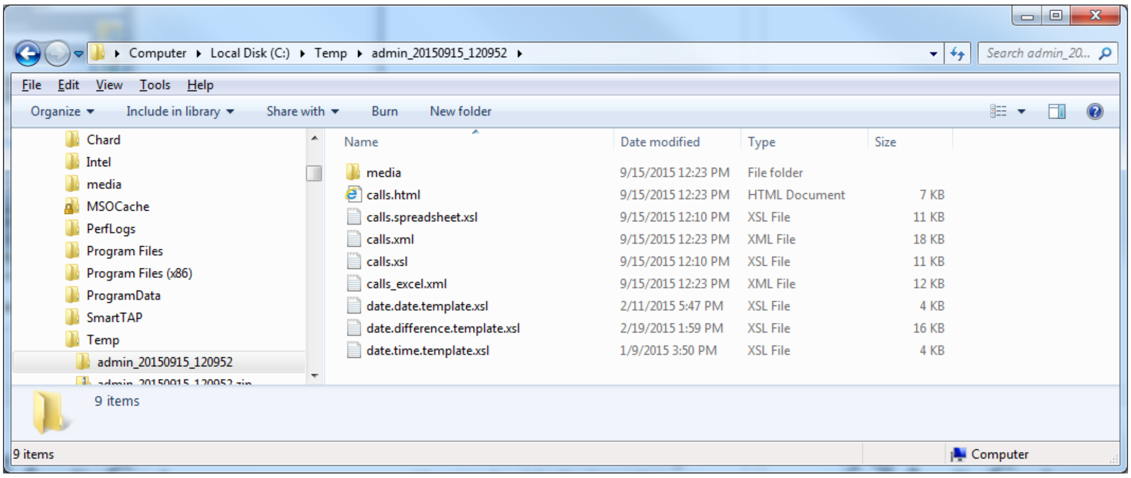


Computer ▸ Local Disk (C:) ▸ Temp ▸
Search Temp
File Edit View Tools Help
Organize ▾ Open Include in library ▾ Share with ▾ Burn New folder
Local Disk (C:)
Chard
Intel
media
MSOCache
PerfLogs
Program Files
Program Files (x86)
ProgramData
SmartTAP
Temp
admin_20150915_120952
admin_20150915_120952 Date modified: 9/15/2015 12:23 PM
File folder
1 item selected
Computer

Name	Date modified	Type	Size
admin_20150915_120952	9/15/2015 12:23 PM	File folder	
admin_20150915_120952.zip	9/15/2015 12:23 PM	Compressed (zipp...	32,681 KB

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

Figure 9-7: Contents of Folder



Computer ▸ Local Disk (C:) ▸ Temp ▸ admin_20150915_120952 ▸
Search admin_20...
File Edit View Tools Help
Organize ▾ Include in library ▾ Share with ▾ Burn New folder
Chard
Intel
media
MSOCache
PerfLogs
Program Files
Program Files (x86)
ProgramData
SmartTAP
Temp
admin_20150915_120952
admin_20150915_120952.zip
9 items
9 items
Computer

Name	Date modified	Type	Size
media	9/15/2015 12:23 PM	File folder	
calls.html	9/15/2015 12:23 PM	HTML Document	7 KB
calls.spreadsheet.xsl	9/15/2015 12:10 PM	XSL File	11 KB
calls.xml	9/15/2015 12:23 PM	XML File	18 KB
calls.xsl	9/15/2015 12:10 PM	XSL File	11 KB
calls_excel.xml	9/15/2015 12:23 PM	XML File	12 KB
date.date.template.xsl	2/11/2015 5:47 PM	XSL File	4 KB
date.difference.template.xsl	2/19/2015 1:59 PM	XSL File	16 KB
date.time.template.xsl	1/9/2015 3:50 PM	XSL File	4 KB

Calls.html: Call Manifest

Calls.xml: Call Meta Data exported from SmartTAP 360° loaded with Calls.html

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

10 API Integration

The SmartTAP 360° API is a RESTful Web Services API that provides complete access to and control over the SmartTAP 360° 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

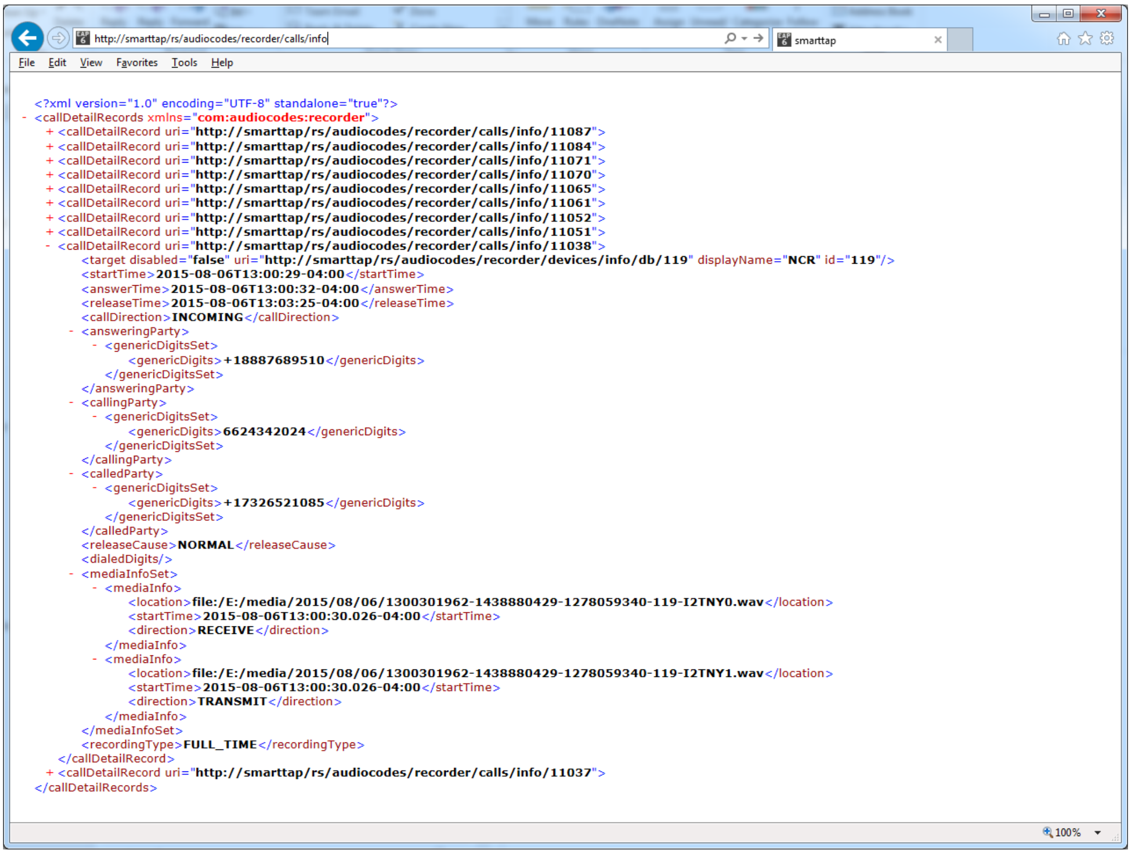
Change 'URL' to the IP address or the name of your SmartTAP 360° product.

http://SmartTAP 360°/rs/audiocodes/recorder - path to SmartTAP 360°

/calls - SmartTAP 360° Rest API resource

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

Figure 10-1: API Integration



```
  <?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <callDetailRecords xmlns="com:audiocodes:recorder">
  + <callDetailRecord uri="http://smarttap/rs/audiocodes/recorder/calls/info/11087">
  + <callDetailRecord uri="http://smarttap/rs/audiocodes/recorder/calls/info/11084">
  + <callDetailRecord uri="http://smarttap/rs/audiocodes/recorder/calls/info/11071">
  + <callDetailRecord uri="http://smarttap/rs/audiocodes/recorder/calls/info/11070">
  + <callDetailRecord uri="http://smarttap/rs/audiocodes/recorder/calls/info/11065">
  + <callDetailRecord uri="http://smarttap/rs/audiocodes/recorder/calls/info/11061">
  + <callDetailRecord uri="http://smarttap/rs/audiocodes/recorder/calls/info/11052">
  + <callDetailRecord uri="http://smarttap/rs/audiocodes/recorder/calls/info/11051">
  - <callDetailRecord uri="http://smarttap/rs/audiocodes/recorder/calls/info/11038">
        <target disabled="false" uri="http://smarttap/rs/audiocodes/recorder/devices/info/db/119" displayName="NCR" id="119"/>
        <startTime>2015-08-06T13:00:29-04:00</startTime>
        <answerTime>2015-08-06T13:00:32-04:00</answerTime>
        <releaseTime>2015-08-06T13:03:25-04:00</releaseTime>
        <callDirection>INCOMING</callDirection>
      - <answeringParty>
          - <genericDigitsSet>
                <genericDigits>+18887689510</genericDigits>
            </genericDigitsSet>
        </answeringParty>
      - <callingParty>
          - <genericDigitsSet>
                <genericDigits>6624342024</genericDigits>
            </genericDigitsSet>
        </callingParty>
      - <calledParty>
          - <genericDigitsSet>
                <genericDigits>+17326521085</genericDigits>
            </genericDigitsSet>
        </calledParty>
        <releaseCause>NORMAL</releaseCause>
        <dialedDigits/>
      - <mediaInfoSet>
          - <mediaInfo>
                <location>file:/E:/media/2015/08/06/1300301962-1438880429-1278059340-119-I2TNY0.wav</location>
                <startTime>2015-08-06T13:00:30.026-04:00</startTime>
                <direction>RECEIVE</direction>
            </mediaInfo>
          - <mediaInfo>
                <location>file:/E:/media/2015/08/06/1300301962-1438880429-1278059340-119-I2TNY1.wav</location>
                <startTime>2015-08-06T13:00:30.026-04:00</startTime>
                <direction>TRANSMIT</direction>
            </mediaInfo>
        </mediaInfoSet>
        <recordingType>FULL_TIME</recordingType>
    </callDetailRecord>
  + <callDetailRecord uri="http://smarttap/rs/audiocodes/recorder/calls/info/11037">
  </callDetailRecords>
```

To learn more about the SmartTAP 360° REST API, see the HTML documentation included with the SmartTAP 360° software distribution.

11 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:

- recording_report_YEAR-Month-Day.txt – general report of all targeted users and calls in text format.
- recording_summary_report_YEAR-Month-Day.csv - general report of all targeted users and calls in CSV format (Excel).
- 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).

⚠ Scanning of Microsoft Azure Blob storage for validation of the recording in storage is not yet supported.

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 360° server as a part of the SmartTAP 360° 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”.

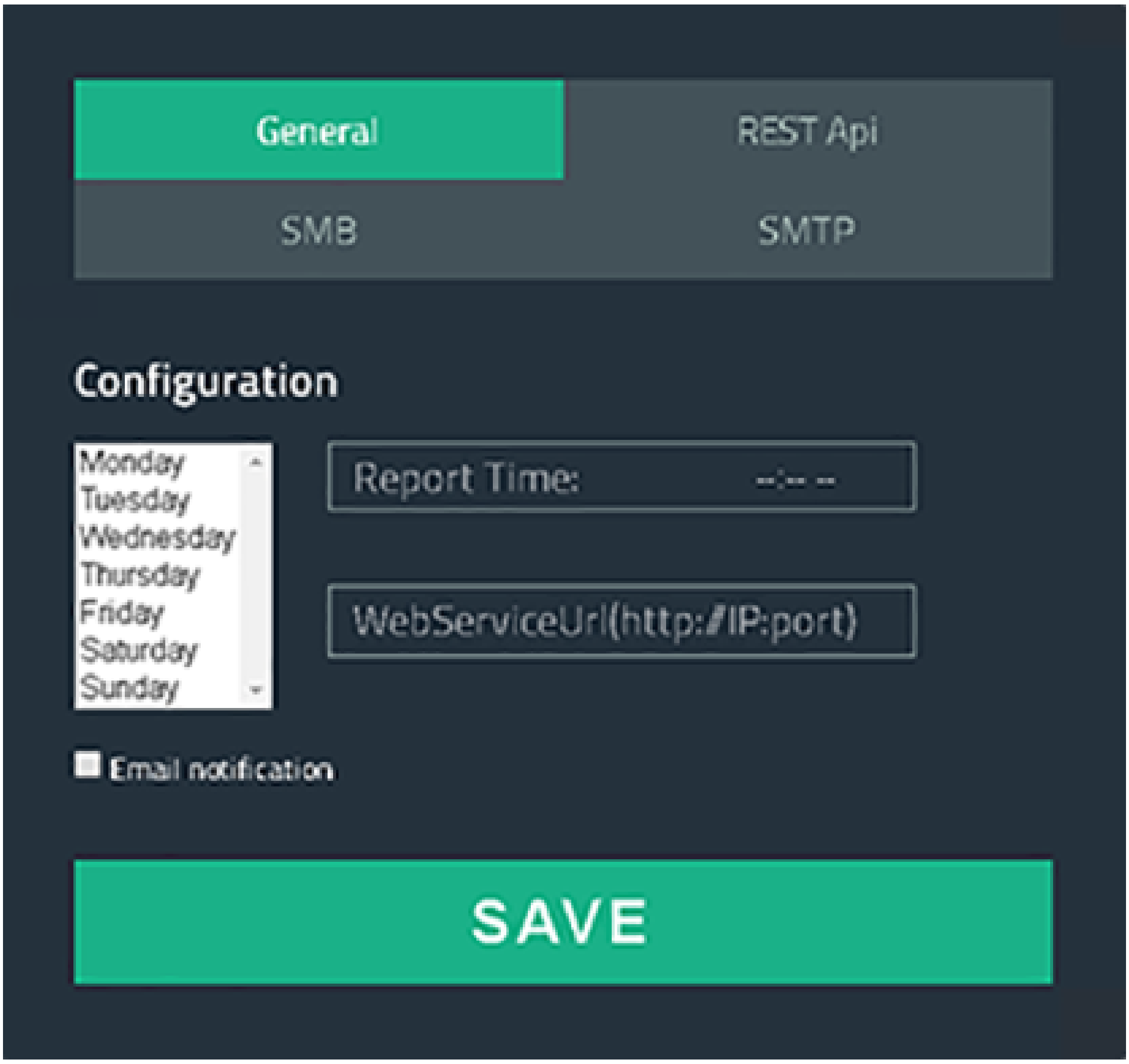
For configuring the health monitor, see the following:

- General Configuration below
- REST API Configuration on page 227
- SMB Configuration on page 227

General Configuration

This section describes the general configuration for Recording Health Monitor utility.

Figure 11-1: 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>
```

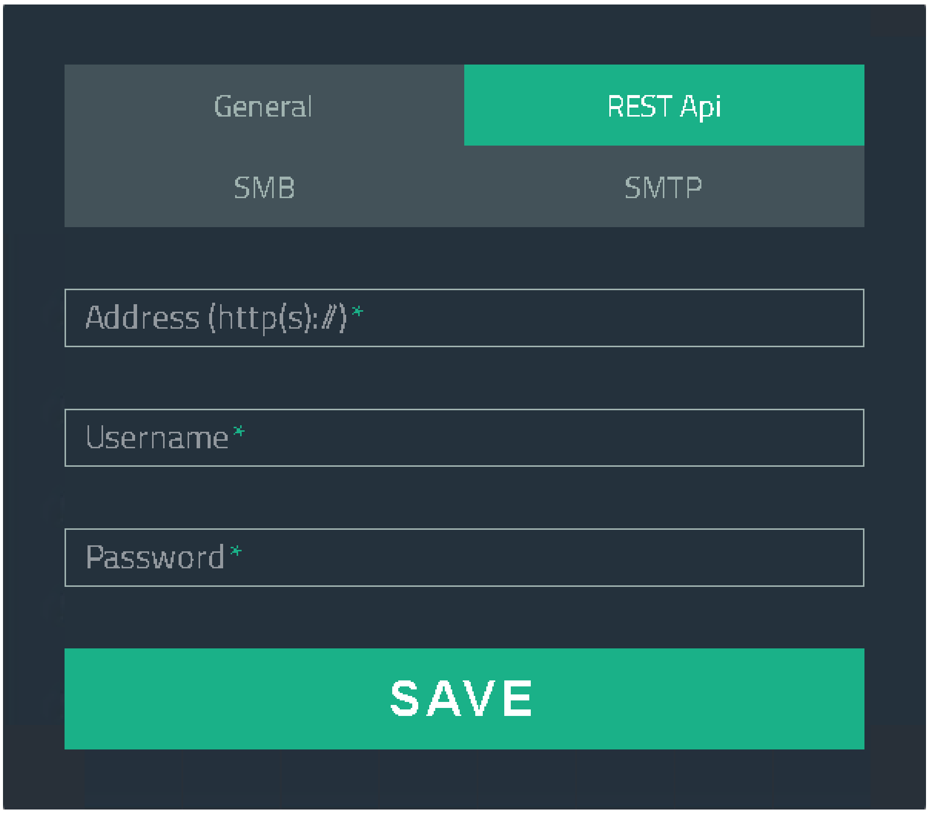
- **WebServiceUrl:** Health Monitor Web Service configuration page. Default: http://localhost:10101.
- **Email notification:** enables email notification option. HM sends an email with attached daily reports on a scheduled time. SMTP configuration is required if this

option is enabled. For more details see Configuring Email Server Settings on page 62 Default: Disabled.

REST API Configuration

This section describes the REST API configuration for the Recording Health Monitor.

Figure 11-2: 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).

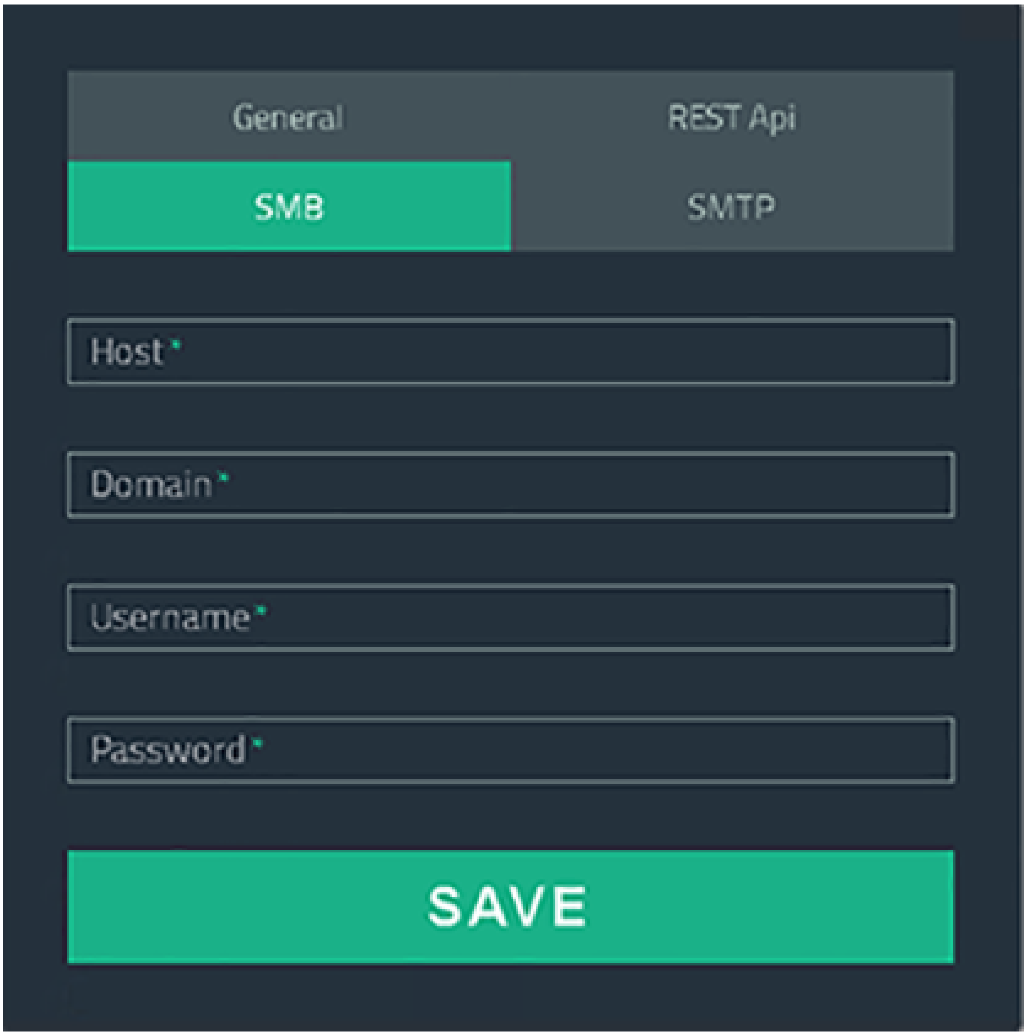
In case the Application server is configured for HTTPS only, the Address field should be changed to https://FQDN of Application Server, where FQDN should be the same as in the certificate that was issued for the Application Server. This is necessary for authentication purposes.

SMB Configuration

This section describes the SMB configuration for the Recording Health Monitor.

SMB – network media files location:

Figure 11-3: SMB Configuration

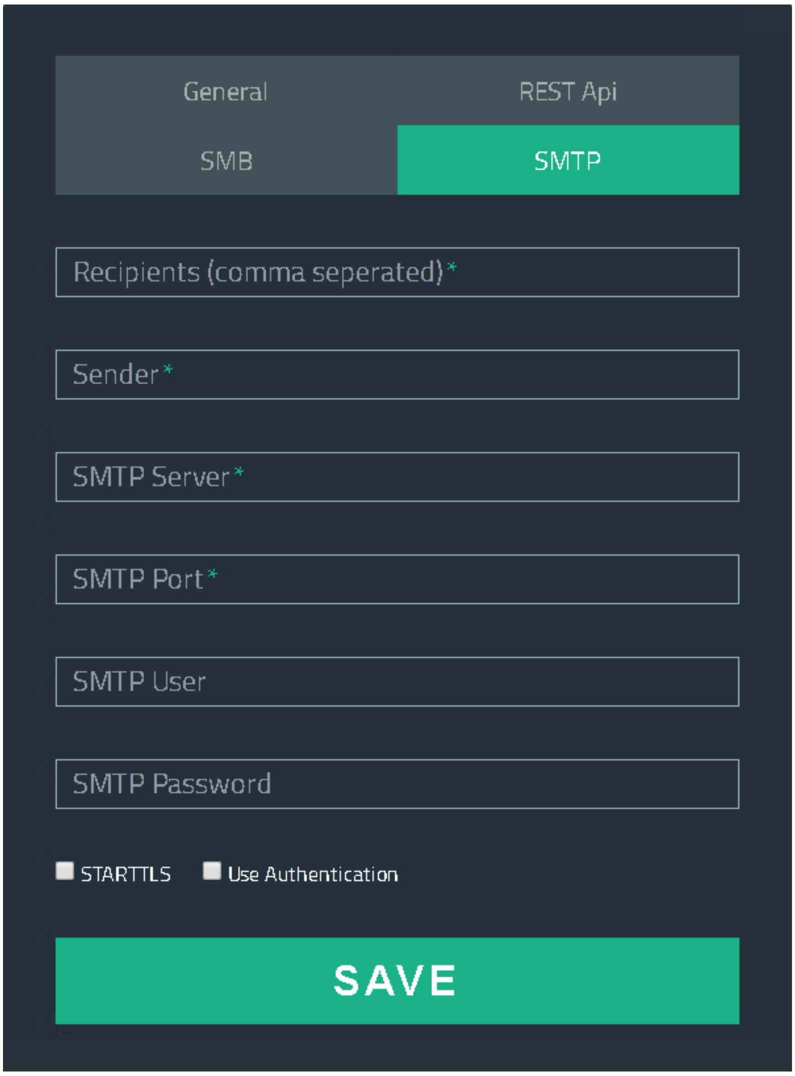


In case SmartTAP 360° uses a network location for media storage, this configuration must be updated with the following parameters:

- 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 11-4: SMTP Configuration



The following parameters can be configured in this screen:

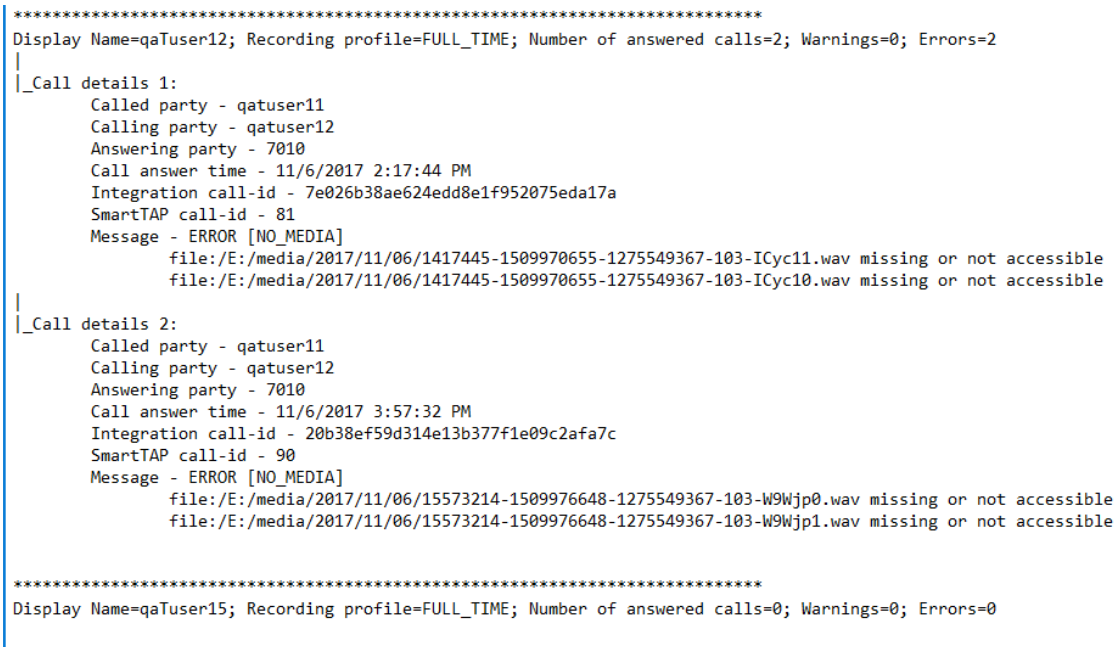
- Recipients – mail notification recipient list. Comma separated format for multiple recipients.
- Sender – mail notification initiator address. All reports will be sent from this mail address.
- SMTP Server – mail server address (IP, FQDN).
- SMTP Port – mail server port.
- SMTP User – mail server user.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

Report Formats

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

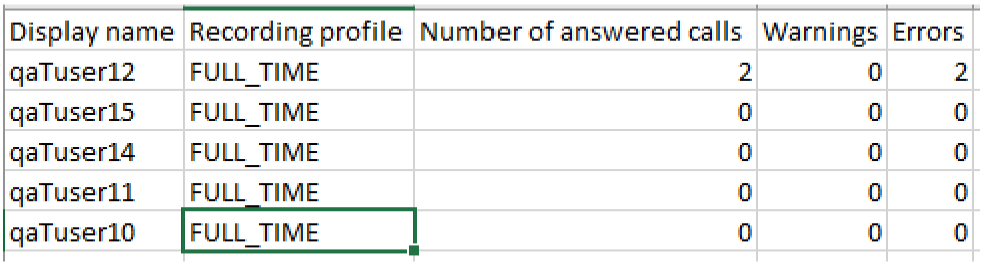
- Display name – display name of targeted user
- Recording profile – assigned call recording type
- Number of answered calls – total number of answered calls
- Warnings – number of warnings
- Errors – number of errors

Figure 11-5: Example 1: recording_report_YEAR-Month-Day.txt



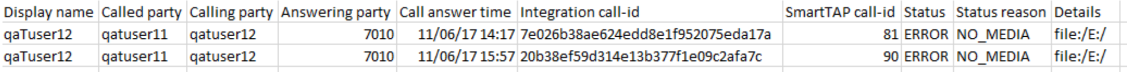
```
*****************************************************************************
Display Name=qaTuser12; Recording profile=FULL_TIME; Number of answered calls=2; Warnings=0; Errors=2
|
|_Call details 1:
        Called party - qatuser11
        Calling party - qatuser12
        Answering party - 7010
        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 11-6: Example 2: recording_summary_report_YEAR-Month-Day.csv:



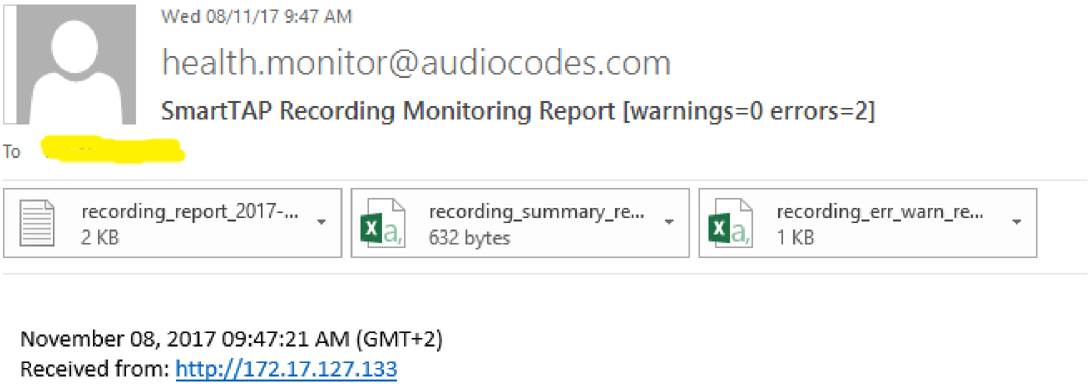
Display name	Recording profile	Number of answered calls	Warnings	Errors
qaTuser12	FULL_TIME	2	0	2
qaTuser15	FULL_TIME	0	0	0
qaTuser14	FULL_TIME	0	0	0
qaTuser11	FULL_TIME	0	0	0
qaTuser10	FULL_TIME	0	0	0

Figure 11-7: 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 11-8: Email Format:



Wed 08/11/17 9:47 AM

health.monitor@audiocodes.com

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

To [redacted]

November 08, 2017 09:47:21 AM (GMT+2)
Received from: http://172.17.127.133

12 Announcement Server (Skype for Business)

SmartTAP 360° 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 360° 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 in the Recording Profile (see Managing Recording Profiles on page 112 and Announcement Server - Example Configurations). For installing and setting up the Announcement server,

> ⚠ SmartTAP 360° 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.

This section includes the following:

- Simple Annoucement below
- IVR on the next page
- Example Annoucement Server Scenarios on page 237
- Annoucement Server Configuration Parameters on page 239
- Announcement Server - Example Configurations

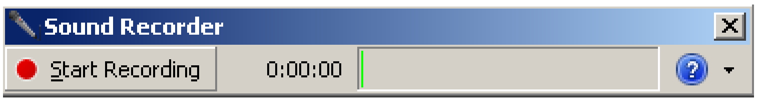
Simple Annoucement

SmartTAP 360° can be configured to play announcements to the calling party and if required called parties on a call with a targeted user. 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 12-1: Sound Recorder

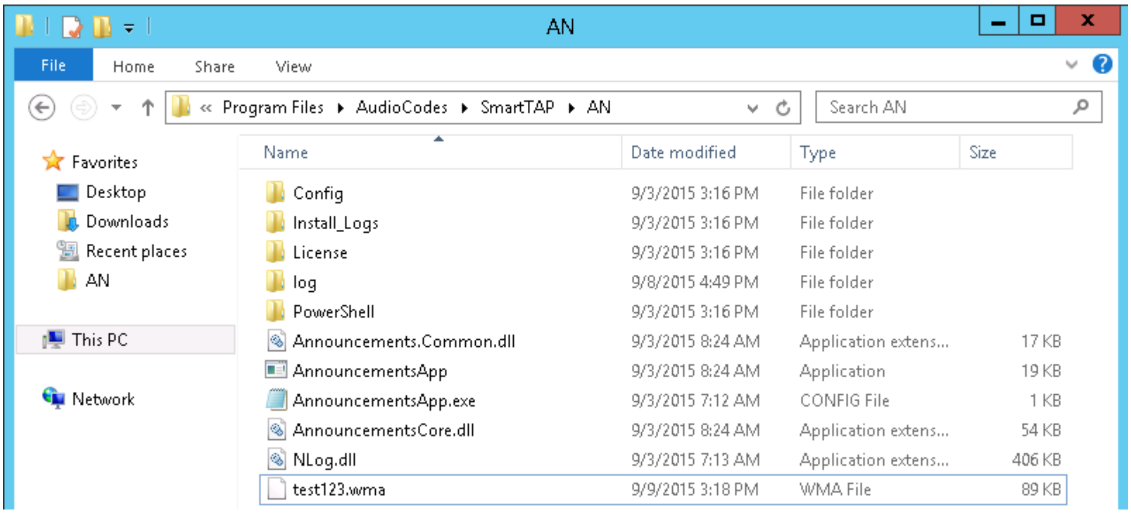


Example: "Thank you for calling Company A, your call may be recorded for quality assurance".

2. When done, click Stop Recording and it will prompt for the new file destination.
3. Save the file to the following location:
Program Files\AudioCodes\SmartTAP 360°\AN\Config\StateMachineConfig

Ensure that you save the file in WMA format.

Figure 12-2: Annoucement Server



Name	Date modified	Type	Size
Config	9/3/2015 3:16 PM	File folder	
Install_Logs	9/3/2015 3:16 PM	File folder	
License	9/3/2015 3:16 PM	File folder	
log	9/8/2015 4:49 PM	File folder	
PowerShell	9/3/2015 3:16 PM	File folder	
Announcements.Common.dll	9/3/2015 8:24 AM	Application extens...	17 KB
AnnouncementsApp	9/3/2015 8:24 AM	Application	19 KB
AnnouncementsApp.exe	9/3/2015 7:12 AM	CONFIG File	1 KB
AnnouncementsCore.dll	9/3/2015 8:24 AM	Application extens...	54 KB
NLog.dll	9/3/2015 7:13 AM	Application extens...	406 KB
test123.wma	9/9/2015 3:18 PM	WMA File	89 KB

IVR

SmartTAP 360° 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 (see Enabling Text-to-Speech Platform on the next page)
- Enable Consent to record calls (see Consent to Record Calls on page 235)

For details on configuring IVR files, see Section Configuring IVR Script Files below. Once configured, the IVR files can be loaded to the user's Recording Profile (see Managing Recording Profiles on page 112).

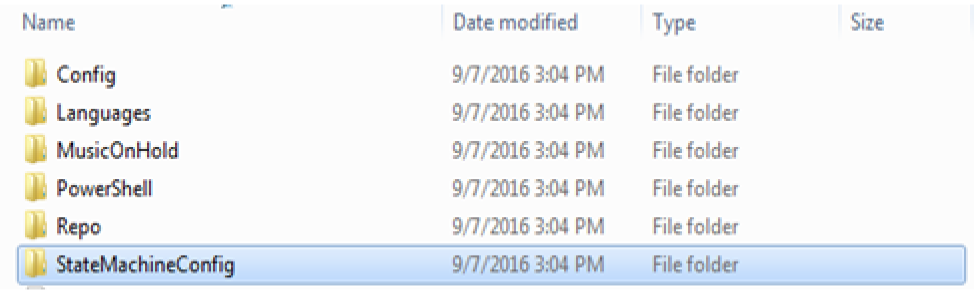
Configuring IVR Script Files

The IVR files are located as follows:

- The prompt media files are located under ...\Program Files\AudioCodes\SmartTAP 360°\AN\Languages. USA English media files are under en-us folder.
- The IVR state machines are located under Program Files\AudioCodes\SmartTAP 360°\AN\Config\StateMachineConfig

IVR scripts files must be saved in JSON format to the StateMachineConfig file in order to be configured in the Recording Profile (see Managing Recording Profiles on page 112).

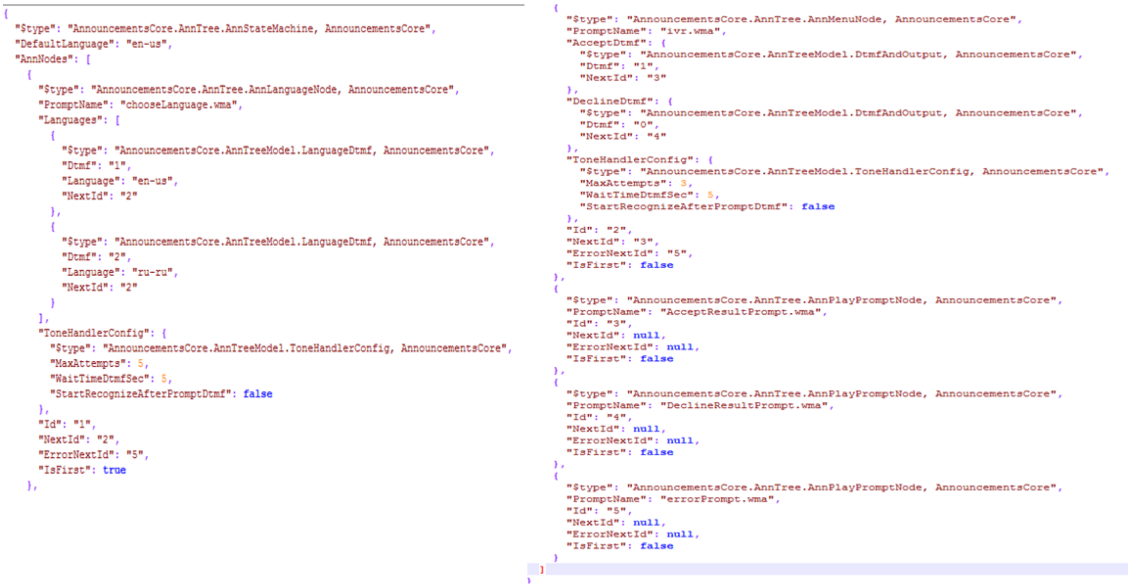
- The IVR sample state machines are located under Program Files\AudioCodes\SmartTAP 360°\AN\Config\Repo



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. The following shows example IVR file :

Figure 12-3: Example IVR Script File



```
{
  "$type": "AnnouncementsCore.AnnTree.AnnStateMachine, AnnouncementsCore",
  "DefaultLanguage": "en-us",
  "AnnNodes": [
    {
      "$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
    }
  ]
}
```

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. This section describes how to setup to use the TTS method.

➢ **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.

- It is not recommended to install Speech Recognition (SR) files because currently AN doesn't support speech recognition. This feature may be supported in the future. If you install SR files, this files will not be used and AN behavior is not affected.
- Install platform and language from the same Version 11. A combination of Versions 10 and 11 is invalid.

4. To enable TTS copy over and if required modify state machine(s) from the folder ending with tts in ...\Program Files\AudioCodes\SmartTAP 360°\AN\Repo to the Program Files\AudioCodes\SmartTAP 360°\AN\StateMachineConfig folder.

Consent to Record Calls

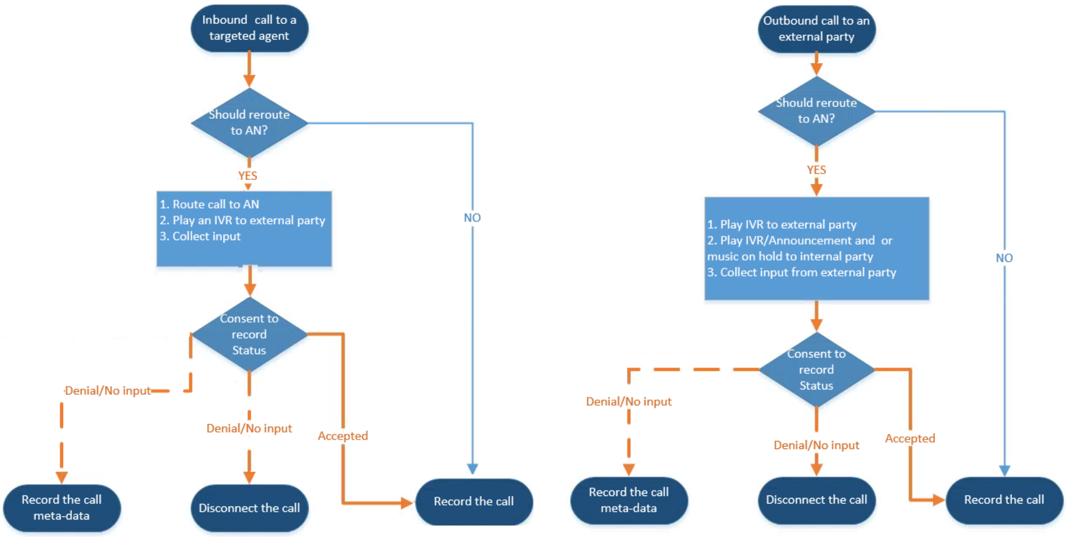
SmartTAP 360° supports interactive voice response (IVR) announcements requesting consent from the call party to record the conversation of the call. If the call party does not consent, the conversation is not recorded. Below is an example of a call consent prompt:

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

The Demo IVR files provided by SmartTAP 360°, by default, disable call consent.

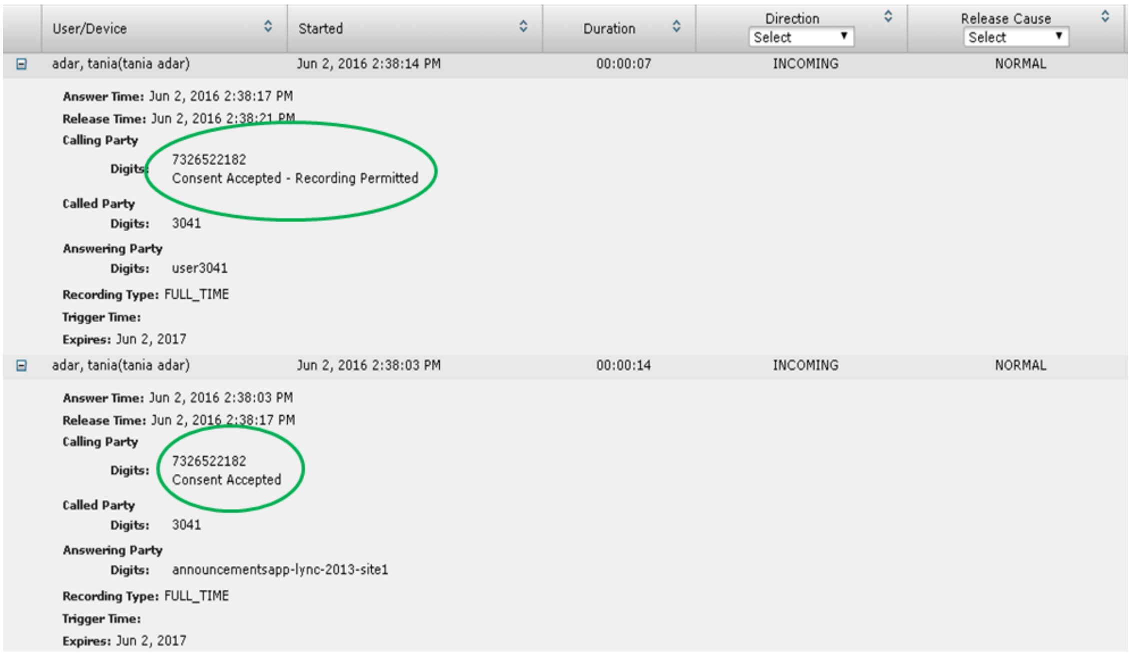
The following figure illustrates the Call Consent process for Inbound and Outbound calls:

Figure 12-4: IVR Announcements



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

Figure 12-5: Consent Accepted



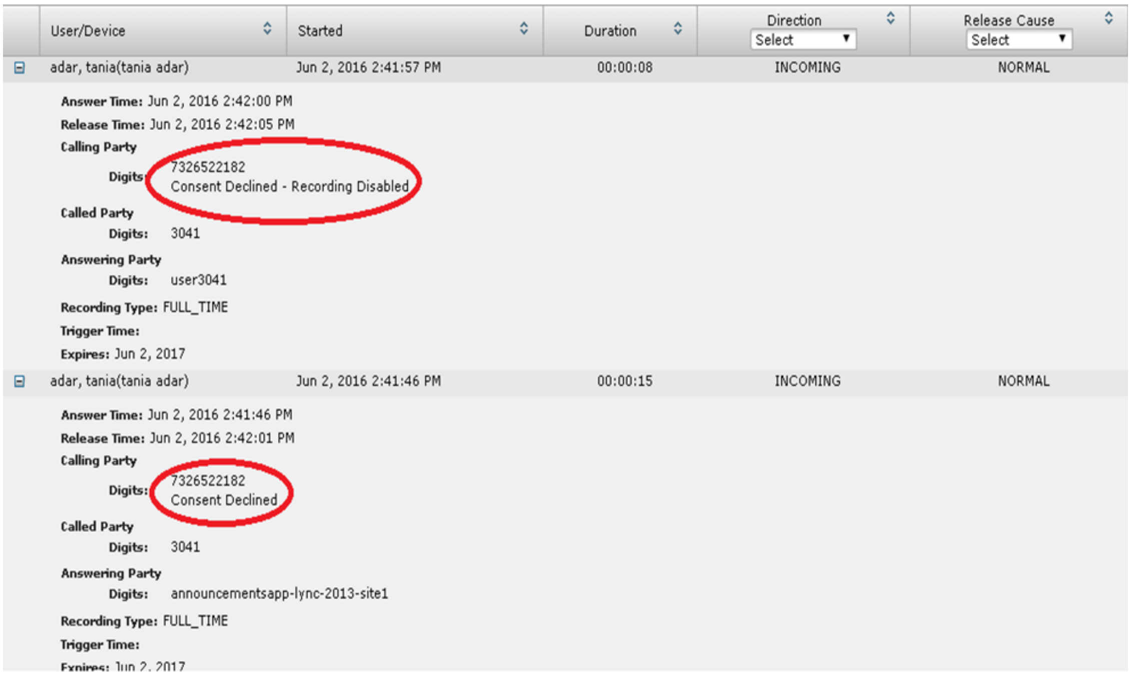
	User/Device	Started	Duration	Direction Select ▼	Release Cause Select ▼
⊟	adar, tania(tania adar)	Jun 2, 2016 2:38:14 PM	00:00:07	INCOMING	NORMAL

Answer Time: Jun 2, 2016 2:38:17 PM
Release Time: Jun 2, 2016 2:38:21 PM
Calling Party
Digits: 7326522182
Consent Accepted - Recording Permitted
Called Party
Digits: 3041
Answering Party
Digits: user3041
Recording Type: FULL_TIME
Trigger Time:
Expires: Jun 2, 2017

⊟	adar, tania(tania adar)	Jun 2, 2016 2:38:03 PM	00:00:14	INCOMING	NORMAL

Answer Time: Jun 2, 2016 2:38:03 PM
Release Time: Jun 2, 2016 2:38:17 PM
Calling Party
Digits: 7326522182
Consent Accepted
Called Party
Digits: 3041
Answering Party
Digits: announcementsapp-lync-2013-site1
Recording Type: FULL_TIME
Trigger Time:
Expires: Jun 2, 2017

Figure 12-6: Consent Declined



	User/Device	Started	Duration	Direction Select ▼	Release Cause Select ▼
⊟	adar, tania(tania adar)	Jun 2, 2016 2:41:57 PM	00:00:08	INCOMING	NORMAL

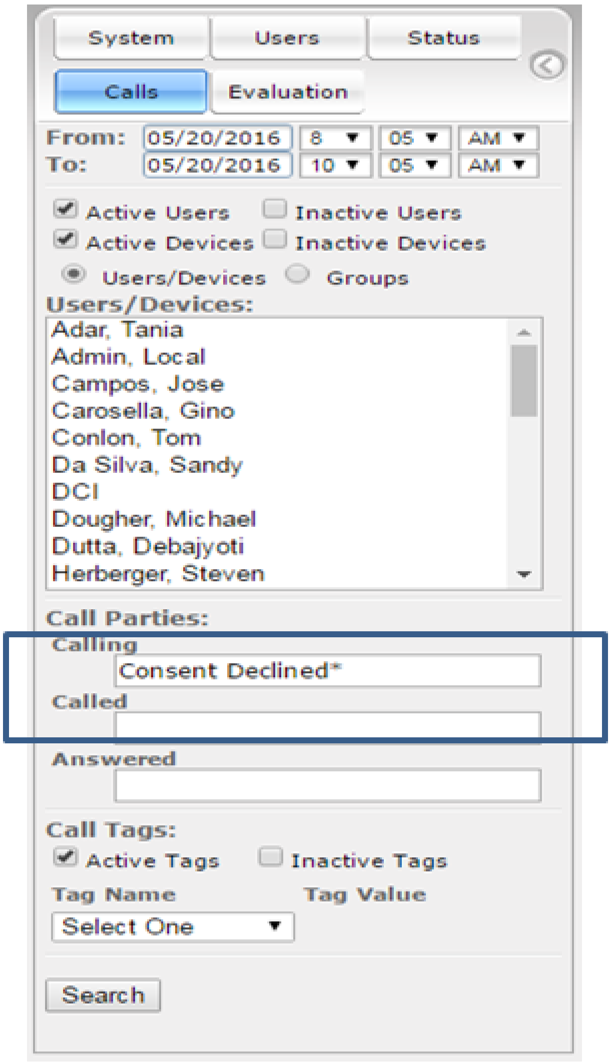
Answer Time: Jun 2, 2016 2:42:00 PM
Release Time: Jun 2, 2016 2:42:05 PM
Calling Party
Digits: 7326522182
Consent Declined - Recording Disabled
Called Party
Digits: 3041
Answering Party
Digits: user3041
Recording Type: FULL_TIME
Trigger Time:
Expires: Jun 2, 2017

⊟	adar, tania(tania adar)	Jun 2, 2016 2:41:46 PM	00:00:15	INCOMING	NORMAL

Answer Time: Jun 2, 2016 2:41:46 PM
Release Time: Jun 2, 2016 2:42:01 PM
Calling Party
Digits: 7326522182
Consent Declined
Called Party
Digits: 3041
Answering Party
Digits: announcementsapp-lync-2013-site1
Recording Type: FULL_TIME
Trigger Time:
Expires: Jun 2, 2017

Search calls based on the consent as shown below:

Figure 12-7: Call Parties



From: 05/20/2016 8 05 AM

To: 05/20/2016 10 05 AM

☑ Active Users ☐ Inactive Users

☑ Active Devices ☐ Inactive Devices

● Users/Devices ○ Groups

Users/Devices:

Adar, Tania
Admin, Local
Campos, Jose
Carosella, Gino
Conlon, Tom
Da Silva, Sandy
DCI
Dougher, Michael
Dutta, Debajyoti
Herberger, Steven

Call Parties:

Calling

Consent Declined*

Called

Answered

Call Tags:

☑ Active Tags ☐ Inactive Tags

Tag Name Tag Value

Select One

Example Annoucement Server Scenarios

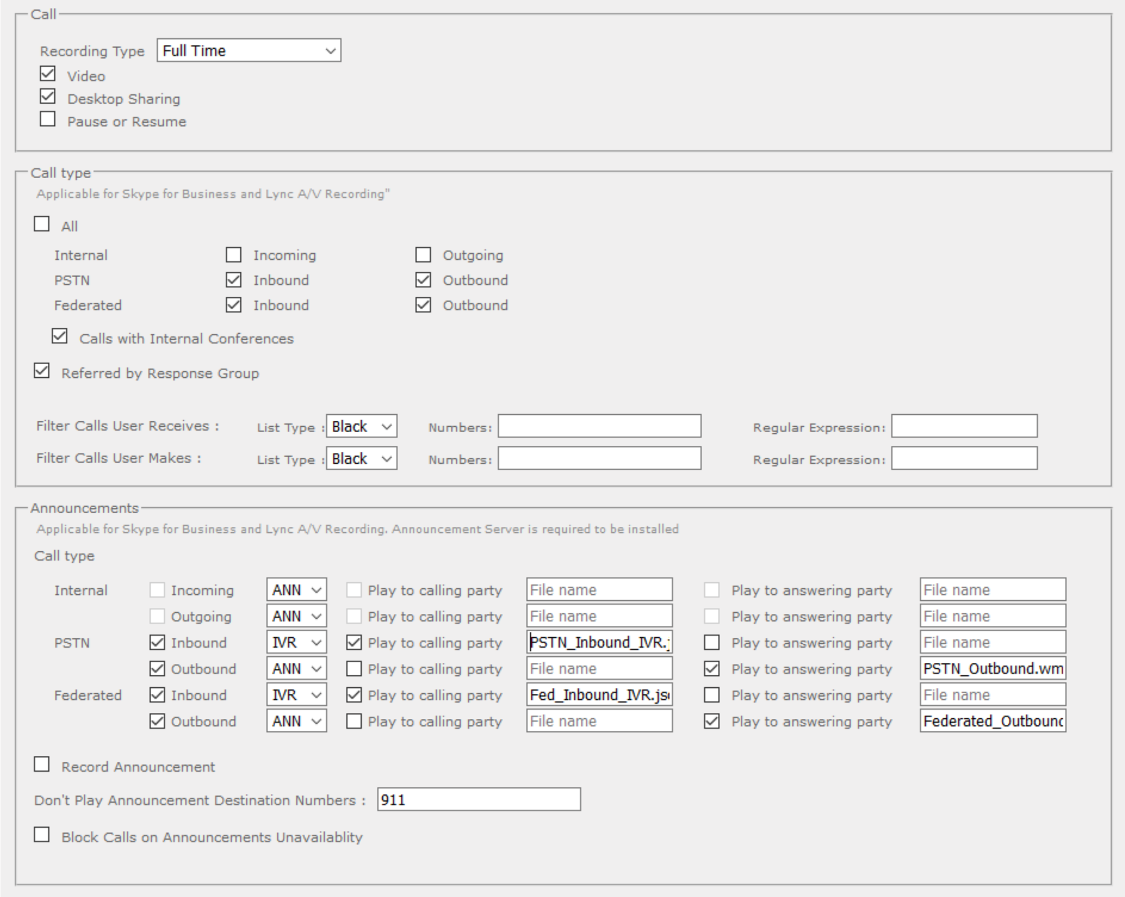
This section describes the following example scenarios for assigning Media files and IVR script files for the Annoucement server using the Recording Profile (:

- PSTN and Federated Calls below
- All Inbound Calls on the next page

PSTN and Federated Calls

The figure below shows the attaching of announcement audio files for Federated and PSTN calls. An IVR file is configured to play to the Calling party for Inbound PSTN and Federated calls. Likewise, an ANN file is configured to play to the Answering party for Outbound PSTN and Federated calls.

Figure 12-8: PSTN and Federated Calls



Call

Recording Type: Full Time

☑ Video

☑ Desktop Sharing

□ Pause or Resume

Call type

Applicable for Skype for Business and Lync A/V Recording"

□ All

Internal	□ Incoming	□ Outgoing
PSTN	☑ Inbound	☑ Outbound
Federated	☑ Inbound	☑ Outbound

☑ Calls with Internal Conferences

☑ Referred by Response Group

Filter Calls User Receives :	List Type : Black	Numbers:	Regular Expression:
Filter Calls User Makes :	List Type : Black	Numbers:	Regular Expression:

Announcements

Applicable for Skype for Business and Lync A/V Recording. Announcement Server is required to be installed

Call type

Internal	□ Incoming	ANN	□ Play to calling party	File name	□ Play to answering party	File name
	□ Outgoing	ANN	□ Play to calling party	File name	□ Play to answering party	File name
PSTN	☑ Inbound	IVR	☑ Play to calling party	PSTN_Inbound_IVR.:	□ Play to answering party	File name
	☑ Outbound	ANN	□ Play to calling party	File name	☑ Play to answering party	PSTN_Outbound.wm
Federated	☑ Inbound	IVR	☑ Play to calling party	Fed_Inbound_IVR.js	□ Play to answering party	File name
	☑ Outbound	ANN	□ Play to calling party	File name	☑ Play to answering party	Federated_Outbounc

□ Record Announcement

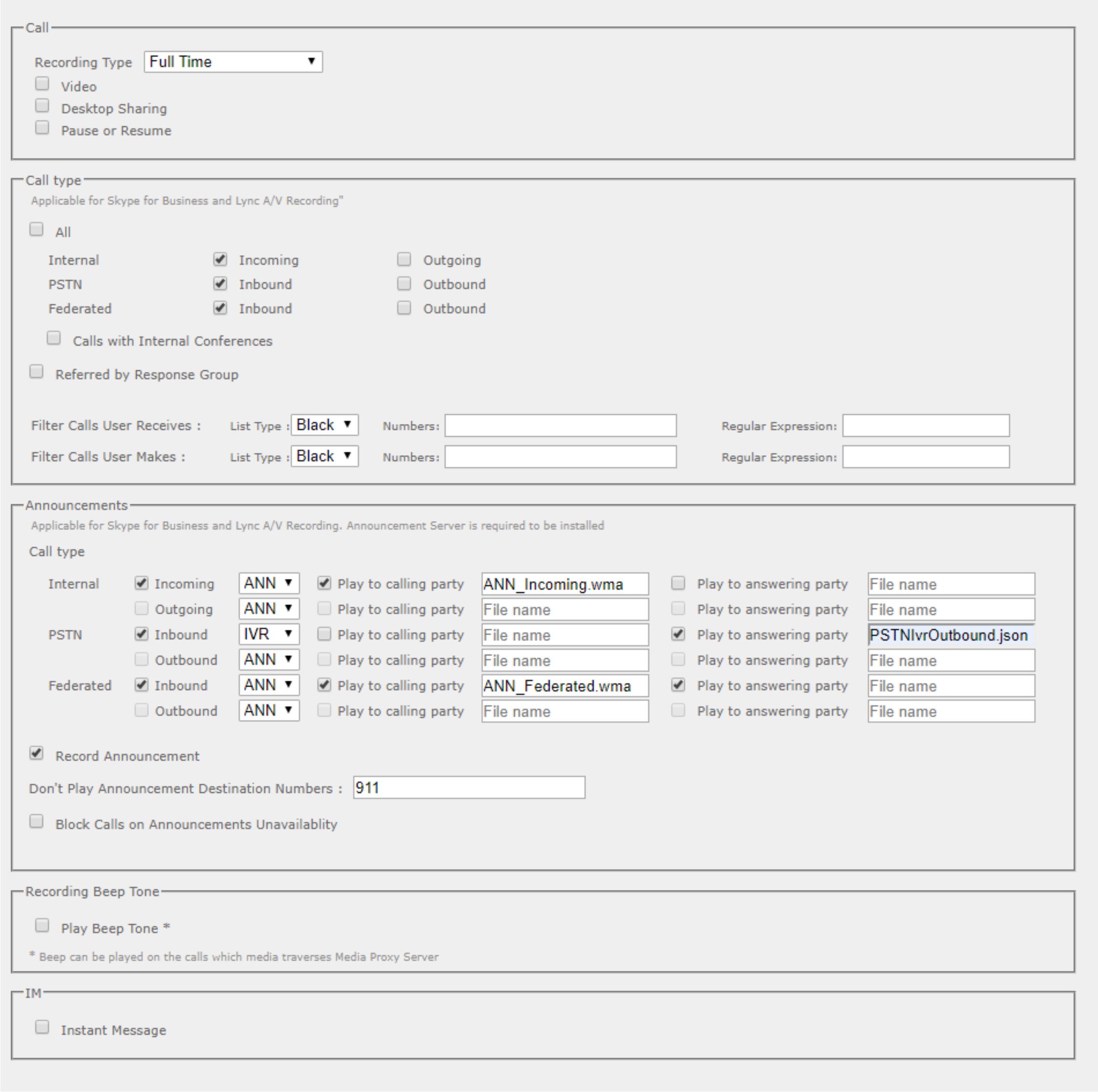
Don't Play Announcement Destination Numbers : 911

□ Block Calls on Announcements Unavailablity

All Inbound Calls

The figure below shows the configuration of announcement audio files for Incoming Internal calls and Inbound PSTN and Federated calls. An ANN file is configured to play to the Calling party for Incoming Internal calls and for Inbound Federated calls. Likewise, an IVR file is configured to play to the Answering party for Inbound PSTN calls.

Figure 12-9: Incoming Calls



Call

Recording Type: Full Time

□ Video

□ Desktop Sharing

□ Pause or Resume

Call type

Applicable for Skype for Business and Lync A/V Recording"

□ All

Internal	☑ Incoming	□ Outgoing
PSTN	☑ Inbound	□ Outbound
Federated	☑ Inbound	□ Outbound

□ Calls with Internal Conferences

□ Referred by Response Group

Filter Calls User Receives :	List Type : Black	Numbers:	Regular Expression:
Filter Calls User Makes :	List Type : Black	Numbers:	Regular Expression:

Announcements

Applicable for Skype for Business and Lync A/V Recording. Announcement Server is required to be installed

Call type

Internal	☑ Incoming	ANN	☑ Play to calling party	ANN_Incoming.wma	□ Play to answering party	File name
	□ Outgoing	ANN	□ Play to calling party	File name	□ Play to answering party	File name
PSTN	☑ Inbound	IVR	□ Play to calling party	File name	☑ Play to answering party	PSTNIvrOutbound.json
	□ Outbound	ANN	□ Play to calling party	File name	□ Play to answering party	File name
Federated	☑ Inbound	ANN	☑ Play to calling party	ANN_Federated.wma	☑ Play to answering party	File name
	□ Outbound	ANN	□ Play to calling party	File name	□ Play to answering party	File name

☑ Record Announcement

Don't Play Announcement Destination Numbers : 911

□ Block Calls on Announcements Unavailablity

Recording Beep Tone

□ Play Beep Tone *

* Beep can be played on the calls which media traverses Media Proxy Server

IM

□ Instant Message

Annoucement Server Configuration Parameters

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

Table 12-1: 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".

Parameter	Description
inviteDest	If the value is not empty, the application calls to this destination and ignores 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".
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}

Parameter	Description
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.
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".
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

Parameter	Description
	the SIP REFER is 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	Disables the alarms mechanism. Possible values: ■ True (disable) ■ False (default)
uaDontReceiveReferRegex	A regular expression (case insensitive). If the value of the UserAgent header matches the expression then the SIP REFER is not sent to that device when rerouting the call to the original destination. This solves the problem for Skype for Business clients when answering '488 not acceptable' on reception of SIP INVITE with replaces from the mobile clients. Default Value: "ucwa"

Parameter	Description
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 voice mail 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). For BothParties mode, redirect the caller if both sides don't support the 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 are used to identify voice mail 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 voice mail. Possible values: ■ True ■ False (default)

For AN Server installation instructions, refer to the *SmartTAP 360° Installation Guide*.

Annoucement Server Advanced Call Scenarios

- **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.

- **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 puts A on hold, B calls to C (this doesn't take place in blind transfer scenario) and B transfers A to C.

Table 12-2: 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 places 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 places 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. 2. B places 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 places 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 places 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	B + C	1. A calls B, B answers: announcement is played

Call Scenario	Targeted Users	Flow and expected results from AN (the second line is not applicable in case of blind transfer)
transfer		2. B places 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 places 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)

- **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 12-3: 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

- Conferences: Playing announcements on the calls of targeted users with a conference bridge are not currently supported. with SmartTAP 360° team the feature status if you need it.

- 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 re-initiated.

- 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.

13 Microsoft Azure Active Directory

This section describes how to setup Microsoft Azure Active Directory users and authentication:

- Azure Active Directory User Mapping below
- Azure Active Directory User Authentication on page 261

> Microsoft Azure Active Directory is only supported for Microsoft Teams recordings. Support in other integration platforms is not available in this release.

Azure Active Directory User Mapping

SmartTAP 360° Version 5.1 and later allows mapping of an Organizations' (Tenant) users from Microsoft Azure Active Directory (AAD). SmartTAP 360° uses the Client Credential Flow to authenticate itself and access hosted resources such as Users and Groups from Azure Active Directory.

> Refer to https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-client-creds-grant-flow.

The user mapping process involves the following steps:

- **Step 1:** Register an daemon client application in Azure Active Directory on behalf of SmartTAP 360° (see Step 1 Application Registration in Microsoft Azure below).
- **Step 2:** Configure API permission for this app in AAD (see Step 2 Configure API Permissions on page 250)
- **Step 3:** Configure Certificates & Secrets for this app in AAD (see Step 3 Configure Certificates & Secrets on page 267)
- **Step 4:** Configure this client application in SmartTAP 360° (see Step 4 Configure Azure Active Directory Client in SmartTAP 360° on page 255
- **Step 5:** Add new User Mappings in SmartTAP 360° (see Step 5 Add Azure Active Directory Mapping in SmartTAP 360° on page 256)

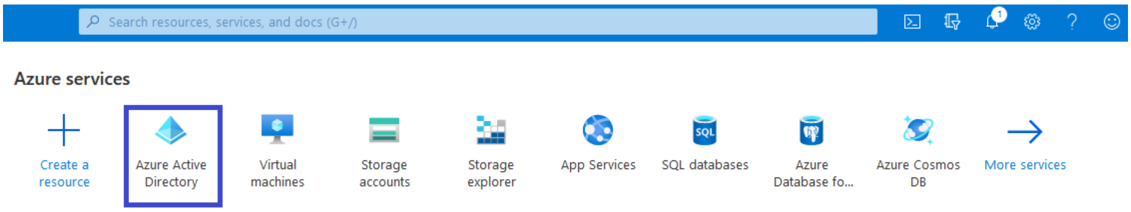
Step 1 Application Registration in Microsoft Azure

This step describes how to register an Application in Microsoft Azure.

➢ **Do the following:**

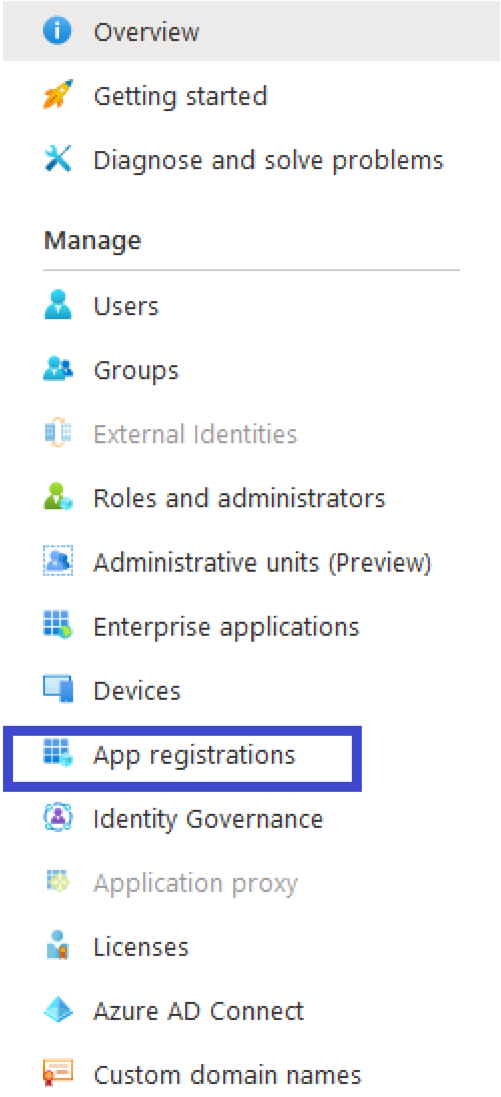
1. Login to the Microsoft Azure portal (https://portal.azure.com/).

Figure 13-1: Azure Services



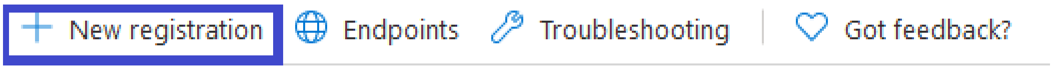
2. Click **Azure Active Directory**.

Figure 13-2: Application Registration



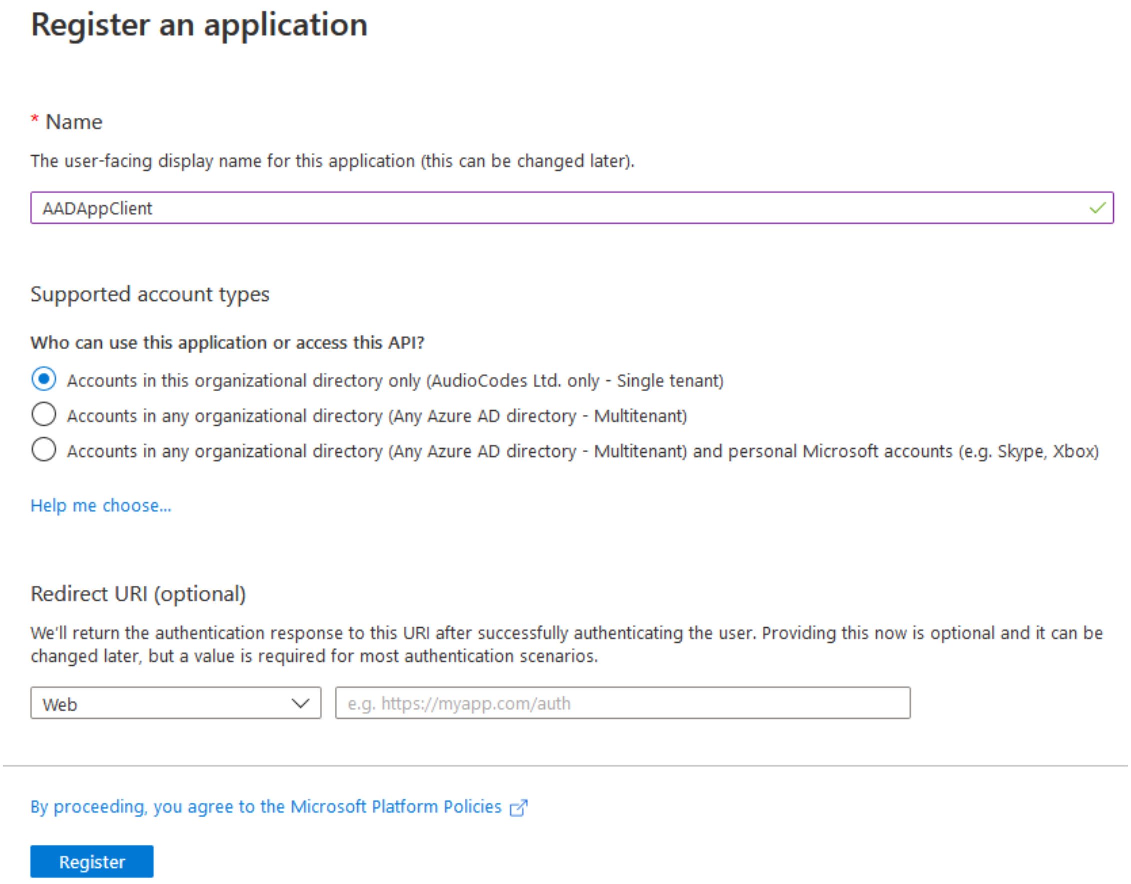
3. In the Navigation pane, select **Manage** > **App Registration**.

Figure 13-3: New Registration



4. Click **+ New Registration**. The Register an application page is displayed.

Figure 13-4: Sample Screens



Register an application

* Name

The user-facing display name for this application (this can be changed later).

AADAppClient ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (AudioCodes Ltd. only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | e.g. https://myapp.com/auth

By proceeding, you agree to the Microsoft Platform Policies

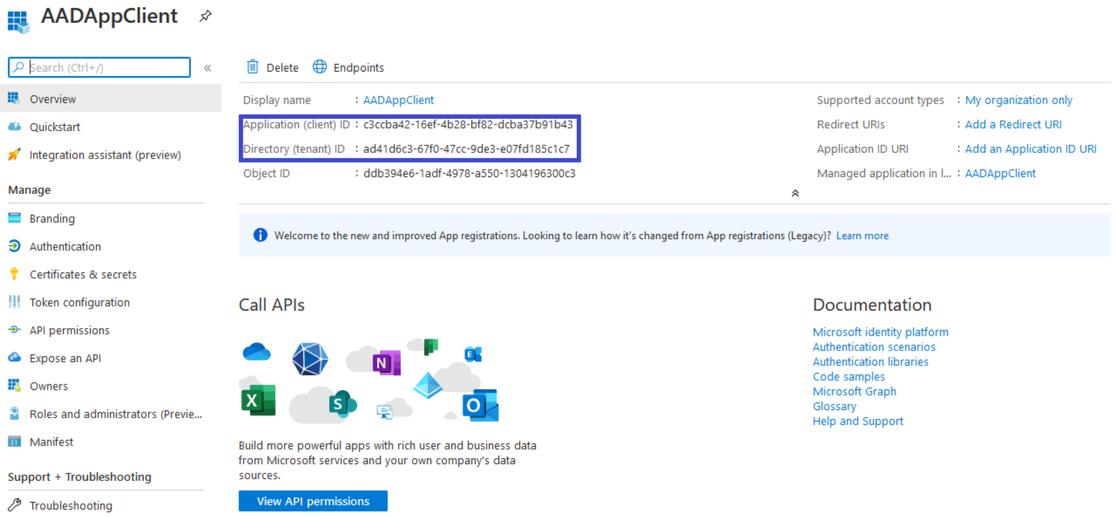
5. Enter the following details:

   - Name: enter a name for the client application
   - Supported account types: select the radio button for "Accounts in this organizational directory only (AudioCodes Ltd. only - Single tenant)"
   - Redirect URI (optional): no action required.

6. Click **Register** to confirm registration.

   Upon successful registration, the following details are displayed.

Figure 13-5: AADAppClient



AADAppClient

Display name : AADAppClient

Application (client) ID : c3ccba42-16ef-4b28-bf82-dcba37b91b43

Directory (tenant) ID : ad41d6c3-67f0-47cc-9de3-e07fd185c1c7

Object ID : ddb394e6-1adf-4978-a550-1304196300c3

Supported account types : My organization only

Redirect URIs : Add a Redirect URI

Application ID URI : Add an Application ID URI

Managed application in l... : AADAppClient

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

Documentation

7. Copy the value of Application (client) ID and Directory (tenant) ID for Client Configuration in SmartTAP 360° (Step 4 Configure Azure Active Directory Client in SmartTAP 360° on page 255).

Step 2 Configure API Permissions

This step describes the configuration of API permissions.

➢ Do the following:

1. Open the API Permissions screen (**Manage** > **API permissions**).

Figure 13-6: API Permissions

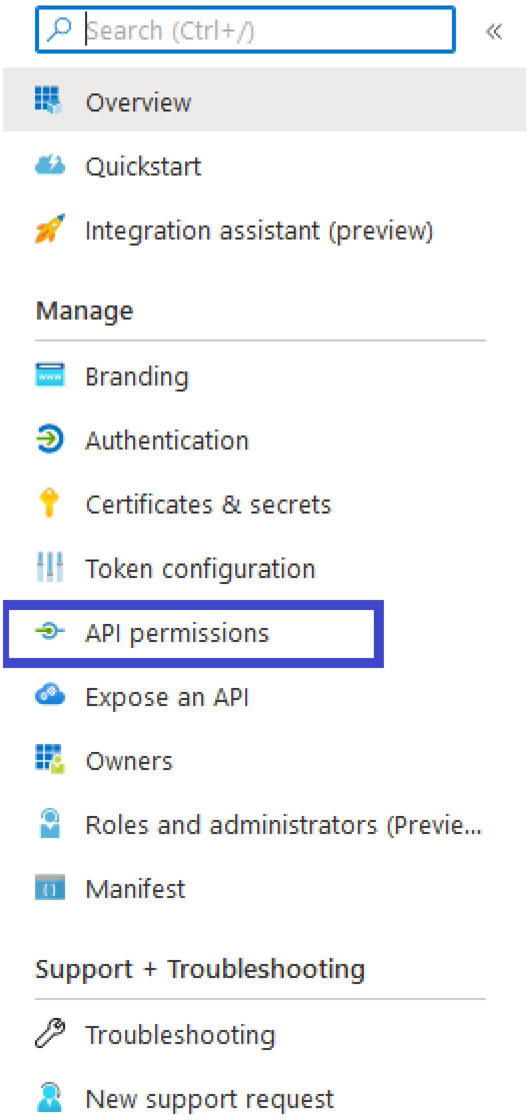
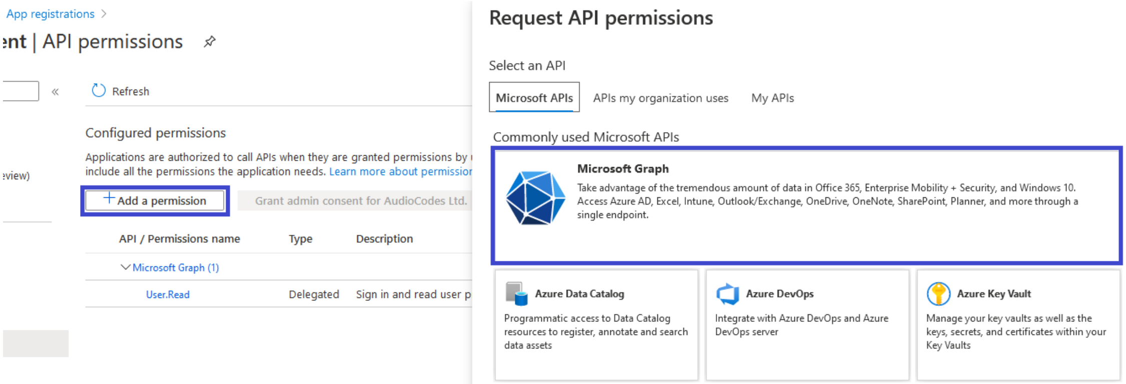


Figure 13-7: Add a Permission



Configured permissions

Applications are authorized to call APIs when they are granted permissions by u include all the permissions the application needs. Learn more about permissior

API / Permissions name	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user p

Select an API

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Data Catalog
Programmatic access to Data Catalog resources to register, annotate and search data assets

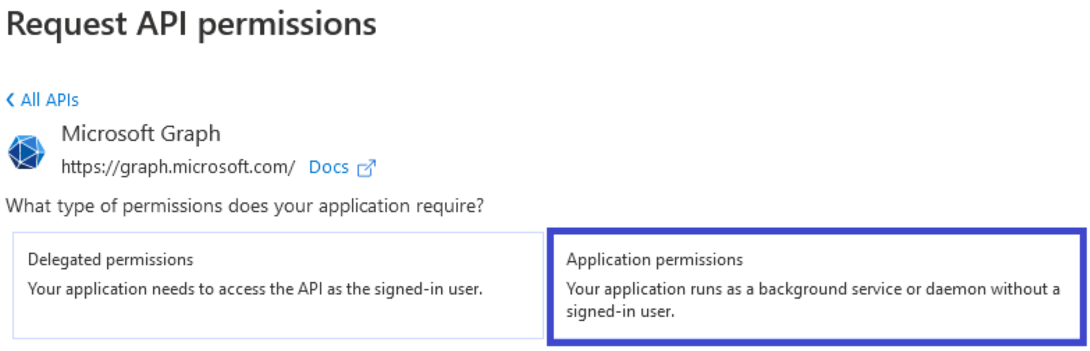
Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Key Vault
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

2. On right side panel, click **+ Add a permission** button and select "Microsoft Graph" link.

3. In the Request API permissions section, click the **Application permissions** link.

Figure 13-8: Request API Permissions



Request API permissions

❮ All APIs

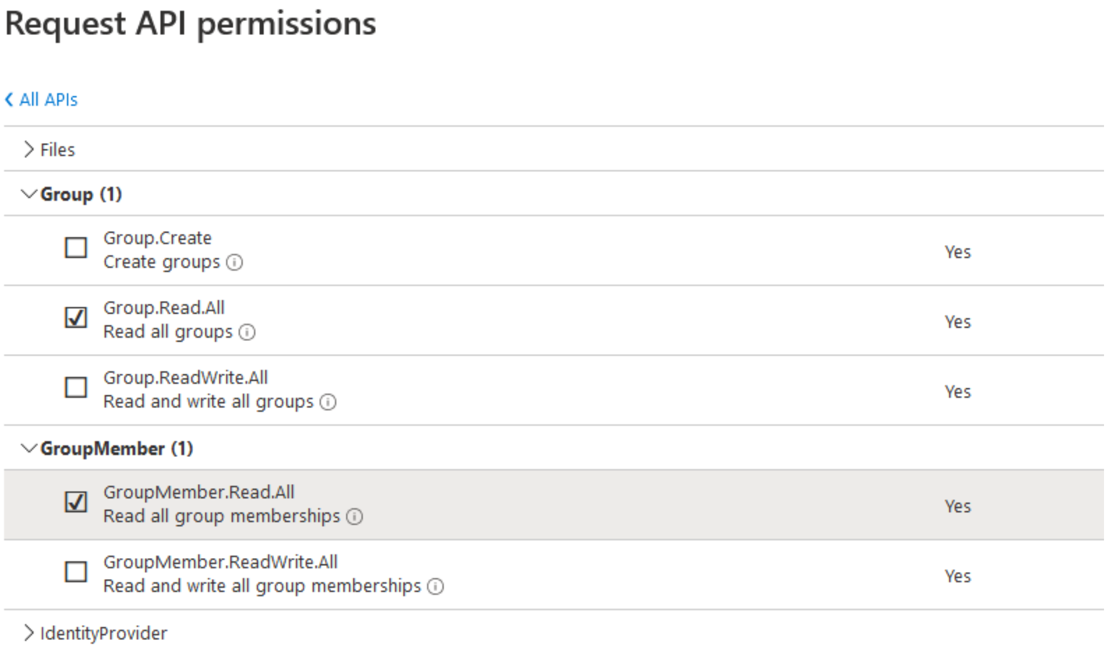
Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Figure 13-9: API Permission-Example 1



Request API permissions

❮ All APIs

> Files

∨ Group (1)

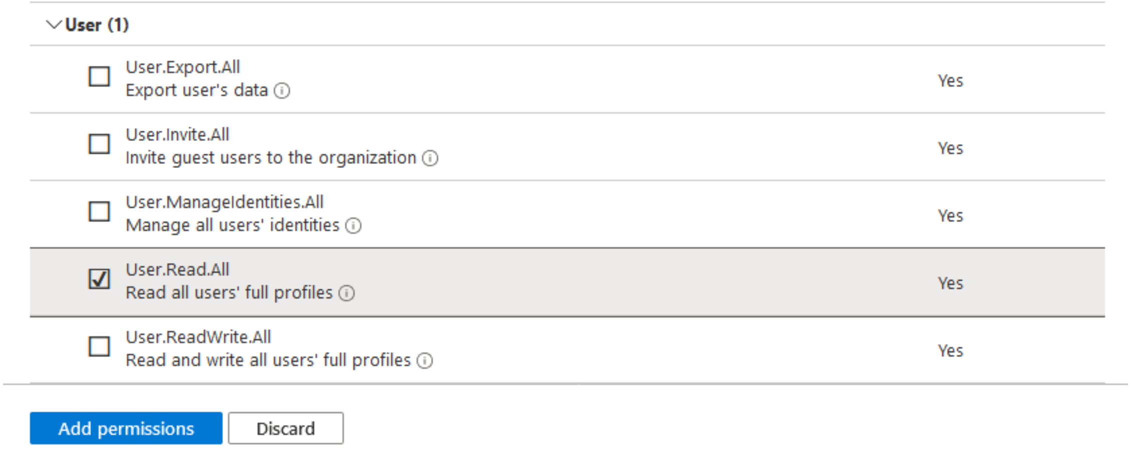
☐	Group.Create Create groups ⓘ	Yes
☑	Group.Read.All Read all groups ⓘ	Yes
☐	Group.ReadWrite.All Read and write all groups ⓘ	Yes

∨ GroupMember (1)

☑	GroupMember.Read.All Read all group memberships ⓘ	Yes
☐	GroupMember.ReadWrite.All Read and write all group memberships ⓘ	Yes

> IdentityProvider

Figure 13-10: API Permissions-Example 2



∨ User (1)

☐	User.Export.All Export user's data ⓘ	Yes
☐	User.Invite.All Invite guest users to the organization ⓘ	Yes
☐	User.ManageIdentities.All Manage all users' identities ⓘ	Yes
☑	User.Read.All Read all users' full profiles ⓘ	Yes
☐	User.ReadWrite.All Read and write all users' full profiles ⓘ	Yes

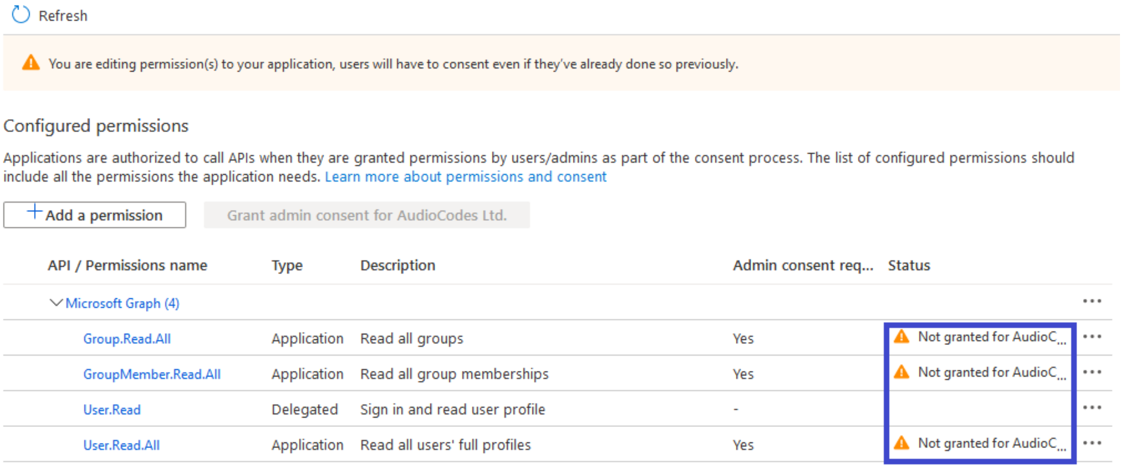
4. Under "Select permissions" list, check the following permissions:

- Group Permissions:

- Select Group.Read.All checkbox
- Group Members Permissions:
  - Select GroupMember.Read.All checkbox
- User Permissions:
  - Select User.Read.All checkbox
- Click **Add permissions**.

5. Under the "Configure permission" section, some of the permission require Admin Consent to be available for use (highlighted in the screen below). Contact the administrator to grant these permissions.

Figure 13-11: Configured Permissions



Refresh

⚠ You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Configured permissions

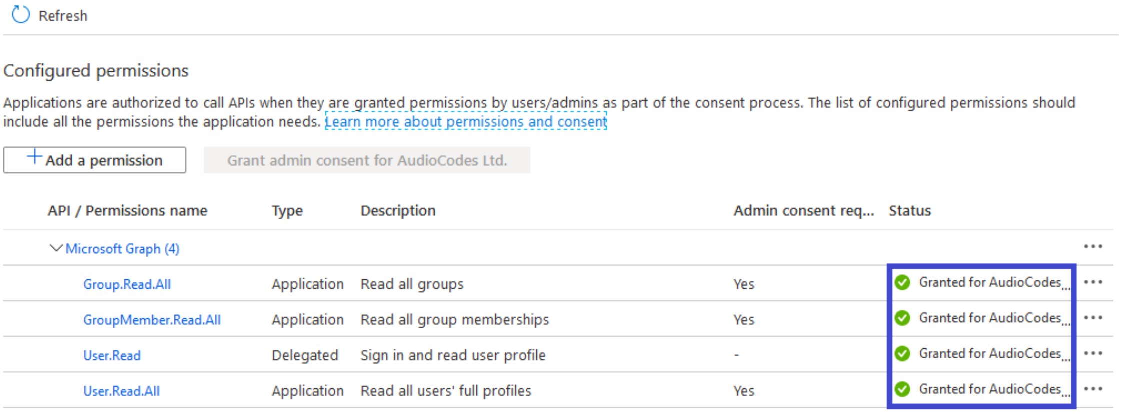
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

+ Add a permission | Grant admin consent for AudioCodes Ltd.

API / Permissions name	Type	Description	Admin consent req...	Status	
Microsoft Graph (4)					···
Group.Read.All	Application	Read all groups	Yes	⚠ Not granted for AudioC...	···
GroupMember.Read.All	Application	Read all group memberships	Yes	⚠ Not granted for AudioC...	···
User.Read	Delegated	Sign in and read user profile	-		···
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for AudioC...	···

6. Once Admin Consent is granted, the permissions are displayed as follows:

Figure 13-12: Configured Permissions



Refresh

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

+ Add a permission | Grant admin consent for AudioCodes Ltd.

API / Permissions name	Type	Description	Admin consent req...	Status	
Microsoft Graph (4)					···
Group.Read.All	Application	Read all groups	Yes	✓ Granted for AudioCodes...	···
GroupMember.Read.All	Application	Read all group memberships	Yes	✓ Granted for AudioCodes...	···
User.Read	Delegated	Sign in and read user profile	-	✓ Granted for AudioCodes...	···
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for AudioCodes...	···

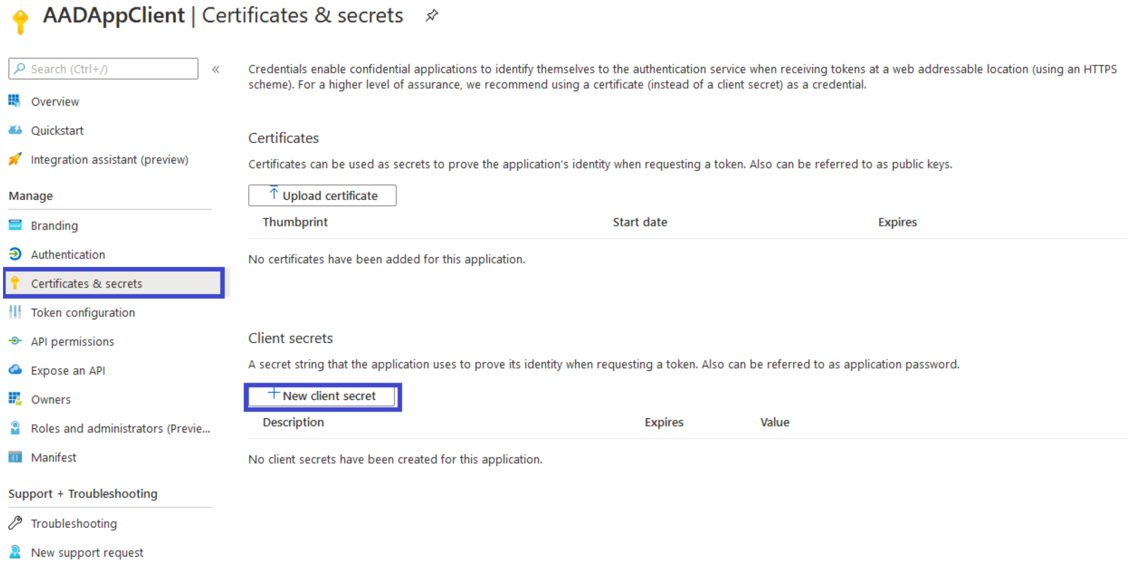
Step 3 Configure Certificates & Secrets for Azure AD Mapping

This section describes how to configure certificates and secrets for Azure AD mapping.

➢ **Do the following:**

1. In the Navigation pane, select **Manage** > **Certificates & secrets.**

Figure 13-13: Certificates and Secrets



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires

No certificates have been added for this application.

Client secrets

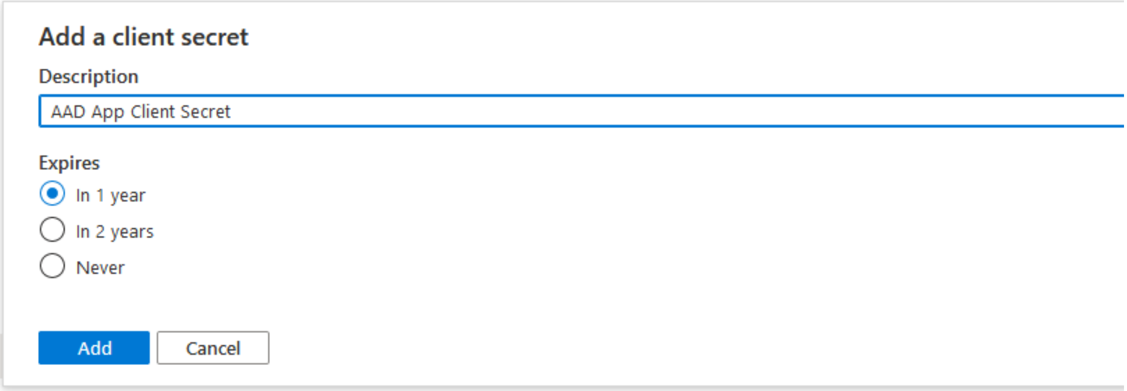
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value

No client secrets have been created for this application.

2. Click **+ New client secret.**

Figure 13-14: Add a Client Secret



Add a client secret

Description

AAD App Client Secret

Expires

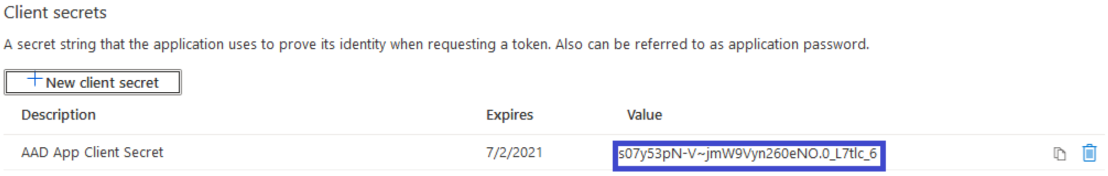
● In 1 year
○ In 2 years
○ Never

3. Enter a "Description", select "Expires" time and then click **Add**.

Its highly recommended to set to 'Never'.

A client secret is generated and displayed as below.

Figure 13-15: New Client Secret



Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value
AAD App Client Secret	7/2/2021	s07y53pN-V~jmW9Vyn260eNO.0_L7tlc_6

4. Copy the Value of the client secret for further configuration in SmartTAP 360° (see Step 4 Configure Azure Active Directory Client in SmartTAP 360° on the next page).

Step 4 Configure Azure Active Directory Client in SmartTAP 360°

To configure the client application in SmartTAP 360°, ensure that you all the required details from AAD Configuration including:

- Application (Client) ID
- Directory (Tenant) ID
- Client Secret

➢ Do the following:

1. Login to the SmartTAP 360° Web with Administrator role.
2. Open the Add AAD Configuration screen (**System** > **AAD** > **Add AAD Configuration**).

Figure 13-16: AAD Tab

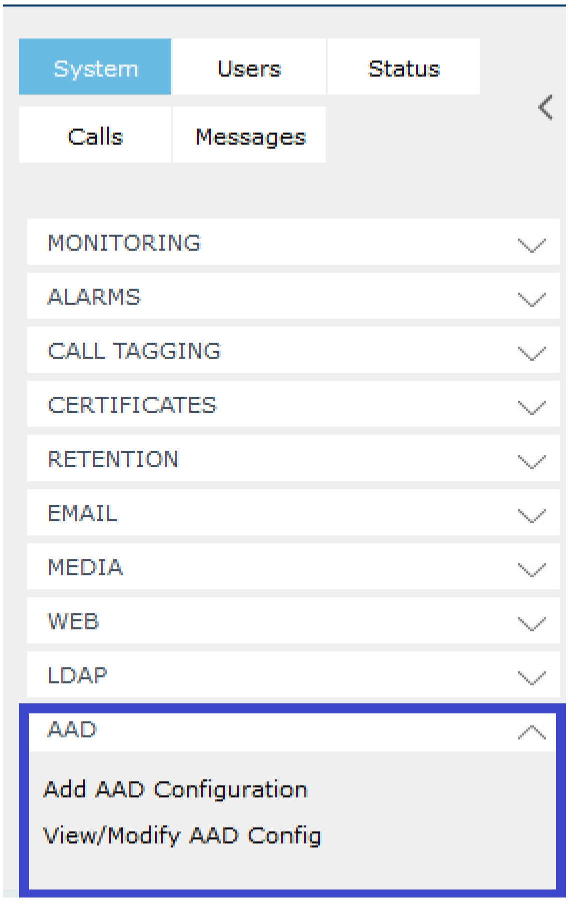
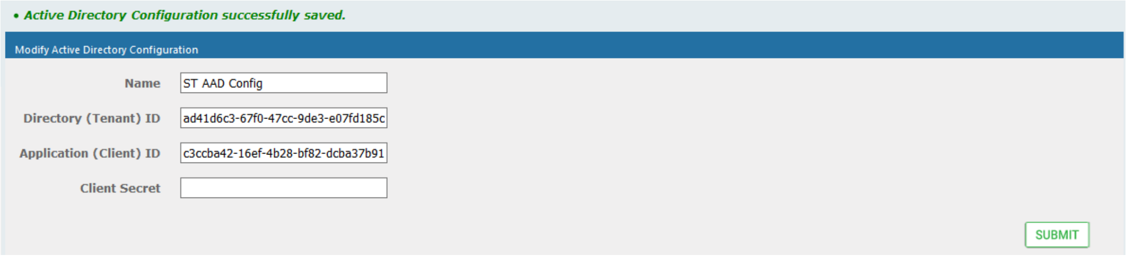


Figure 13-17: Add Active Directory Configuration



• *Active Directory Configuration successfully saved.*

Modify Active Directory Configuration

Name	ST AAD Config
Directory (Tenant) ID	ad41d6c3-67f0-47cc-9de3-e07fd185c
Application (Client) ID	c3ccba42-16ef-4b28-bf82-dcba37b91
Client Secret	

3. Enter the name of the Active Directory configuration.
4. Enter the Directory (Tenant) ID and the Application (Client) ID.
5. Click SUBMIT. A success message is displayed at the top of the screen "Active Directory Configuration successfully saved."

Step 5 Add Azure Active Directory Mapping in SmartTAP 360°

SmartTAP 360° allows mapping of AAD user from one or more member groups. Each group and it's subgroups are checked recursively to retrieve AAD users. For each group you can assign mapping profiles that map regular Active Directory user attributes as well as SmartTAP 360° custom user attributes. In this step, you must assign the custom user attribute that was defined in Adding a Microsoft Teams User Attribute on page 129 for mapping the Teams users object ID. This attribute is assigned to the user mapping profile that is then attached to an AAD group. All users that are attached to this group inherit the attributes that are defined in the mapping profile.

➢ **Do the following:**

1. Map the user attribute Object ID for the Microsoft Teams user (see Adding a Microsoft Teams User Attribute on page 129).
2. In the SmartTAP 360° Web, open the View/Modify AAD Config page (**System tab**> **AAD** folder> **View/Modify AAD Config**).

Figure 13-18: Add Active Directory Configuration

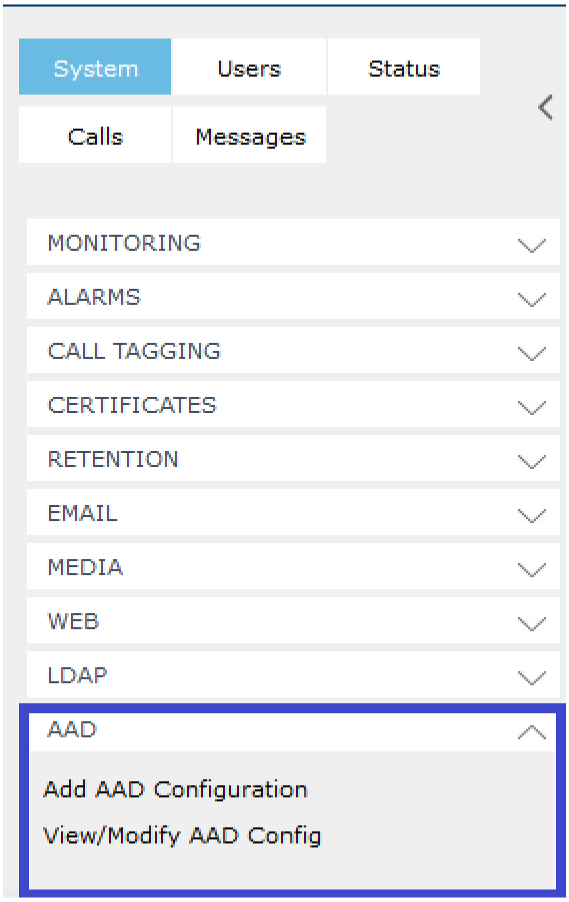
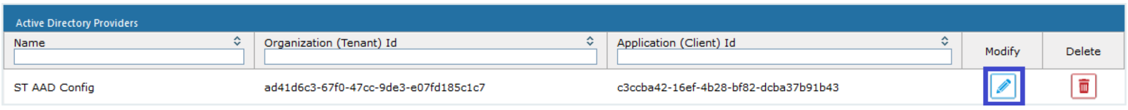


Figure 13-19: Active Directory Providers



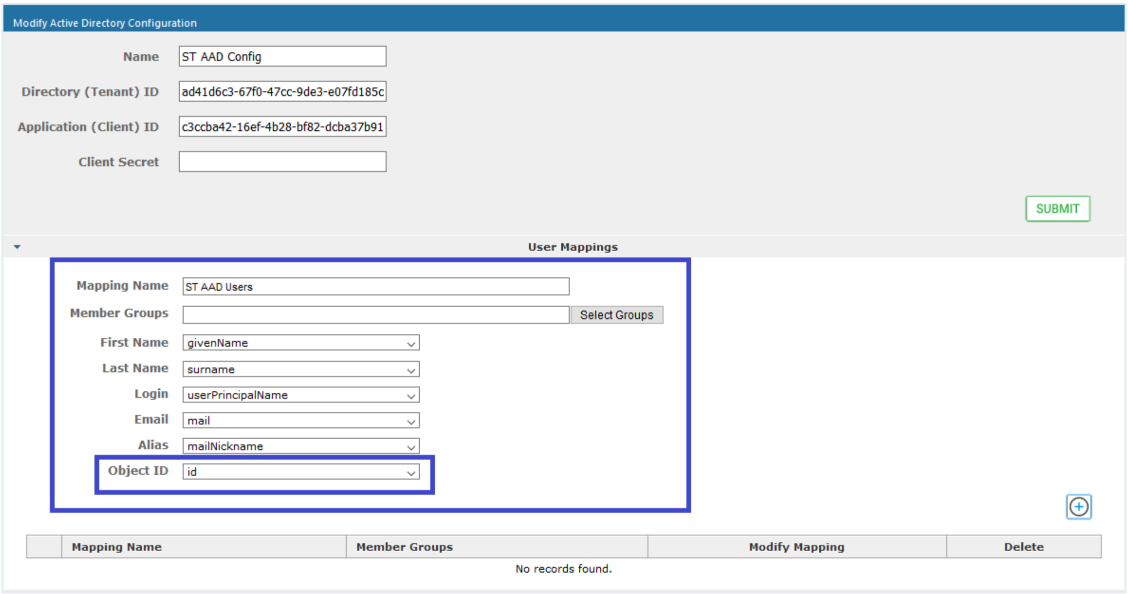
Active Directory Providers

Name	Organization (Tenant) Id	Application (Client) Id	Modify	Delete
ST AAD Config	ad41d6c3-67f0-47cc-9de3-e07fd185c1c7	c3ccba42-16ef-4b28-bf82-dcba37b91b43	✎	🗑

3. Select the provider entry that you configured in Step 4 Configure Azure Active Directory Client in SmartTAP 360° on page 255 and then click ✎.

Figure 13-20: Modify Active Directory Configuration

Figure 13-21:



Modify Active Directory Configuration

Name: ST AAD Config

Directory (Tenant) ID: ad41d6c3-67f0-47cc-9de3-e07fd185c

Application (Client) ID: c3ccba42-16ef-4b28-bf82-dcba37b91

Client Secret:

SUBMIT

User Mappings

Mapping Name: ST AAD Users

Member Groups: Select Groups

First Name: givenName

Last Name: surname

Login: userPrincipalName

Email: mail

Alias: mailNickname

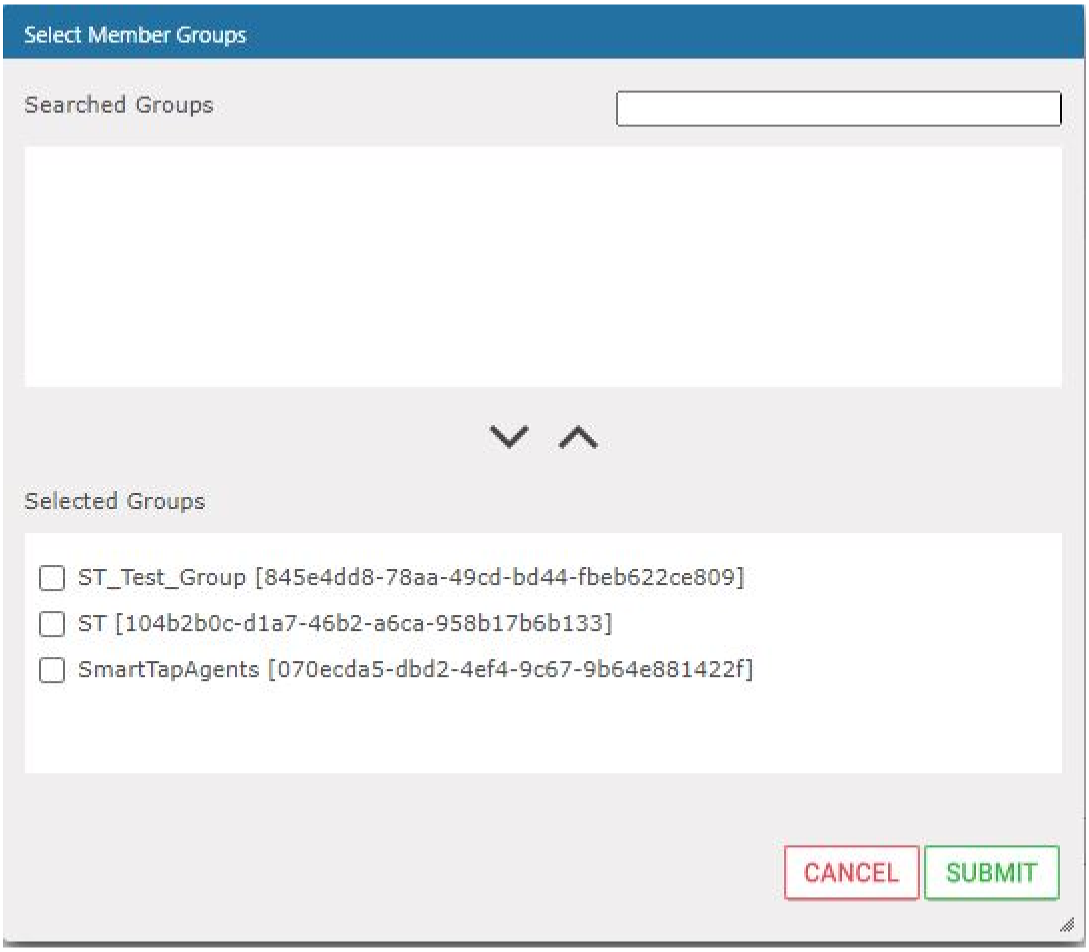
Object ID: id

	Mapping Name	Member Groups	Modify Mapping	Delete

No records found.

4. In the "User Mappings" section the standard Active Directory attributes and the custom attributes are displayed:
   - (Optional) Assign the regular Active Directory attributes as require.
   - (Mandatory) Map the Custom User attribute that you added in Step 1 to the 'id' attribute. In the example in the Figure above, the custom attribute is named 'Object ID' (this may be any user-defined string).
5. To map member groups, click **Select Groups**. In the pop up box, all of the available AAD Groups and their OIDs are displayed.
6. Select the groups from where users are mapped and click SUBMIT.

Figure 13-22: Select Member Groups



□ ST_Test_Group [845e4dd8-78aa-49cd-bd44-fbeb622ce809]

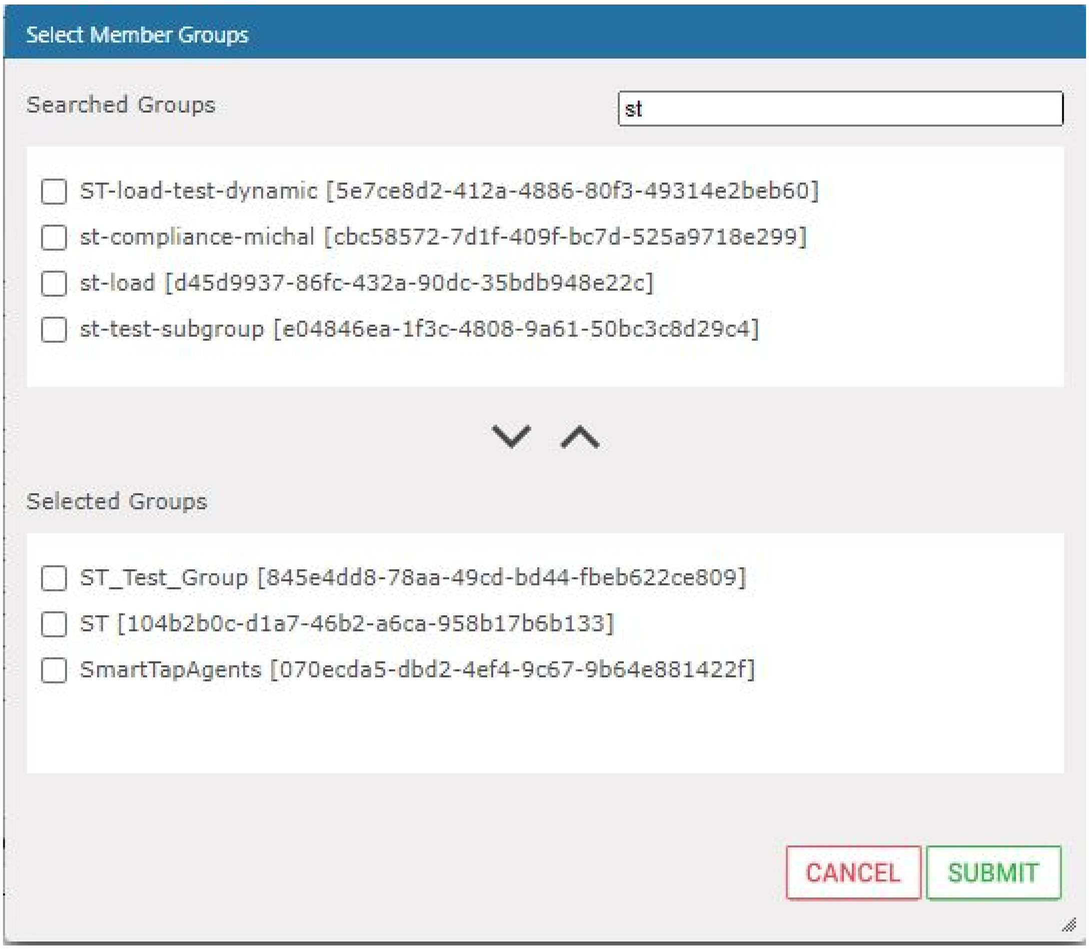
□ ST [104b2b0c-d1a7-46b2-a6ca-958b17b6b133]

□ SmartTapAgents [070ecda5-dbd2-4ef4-9c67-9b64e881422f]

Selected groups are displayed comma-separated in the Member Groups file.

You can search for groups via the group's prefix. After typing a search text string, the results are displayed in the 'Search Groups' section.

Figure 13-23: Select Member Groups



Select Member Groups

Searched Groups st

□ ST-load-test-dynamic [5e7ce8d2-412a-4886-80f3-49314e2beb60]
□ st-compliance-michal [cbc58572-7d1f-409f-bc7d-525a9718e299]
□ st-load [d45d9937-86fc-432a-90dc-35bdb948e22c]
□ st-test-subgroup [e04846ea-1f3c-4808-9a61-50bc3c8d29c4]

Selected Groups

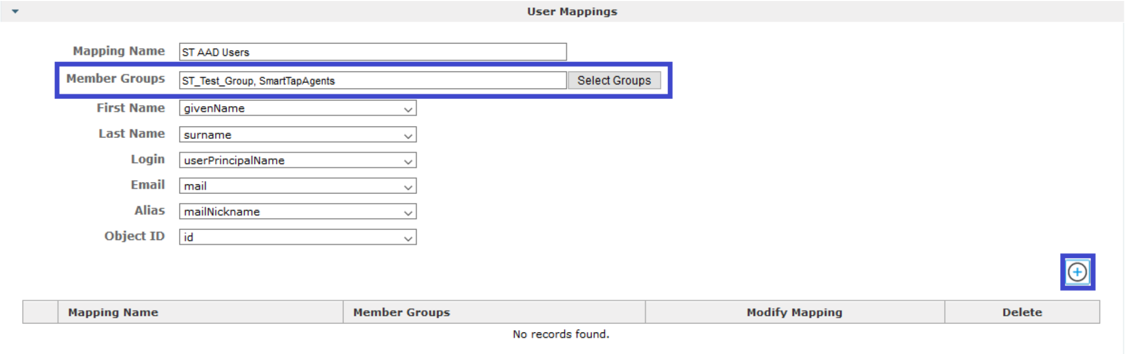
□ ST_Test_Group [845e4dd8-78aa-49cd-bd44-fbeb622ce809]
□ ST [104b2b0c-d1a7-46b2-a6ca-958b17b6b133]
□ SmartTapAgents [070ecda5-dbd2-4ef4-9c67-9b64e881422f]

- Click ⌄ to move selected groups from the ‘Search Groups’ section to the ‘Selected Groups’ section.
- Click ⌃ to remove selected groups from the ‘Selected Groups’ section, and in case the search results should contain those groups, they are moved back to the ‘Search Groups’ section.

⚠ The maximum number of search results is limited to "10".

7. Click ⊕ to add this mapping to SmartTAP 360°.

Figure 13-24: Member Groups



User Mappings

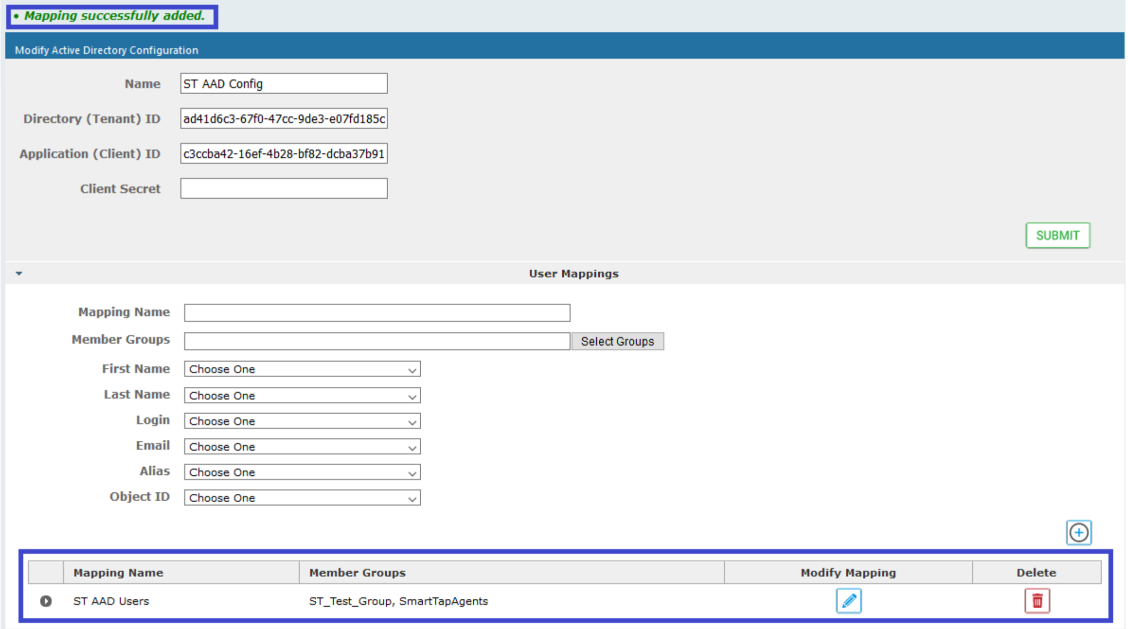
Mapping Name	ST AAD Users
Member Groups	ST_Test_Group, SmartTapAgents [Select Groups]
First Name	givenName
Last Name	surname
Login	userPrincipalName
Email	mail
Alias	mailNickname
Object ID	id

	Mapping Name	Member Groups	Modify Mapping	Delete

No records found.

Successful user mapping is displayed under the User Mapping table.

Figure 13-25: Mapping Successfully Added



- *Mapping successfully added.*

Modify Active Directory Configuration

Name	ST AAD Config
Directory (Tenant) ID	ad41d6c3-67f0-47cc-9de3-e07fd185c
Application (Client) ID	c3ccba42-16ef-4b28-bf82-dcba37b91
Client Secret	

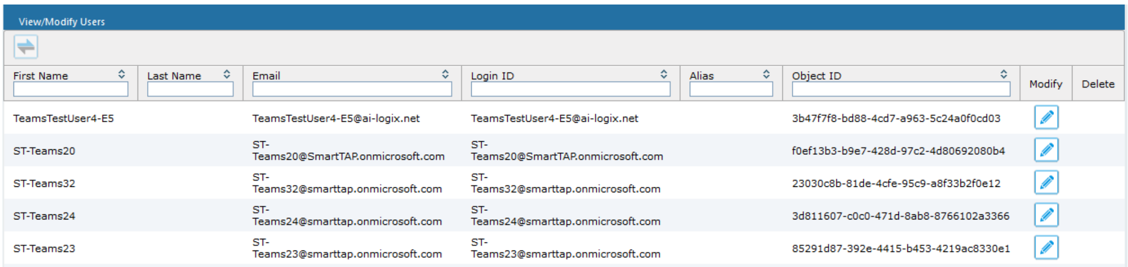
User Mappings

Mapping Name	
Member Groups	[Select Groups]
First Name	Choose One
Last Name	Choose One
Login	Choose One
Email	Choose One
Alias	Choose One
Object ID	Choose One

	Mapping Name	Member Groups	Modify Mapping	Delete
●	ST AAD Users	ST_Test_Group, SmartTapAgents		

All mapped users are displayed in the **Users** > **View/Modify Users** page.

Figure 13-26: Mapped Users



View/Modify Users

First Name	Last Name	Email	Login ID	Alias	Object ID	Modify	Delete
TeamsTestUser4-E5		TeamsTestUser4-E5@ai-logix.net	TeamsTestUser4-E5@ai-logix.net		3b47f7f8-bd88-4cd7-a963-5c24a0f0cd03		
ST-Teams20		ST-Teams20@SmartTAP.onmicrosoft.com	ST-Teams20@SmartTAP.onmicrosoft.com		f0ef13b3-b9e7-428d-97c2-4d80692080b4		
ST-Teams32		ST-Teams32@smarttap.onmicrosoft.com	ST-Teams32@smarttap.onmicrosoft.com		23030c8b-81de-4cfe-95c9-a8f33b2f0e12		
ST-Teams24		ST-Teams24@smarttap.onmicrosoft.com	ST-Teams24@smarttap.onmicrosoft.com		3d811607-c0c0-471d-8ab8-8766102a3366		
ST-Teams23		ST-Teams23@smarttap.onmicrosoft.com	ST-Teams23@smarttap.onmicrosoft.com		85291d87-392e-4415-b453-4219ac8330e1		

Azure Active Directory User Authentication

For SmartTAP 360° version 5.1 and later users are mapped from Organizations' (Tenant) Azure Active Directory (AAD) and authenticate (login) with SmartTAP 360° Web using their Microsoft login credentials. SmartTAP 360° uses the OpenID Connect Authorization Code Flow) to authenticate users with Microsoft Identity Platform.

⚠ Refer to https://openid.net/specs/openid-connect-core-1_0.html#CodeFlowSteps

Azure Active Directory user authentication involves the following steps:

- **Step 1:** Register an web application (client) in Azure Active Directory on behalf of SmartTAP 360° (see Step 1 Register App in Azure Active Directory below).
- **Step 2:** Check the API permission for this app in AAD (see Step 2 Check API Permissions on page 265)
- **Step 3:** Configure Certificates & Secrets for this application in AAD (see Step 3 Configure Certificates & Secrets on page 267)
- **Step 4:** Configure this client in SmartTAP 360° Web as OpenID Connect (OIDC) authentication client, also known as Relying Party (see Step 4 Configure OpenID Connect OIDC Client in SmartTAP 360° on page 268).
- **Step 5:** Assign Security Profile to Azure Active Directory user in SmartTAP 360° (see Step 5 Assign Security profile to Azure Active Directory user in SmartTAP 360° on page 270)

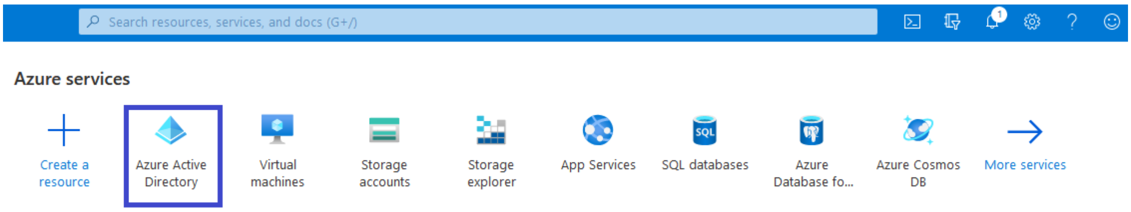
Step 1 Register App in Azure Active Directory

This step describes how to register the App in Azure Active Directory.

➢ To register app in ADD:

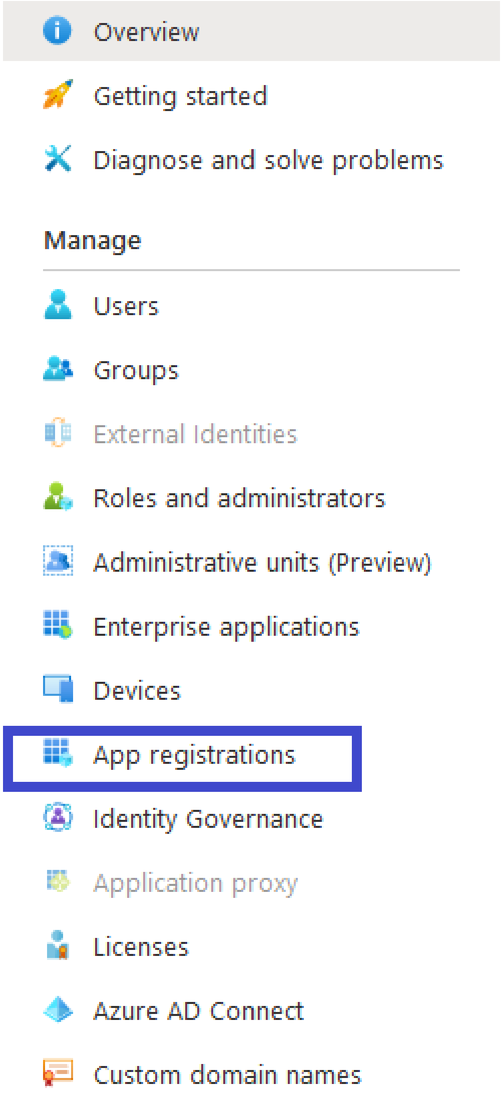
1. Login to Azure portal (https://portal.azure.com/)
2. Access Azure Active Directory Service.

Figure 13-27: Azure Services



3. In the Navigation pane, click "App Registration" link.

Figure 13-28: App Registrations



4. On Right side panel client "New Registration".

Figure 13-29: New Registrations

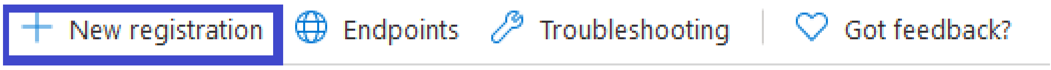
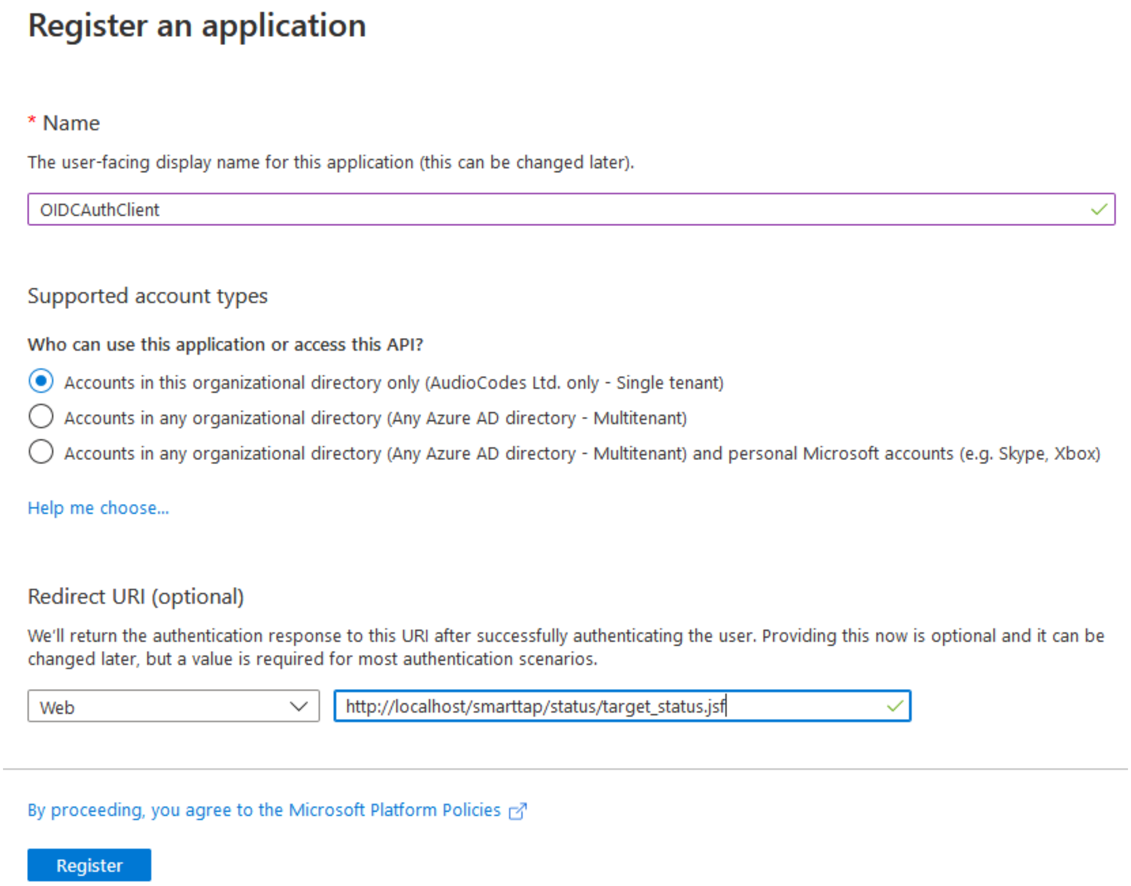


Figure 13-30: Register an Application



Register an application

* Name

The user-facing display name for this application (this can be changed later).

OIDCAuthClient ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (AudioCodes Ltd. only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

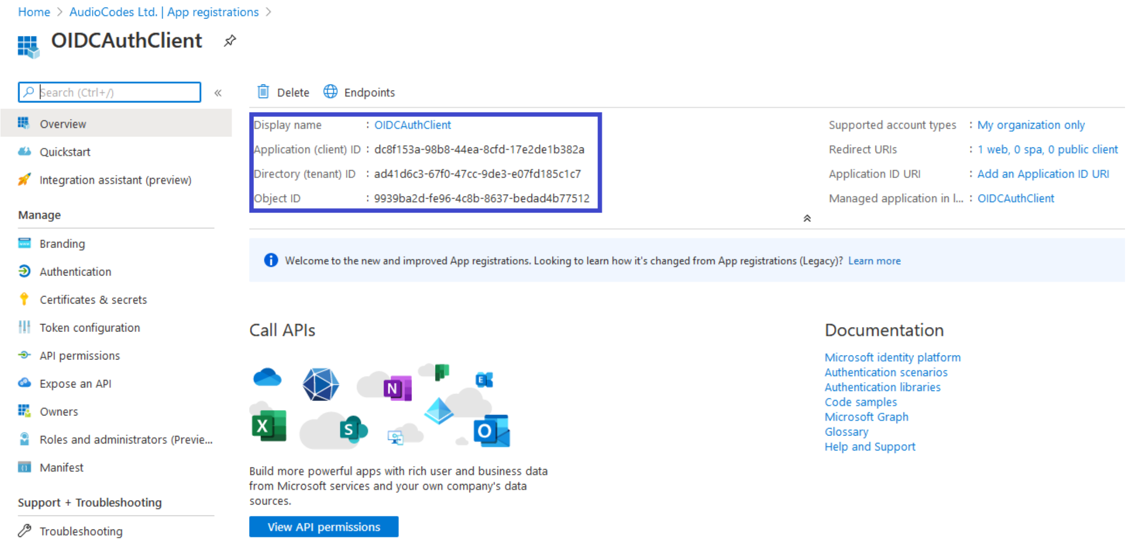
Web | http://localhost/smarttap/status/target_status.jsf ✓

By proceeding, you agree to the Microsoft Platform Policies

5. Enter the following details:
   - Name: Enter a name for the client application
   - Supported account types: select the radio button for "Accounts in this organizational directory only (AudioCodes Ltd. only - Single tenant)"
   - Redirect URI (optional):
     - If only HTTP is configured in SmartTAP 360° enter http://localhost/SmartTAP 360°/status/target_status.jsf
     - If HTTPS is configured in SmartTAP 360° enter https://localhost/SmartTAP 360°/status/target_status.jsf
6. Click **Register** to confirm registration.

   On successful registration the following details will be displayed.

Figure 13-31: OIDCAuthClient



Display name : OIDCAuthClient
Application (client) ID : dc8f153a-98b8-44ea-8cfd-17e2de1b382a
Directory (tenant) ID : ad41d6c3-67f0-47cc-9de3-e07fd185c1c7
Object ID : 9939ba2d-fe96-4c8b-8637-bedad4b77512

Supported account types : My organization only
Redirect URIs : 1 web, 0 spa, 0 public client
Application ID URI : Add an Application ID URI
Managed application in l... : OIDCAuthClient

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

7. Copy the value of Application (client) ID and Directory (tenant) ID for later configuration in the SmartTAP 360° Web(see Step 4 Configure OpenID Connect OIDC Client in SmartTAP 360° on page 268).

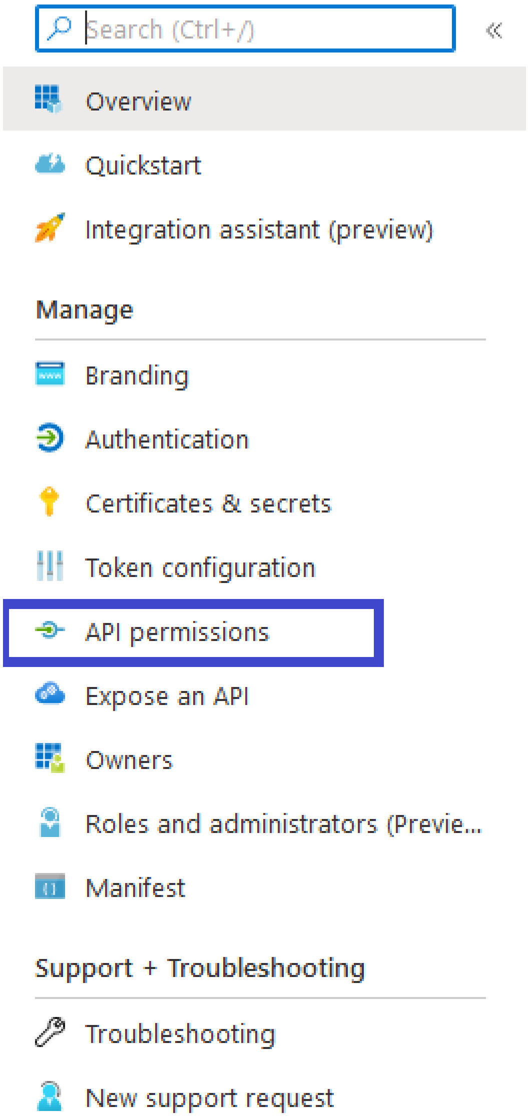
Step 2 Check API Permissions

This step describes how to check API permissions.

➢ To check API permissions:

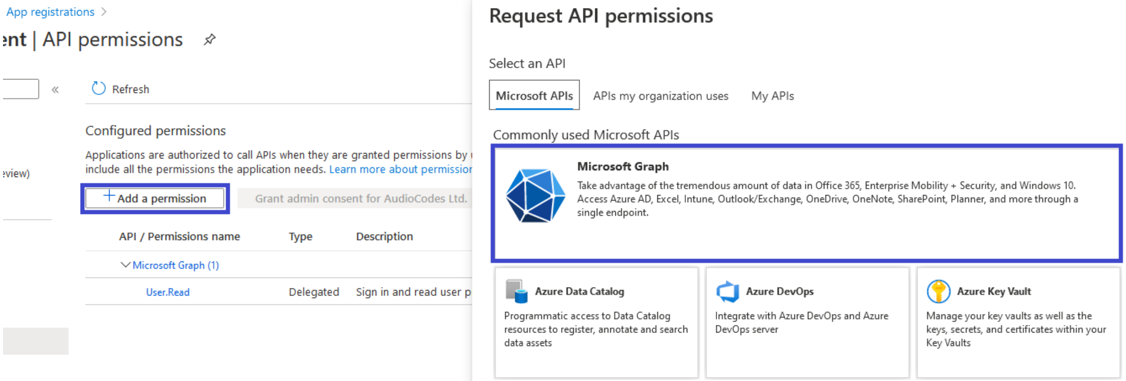
1. Open the API Permissions screen (**Manage** > **API permissions**).

Figure 13-32: API permissions



2. On right side panel click **Add a permission** and select "Microsoft Graph" APIs.

Figure 13-33: Add Permissions



Configured permissions

Applications are authorized to call APIs when they are granted permissions by u include all the permissions the application needs. Learn more about permissior

API / Permissions name	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user p

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

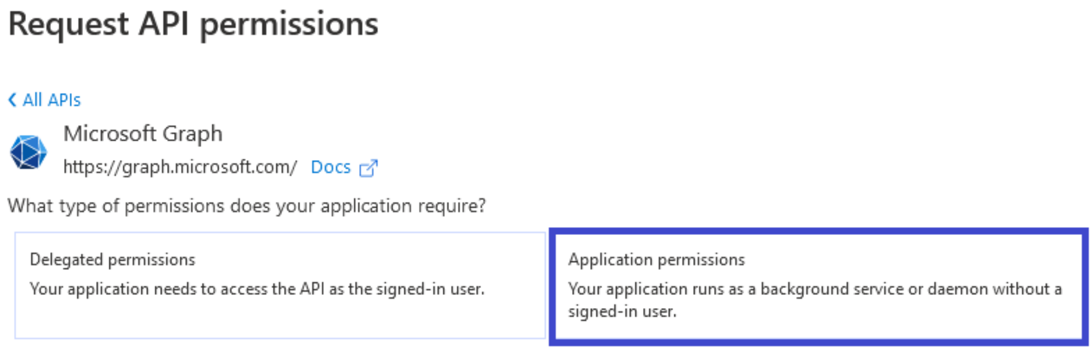
Azure Data Catalog
Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Key Vault
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

3. On the Request API permissions section click **Application permissions** link.

Figure 13-34: Application Permissions



Request API permissions

❮ All APIs

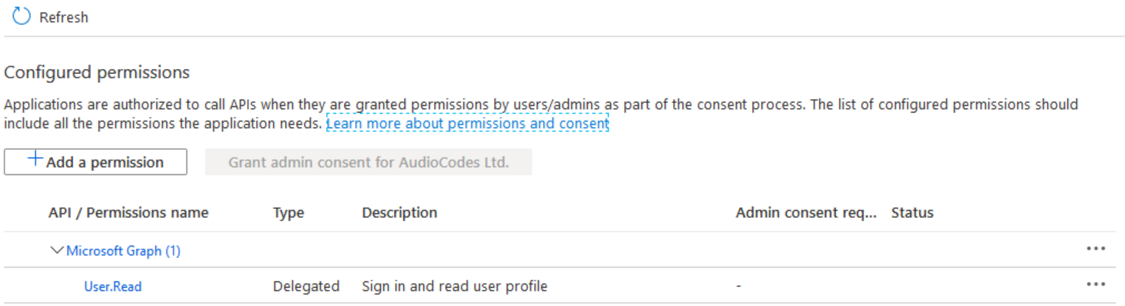
Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Figure 13-35: Configured Permissions



Refresh

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	-	

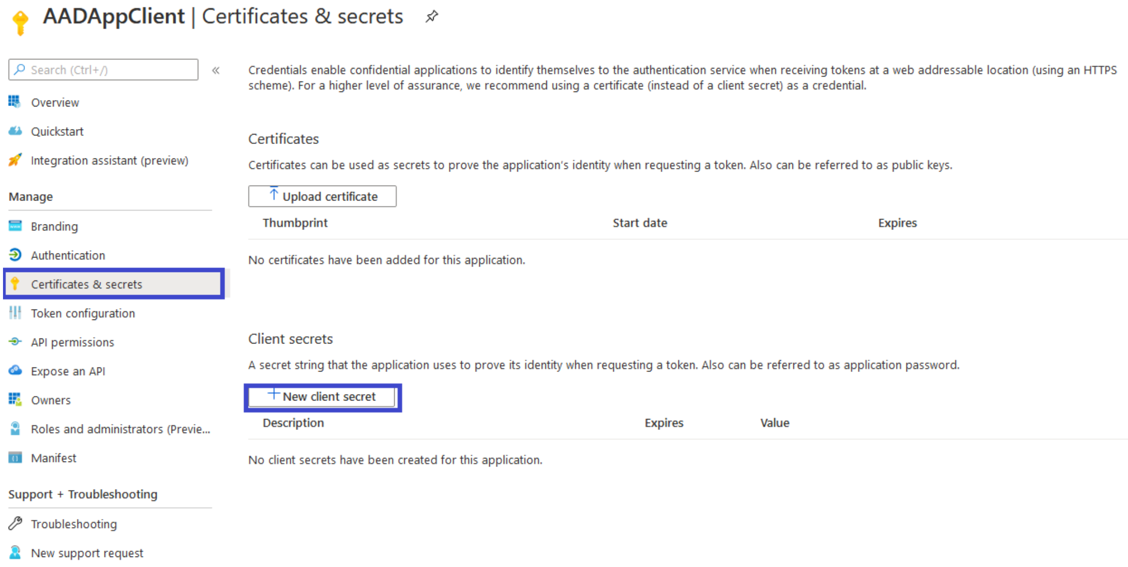
4. Verify that the 'User.Read' permission is displayed.

Step 3 Configure Certificates & Secrets

➢ Do the following:

1. In the Navigation pane, open the Certificates & Secrets page (**Manage** > **Certificate & Secrets**).

Figure 13-36: Certificates & Secrets



AADAppClient | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires
No certificates have been added for this application.		

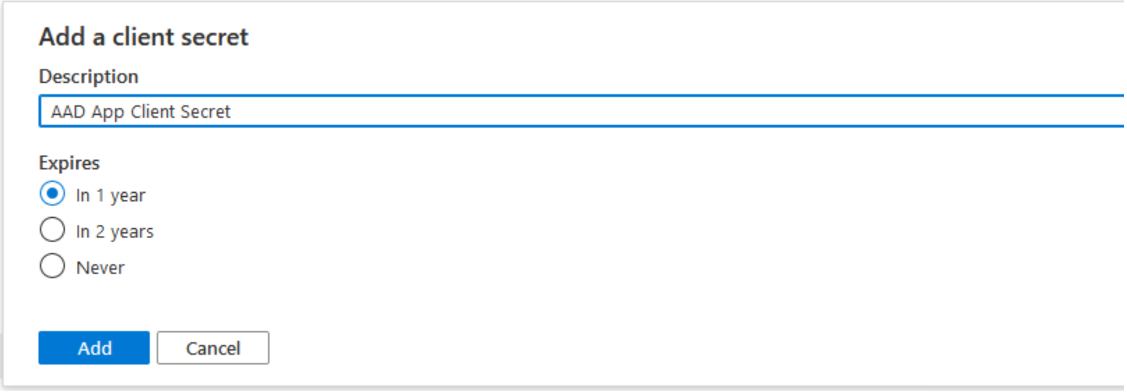
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value
No client secrets have been created for this application.		

2. Click **+ New client secret link.**

Figure 13-37: Add a client secret



Add a client secret

Description

AAD App Client Secret

Expires

● In 1 year

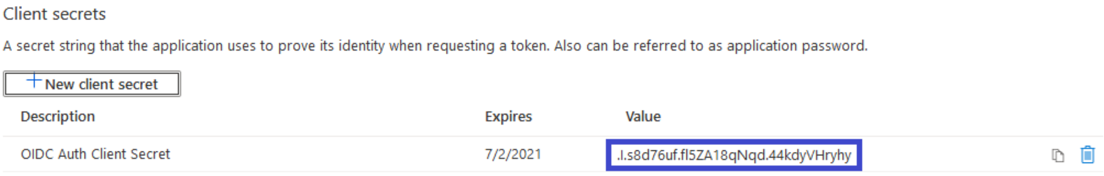
○ In 2 years

○ Never

3. Enter a "Description", select "Expires" time and click **Add**.

A client secret is generated and displayed as below.

Figure 13-38: Client Secret



Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value
OIDC Auth Client Secret	7/2/2021	.l.s8d76uf.fl5ZA18qNqd.44kdyVHryhy

4. Copy the Value of the client secret for later configuration in the SmartTAP 360° Web (see Step 4 Configure Azure Active Directory Client in SmartTAP 360° on page 255).

Step 4 Configure OpenID Connect OIDC Client in SmartTAP 360°

To configure the OIDC Client in SmartTAP 360°, first collect all the required details from Web Application Registration in AAD. This includes the following:

- Application (Client) ID
- Directory (Tenant) ID
- Client Secret
- Redirect URI

➢ **Do the following:**

1. Login to the SmartTAP 360° Web with a user that has "sysAdmin" role.
2. Open the OAuth Client Config screen (**System** > **WEB** > **OAuth Client Config**).

Figure 13-39: OpenID Connect

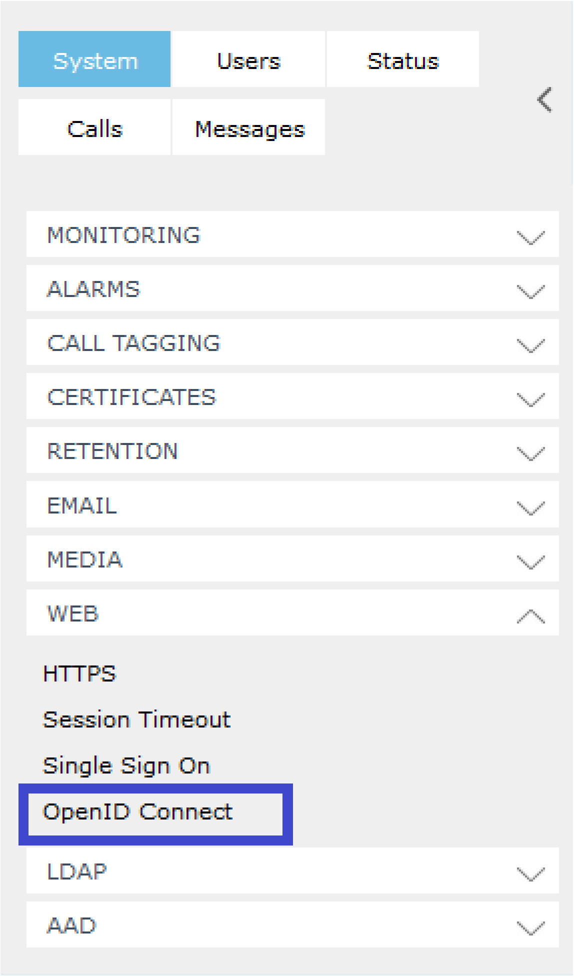
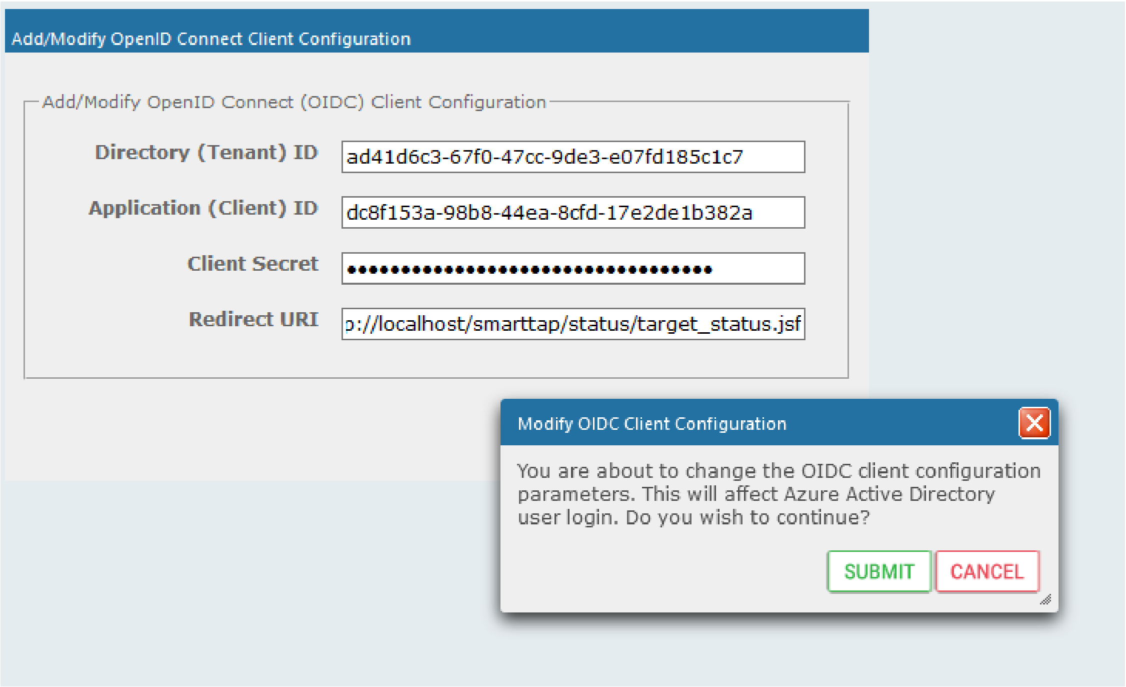


Figure 13-40: OpenID Connect Client Configuration


Add/Modify OpenID Connect Client Configuration

Add/Modify OpenID Connect (OIDC) Client Configuration

Directory (Tenant) ID: ad41d6c3-67f0-47cc-9de3-e07fd185c1c7

Application (Client) ID: dc8f153a-98b8-44ea-8cfd-17e2de1b382a

Client Secret: ••••••••••••••••••••••••••••••••••

Redirect URI: ɔ://localhost/smarttap/status/target_status.jsf

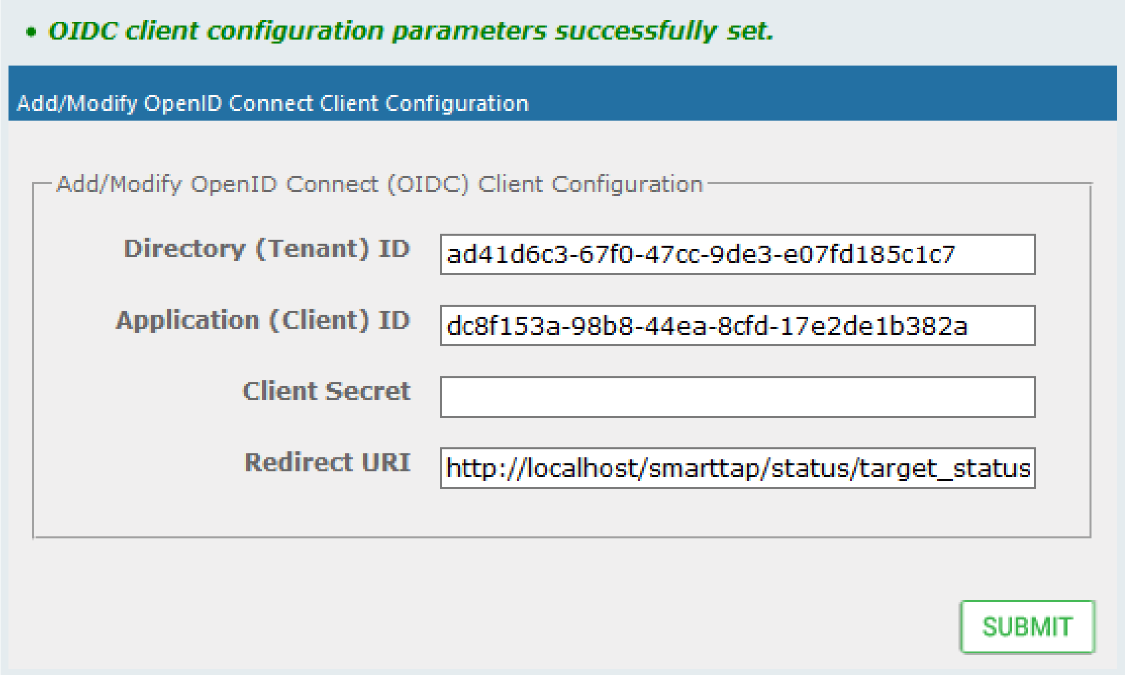
Modify OIDC Client Configuration

You are about to change the OIDC client configuration parameters. This will affect Azure Active Directory user login. Do you wish to continue?

3. Enter the details and then click SUBMIT.

4. A confirmation message is displayed that the OIDC client configuration has been successfully saved to SmartTAP 360°.

Figure 13-41: OID Client Configuration Parameters Successfully Set



- *OIDC client configuration parameters successfully set.*

Add/Modify OpenID Connect Client Configuration

Add/Modify OpenID Connect (OIDC) Client Configuration

Directory (Tenant) ID	ad41d6c3-67f0-47cc-9de3-e07fd185c1c7
Application (Client) ID	dc8f153a-98b8-44ea-8cfd-17e2de1b382a
Client Secret	
Redirect URI	http://localhost/smarttap/status/target_status

Step 5 Assign Security profile to Azure Active Directory user in SmartTAP 360°

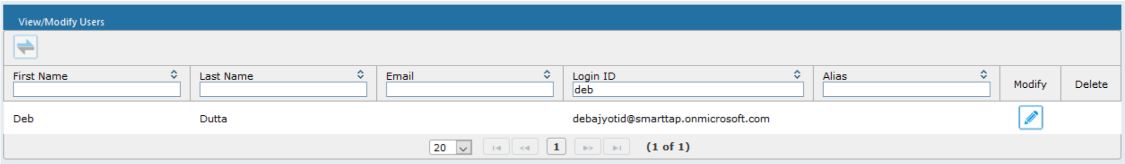
This step describes how to assign a user to "agent" security profile in SmartTAP 360°.

➢ To assign a security profile:

1. Login to SmartTAP 360° with a user that has "userAdmin" permissionns.

2. Open the View/Modify Users page (**Users** tab > **User Management** > **View/Modify Users**).

Figure 13-42: View/Modify Users

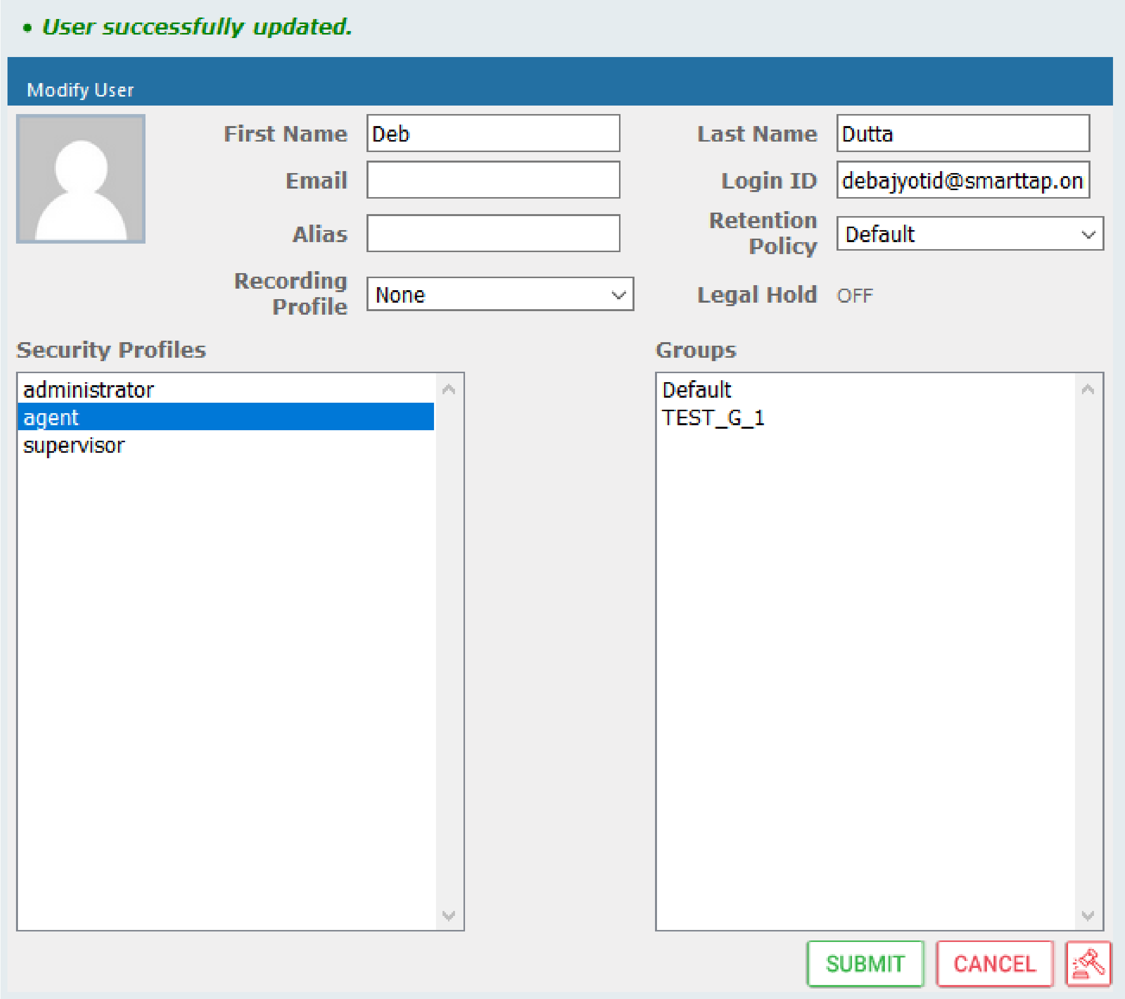


View/Modify Users

First Name	Last Name	Email	Login ID	Alias	Modify	Delete
			deb			
Deb	Dutta		debajyotid@smarttap.onmicrosoft.com		✎	

3. Assign "agent" security profile and then click SUBMIT. A confirmation message is displayed:

Figure 13-43: User Successfully Updated



- *User successfully updated.*

Modify User

First Name	Deb	Last Name	Dutta
Email		Login ID	debajyotid@smarttap.on
Alias		Retention Policy	Default
Recording Profile	None	Legal Hold	OFF

Security Profiles

- administrator
- agent
- supervisor

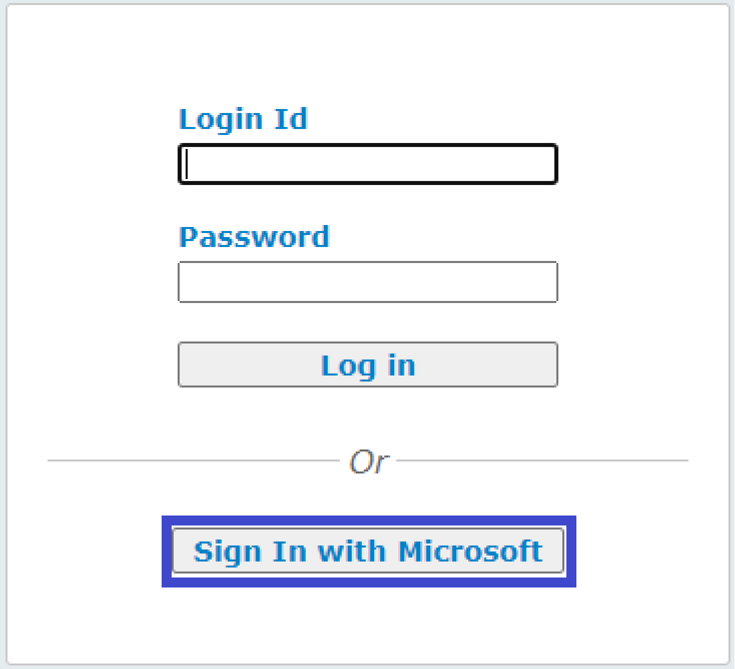
Groups

- Default
- TEST_G_1

4. Login to SmartTAP 360° using Microsoft Login Credentials.

   - On the SmartTAP 360° login page, click **Sign In with Microsoft**.

Figure 13-44: Microsoft Sign in



The user is redirected to Microsoft MFC Login page:

Figure 13-45: Microsoft MFC Login Page

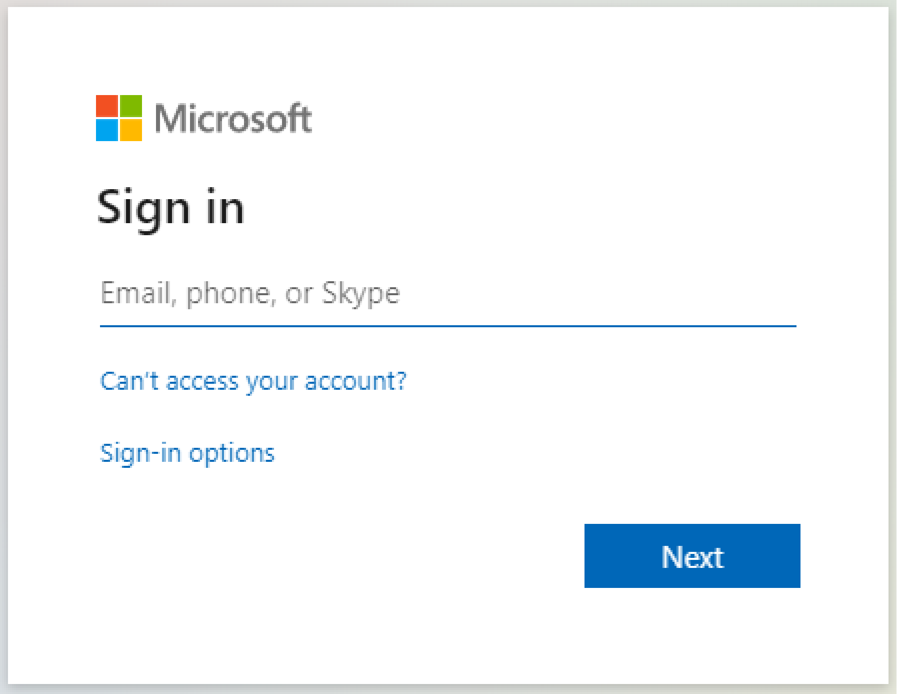
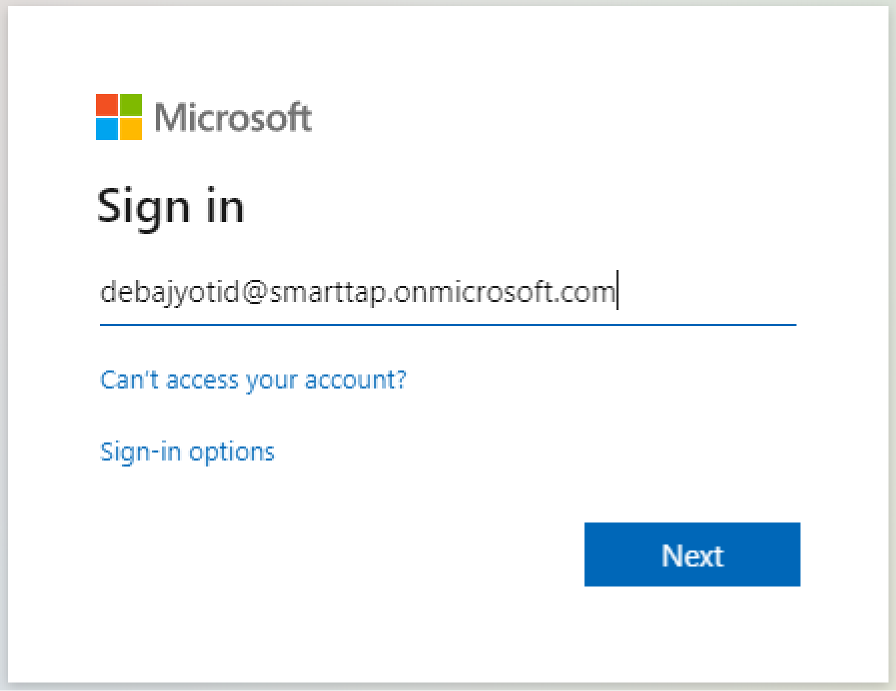


Figure 13-46: Login id

- Enter the Sign in info and password

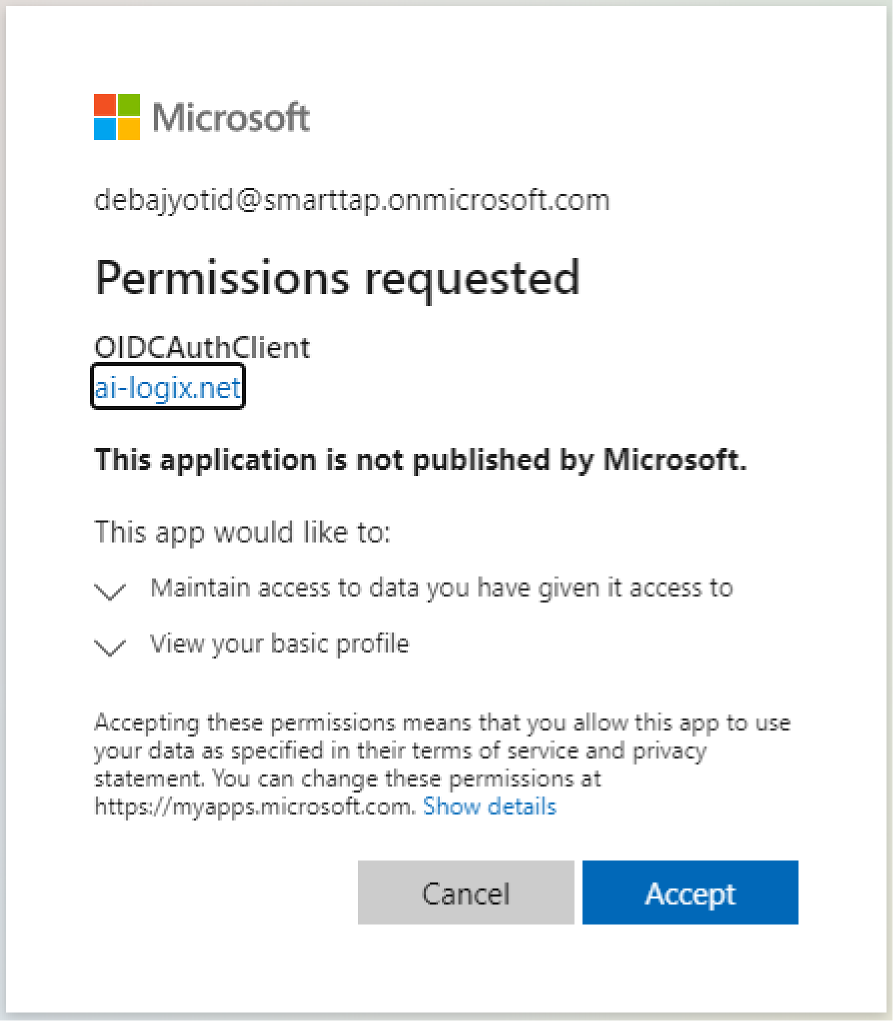
Figure 13-47: Sign In



debajyotid@smarttap.onmicrosoft.com

- Allow permission to the client app to use user authentication data.

Figure 13-48: Permissions Requested



Microsoft

debajyotid@smarttap.onmicrosoft.com

Permissions requested

OIDCAuthClient
ai-logix.net

This application is not published by Microsoft.

This app would like to:

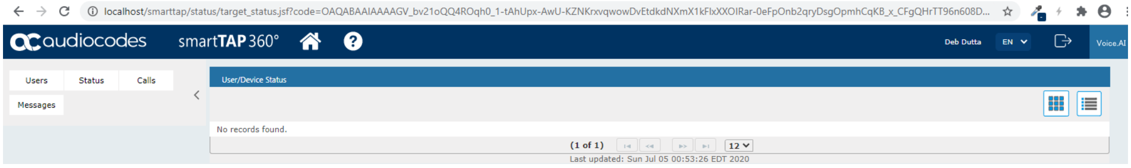
- Maintain access to data you have given it access to
- View your basic profile

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

The user is re-directed to SmartTAP 360° URI configured in AAD (see Step 1 Register App in Azure Active Directory on page 262 i.e. http://localhost/SmartTAP 360°/status/target_status.jsf

Figure 13-49: User Device Status

Figure 13-50:



localhost/smarttap/status/target_status.jsf?code=OAQABAAIAAAAGV_bv21oQQ4ROqh0_1-tAhUpx-AwU-KZNKrxvqwowDvEtdkdNXmX1kFlxXXOIRar-0eFpOnb2qryDsgOpmhCqKB_x_CFgQHrTT96n608D...

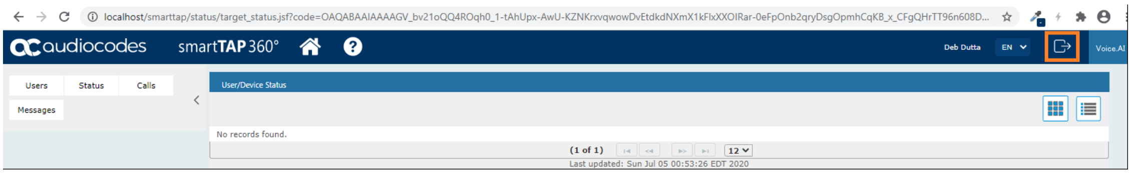
No records found.

(1 of 1) 12

Last updated: Sun Jul 05 00:53:26 EDT 2020

5. An Azure Active Directory user logs off from SmartTAP 360° Web.

Figure 13-51: Logout



localhost/smarttap/status/target_status.jsf?code=OAQABAAIAAAAGV_bv21oQQ4ROqh0_1-tAhUpx-AwU-KZNKrxvqwowDvEtdkdNXmX1kFlxXXOIRar-0eFpOnb2qryDsgOpmhCqKB_x_CFgQHrTT96n608D...

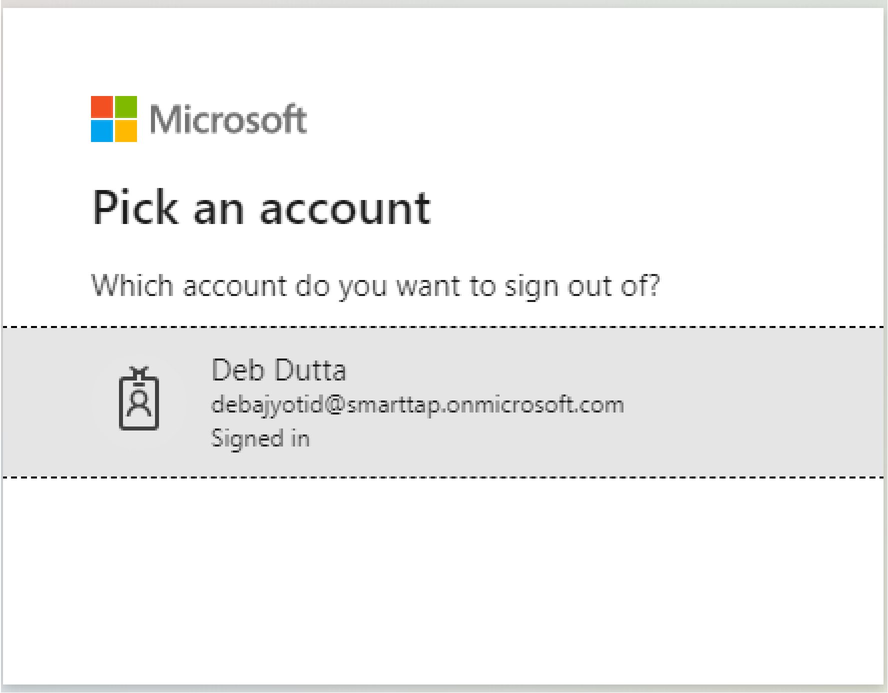
No records found.

(1 of 1) 12

Last updated: Sun Jul 05 00:53:26 EDT 2020

6. User is prompted to select the Microsoft account that needs to be signed out.

Figure 13-52: Pick an Account



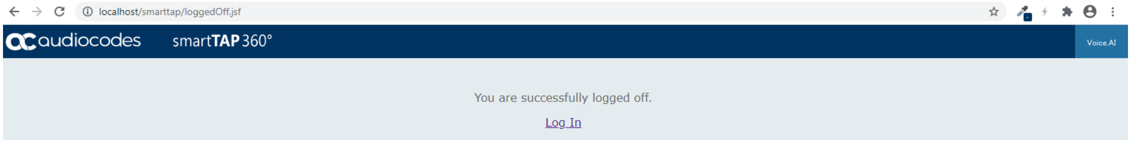
Pick an account

Which account do you want to sign out of?

Deb Dutta
debajyotid@smarttap.onmicrosoft.com
Signed in

7. When the account is selected, the user is redirected to the SmartTAP 360° log off page.

Figure 13-53: SmartTAP 360° LogOff Page



You are successfully logged off.

Log In

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.

200 Cottontail Lane

Suite A101E

Somerset NJ 08873

Tel: +1-732-469-0880

Fax: +1-732-469-2298

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

Website: https://www.audiocodes.com/

Documentation Feedback: https://online.audiocodes.com/documentation-feedback

Document #: LTRT-27175